http://www.icact.org/journal.asp

ICACT-TACT JOURNAL

Transactions on Advanced Communications Technology

Volume 8 Issue 3, May. 2019, ISSN: 2288-0003

Editor-in-Chief
Prof. Thomas Byeongnam YOON, PhD.

GIRI
Global IT Research Institute

Journal Editorial Board

Editor-in-Chief

Editors

Editor Guide

■ Introduction for Editor or Reviewer

All the editor group members are to be assigned as a evaluator(editor or reviewer) to submitted journal papers at the discretion of the Editor-in-Chief. It will be informed by eMail with a Member Login ID and Password.

Once logined the Website via the Member Login menu in left as a evaluator, you can find out the paper assigned to you. You can evaluate it there. All the results of the evaluation are supposed to be shown in the Author Homepage in the real time manner. You can also enter the Author Homepage assigned to you by the Paper ID and the author's eMail address shown in your Evaluation Webpage. In the Author Homepage, you can communicate each other efficiently under the peer review policy. Please don't miss it!

All the editor group members are supposed to be candidates of a part of the editorial board, depending on their contribution which comes from history of ICACT TACT as an active evaluator. Because the main contribution comes from sincere paper reviewing role.

■ Role of the Editor

The editor's primary responsibilities are to conduct the peer review process, and check the final camera-ready manuscripts for any technical, grammatical or typographical errors.

As a member of the editorial board of the publication, the editor is responsible for ensuring that the publication maintains the highest quality while adhering to the publication policies and procedures of the ICACT TACT(Transactions on the Advanced Communications Technology).

For each paper that the editor-in-chief gets assigned, the Secretariat of ICACT Journal will send the editor an eMail requesting the review process of the paper.

The editor is responsible to make a decision on an "accept", "reject", or "revision" to the Editor-in-Chief via the Evaluation Webpage that can be shown in the Author Homepage also.

■ Deadlines for Regular Review

Editor-in-Chief will assign a evalaution group(a Editor and 2 reviewers) in a week upon receiving a completed Journal paper submission. Evaluators are given 2 weeks to review the paper. Editors are given a week to submit a recommendation to the Editor-in-Chief via the evaluation Webpage, once all or enough of the reviews have come in. In revision case, authors have a maximum of a month to submit their revised manuscripts. The deadlines for the regular review process are as follows:

Evalution Procedure	Deadline
Selection of Evaluation Group	1 week
Review processing	2 weeks
Editor's recommendation	1 week
Final Decision Noticing	1 week

■ Making Decisions on Manuscript

Editor will make a decision on the disposition of the manuscript, based on remarks of the reviewers. The editor's recommendation must be well justified and explained in detail. In cases where the revision is requested, these should be clearly indicated and explained. The editor must then promptly convey this decision to the author. The author may contact the editor if instructions regarding amendments to the manuscript are unclear. All these actions could be done via the evaluation system in this Website. The guidelines of decisions for publication are as follows:

Decision	Description
Accept	An accept decision means that an editor is accepting the paper with no further modifications. The paper will not be seen again by the editor or by the reviewers.
Reject	The manuscript is not suitable for the ICACT TACT publication.
Revision	The paper is conditionally accepted with some requirements. A revision means that the paper should go back to the original reviewers for a second round of reviews. We strongly discourage editors from making a decision based on their own review of the manuscript if a revision had been previously required.

■ Role of the Reviewer

Reviewer Webpage:

Once logined the Member Login menu in left, you can find out papers assigned to you. You can also login the Author Homepage assigned to you with the paper ID and author's eMail address. In there you can communicate each other via a Communication Channel Box.

Quick Review Required:

You are given 2 weeks for the first round of review and 1 week for the second round of review. You must agree that time is so important for the rapidly changing IT technologies and applications trend. Please respect the deadline. Authors undoubtedly appreciate your quick review.

Anonymity:

Do not identify yourself or your organization within the review text.

Review:

Reviewer will perform the paper review based on the main criteria provided below. Please provide detailed public comments for each criterion, also available to the author.

- How this manuscript advances this field of research and/or contributes something new to the literature?
- Relevance of this manuscript to the readers of TACT?
- Is the manuscript technically sound?
- Is the paper clearly written and well organized?
- Are all figures and tables appropriately provided and are their resolution good quality?
- Does the introduction state the objectives of the manuscript encouraging the reader to read on?
- Are the references relevant and complete?

Supply missing references:

Please supply any information that you think will be useful to the author in revision for enhancing quality of the paperor for convincing him/her of the mistakes.

Review Comments:

If you find any already known results related to the manuscript, please give references to earlier papers which contain these or similar results. If the reasoning is incorrect or ambiguous, please indicate specifically where and why. If you would like to suggest that the paper be rewritten, give specific suggestions regarding which parts of the paper should be deleted, added or modified, and please indicate how.

Journal Procedure

Dear Author,

- **You can see all your paper information & progress.**

Step 1. Journal Full Paper Submission

Using the Submit button, submit your journal paper through ICACT Website, then you will get new paper ID of your journal, and send your journal Paper ID to the Secretariat@icact.org for the review and editorial processing. Once you got your Journal paper ID, never submit again! Journal Paper/CRF Template

Step 2. Full Paper Review

Using the evaluation system in the ICACT Website, the editor, reviewer and author can communicate each other for the good quality publication. It may take about 1 month.

Step 3. Acceptance Notification

It officially informs acceptance, revision, or reject of submitted full paper after the full paper review process.

Status	Action
Acceptance	Go to next Step.
Revision	Re-submit Full Paper within 1 month after Revision Notification.
Reject	Drop everything.

Step 4. Payment Registration

So far it's free of charge in case of the journal promotion paper from the registered ICACT conference paper! But you have to regist it, because you need your Journal Paper Registration ID for submission of the final CRF manuscripts in the next step's process. Once you get your Registration ID, send it to Secretariat@icact.org for further process.

Step 5. Camera Ready Form (CRF) Manuscripts Submission

After you have received the confirmation notice from secretariat of ICACT, and then you are allowed to submit the final CRF manuscripts in PDF file form, the full paper and the Copyright Transfer Agreement. Journal Paper Template, Copyright Form Template, BioAbstract Template,

Journal Submission Guide

All the Out-Standing ICACT conference papers have been invited to this "ICACT Transactions on the Advanced Communications Technology" Journal, and also welcome all the authors whose conference paper has been accepted by the ICACT Technical Program Committee, if you could extend new contents at least 30% more than pure content of your conference paper. Journal paper must be followed to ensure full compliance with the IEEE Journal Template Form attached on this page.

➢ How to submit your Journal paper and check the progress?

Step 1. Submit	Using the Submit button, submit your journal paper through ICACT Website, then you will get new paper ID of your journal, and send your journal Paper ID to the Secretariat@icact.org for the review and editorial processing. Once you got your Journal paper ID, never submit again! Using the Update button, you can change any information of journal paper related or upload new full journal paper.
Step 2. Confirm	Secretariat is supposed to confirm all the necessary conditions of your journal paper to make it ready to review. In case of promotion from the conference paper to Journal paper, send us all the .DOC(or Latex) files of your ICACT conference paper and journal paper to evaluate the difference of the pure contents in between at least 30% more to avoid the self replication violation under scrutiny. The pure content does not include any reference list, acknowledgement, Appendix and author biography information.
Step 3. Review	Upon completing the confirmation, it gets started the review process thru the Editor & Reviewer Guideline. Whenever you visit the Author Homepage, you can check the progress status of your paper there from start to end like this, " Confirm OK! -> Gets started the review process -> ...", in the Review Status column. Please don't miss it!

Volume. 8 Issue. 3

IEEE 802.15.4 Now and Then: Evolution of the LR-WPAN Standard

Alberto Gallegos Ramonet*, Taku Noguchi**
College of Information Science and Engineering
Ritsumeikan University
Shiga, Japan
ramonet@fc.ritsumei.ac.jp, noguchi@is.ritsumei.ac.jp

***Abstract*—For 15 years, the popular IEEE 802.15.4 standard has served as de facto standard for applications with low latency and small energy consumption requirements. During this time, it has evolved and dramatically extend its original purpose. With thousand of possible parameters and combinations, its objectives are not as clear as they were when it was first introduced. In this paper, we present a concise and chronological description of the standard highlighting the main features introduced by each one of its revisions as well as a notion of its usage. A compendium of this kind can be valuable to researchers working on implementations and improvements and to users seeking a general reference. This is relevant now more than ever because the standard must coexist with hundreds of other standards that are also constantly evolving. As presented in this document and despite its popularity and importance, there are very few capable IEEE 802.15.4 simulators and these are often outdated and incomplete. The aim of this paper is to provide a quick reference but also present the evolution of the standard and its future directions. Similarly, we hope that this study fosters the creation of new implementations, particularly new simulations modules.**

***Index Terms*—LR-WPAN, protocols, survey, WSN, simulations, Zigbee, IEEE 802.15.4, modulations**

I. Introduction

Networks in our homes, offices, and mobile devices are constantly evolving. Not all network-enabled devices are connected to the Internet nor do they need to be. For example, devices found in our homes such as electric doors, televisions, and air conditioning systems may benefit from sharing information between each other, but in most cases, using the internet to connect these appliances may not be a cost effective solution because of the unnecessary added complexity, communication overhead, and unwanted privacy concerns. In such cases, internet independent networks are a preferred choice. Independent networks used in Wireless Sensor Networks (WSN) are an example.

The IEEE 802.15.4 standard was released in 2003 [1] to describe such types of networks. WSN have been developed for strict power constraints in specialized applications with low latency or for applications characterized by disruptive connections. In this paper, we present a chronological description of the IEEE 802.15.4 standard known as Low-Rate Wireless Personal Area Networks (LR-WPAN). Furthermore, this study describes the MAC behaviors and the available options of its physical layers and also clarifies the often overlooked formation of semi-mesh networks and available simulations. Despite the popularity of the IEEE 802.15.4 standard, to our knowledge, no other authors have presented any similar evolutionary summary of the standard. The present work is an extension of our own observations first introduced in [2]. This document is relevant for multiple reasons. For instance, the standard includes an extensive collection of physical layer options and MAC layer improvements that are not available in all revisions. In some cases, drastic changes make certain implementations obsolete or incompatible. Moreover, official IEEE standard descriptions assume the knowledge of prior revisions, making such documents hard to navigate without having a general idea of the standard such as the one presented in this study. Consequently, new improvements and implementations can be convoluted and time consuming to develop. It is also worth noting that implementations and simulations of the standard are considerably behind the most recent revisions. For example, Zigbee, arguably the most popular commercial implementation of the IEEE 802.15.4 standard, only until recently (V3.0) supported the 2011 revision of the standard [3] despite the existence of amendments as late as 2019. Owing to these reasons, we believe that users and implementers will find the summary presented in this document relevant and useful. This paper is organized as follows: Section II describes the complete evolution of the IEEE 802.15.4 standard, highlighting differences between each revision. Section III presents a brief description of some of the most popular simulation and physical implementations, followed by our conclusions. Finally, a complete IEEE 802.15.4 PHY evolution Table can be found in the Appendix. The Table summarize all datarates and modulations of the standard to date (2019).

Manuscript received Dec 18, 2018. This work was in part supported by the JSPS KAKENHI Grant Number 19K11955, and a follow-up of the invited journal to the accepted & presented paper of the 21th International Conference on Advanced Communication Technology (ICACT2019).

Alberto Gallegos Ramonet, is an Assistant Professor at College of Information Science and Engineering, Ritsumeikan University, Shiga prefecture, 1-1-1 Noji-Higashi, Kusatsu, CO 525-8577 Japan (Corresponding author e-mail: ramonet@fc.ritsumei.ac.jp).

Taku Noguchi, is a Professor at College of Information Science and Engineering, Ritsumeikan University, Shiga prefecture, 1-1-1 Noji-Higashi, Kusatsu, CO 525-8577 Japan (e-mail: noguchi@is.ritsumei.ac.jp).

II. Evolution of the IEEE 802.15.4 Std.

A. IEEE 802.15.4 (2003)

Initially released in 2003, the IEEE 802.15.4 standard [1] defines the interconnection of LR-WPAN devices. It uses the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) to access the medium and support star and peer-to-peer topologies. Its architecture layout can be described in terms of blocks based on the open systems interconnection (OSI) seven-layer model in which each block (also called layer) has a specific task and provides services to upper blocks. The Physical layer (PHY) or layer 1, contains the radio frequency (RF) transceiver with a low-level control mechanism. The 2003 standard defines two PHYs: a *2450 MHz band* PHY operating with a Optional Offset Quadrature Phase-Shift Keying (O-QPSK) modulation and a maximum data rate over-the-air of 250 kb/s. The standard also describes the less commonly used *915/868 Mhz band* PHY with a Binary Phase-Shift Keying (BPSK) modulation and data rates of 40 kb/s and 20 kb/s, respectively. Both of these PHY use a direct sequence spread spectrum (DSSS). The MAC layer (Media Access Control or layer 2) provides access to the physical channel. Although the standard primarily consists of these two layers, the standard also describes an additional Logical Link Control (LLC) and a Service Specific Convergence Sublayer (SSCS) between the MAC layer and the next layer to facilitate communication. The implementation details of the upper layers are beyond the scope of the standard. Transmission of data can be performed with or without the help of beacon messages. In a beacon-enabled Personal Area Network (PAN), a single Full Functional Device (FFD) acts as a PAN coordinator while the remaining devices are either FFD or Reduced Functional Devices (RFD). Different from a beacon-enabled PAN, in a non-beacon enabled PAN, devices compete for the medium at all times.

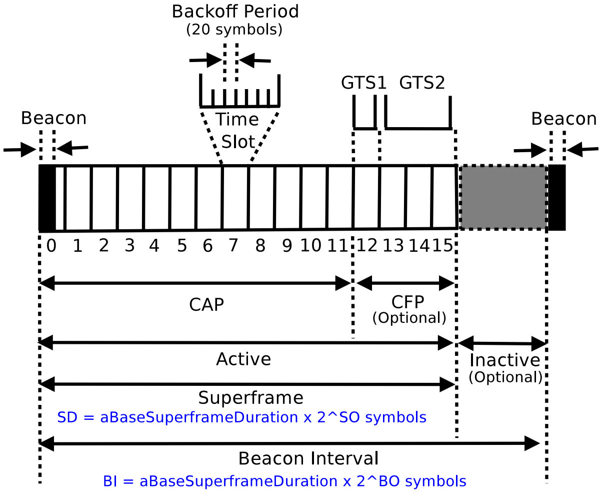


Fig. 1: Beacon-enabled mode superframe description.

In a beacon-enabled PAN, the PAN coordinator transmits in intervals beacons containing a *superframe* structure that defines an active period of time between beacons. The superframe is used to realize synchronized communication between the PAN devices. Figure 1 summarizes the structure of a superframe. A superframe is formed by 16 time slots in which a beacon is always sent during the first time slot. Similarly, each of these time slots consist of multiple *backoff periods* formed by *symbols*. A symbol is a representation of time in bits. For example, in the IEEE 802.15.4 standard that uses a O-QPSK modulation, 1 symbol is equivalent to 4 bits (0.016 ms in a 250-kbps connection). A Beacon Interval (BI) is defined by $aBaseSuperframeDuration \times 2^{BO}$ symbols. The Beacon Order (BO) is a user defined integer between 0 and 14 and $aBaseSuperframeDuration$ is a constant equal to 960 symbols. The BI includes both the active and inactive periods of time. The inactive period is optional with no transmissions, and the radio transceiver can be turned off to preserve energy. The active portion depends on the user defined variable Superframe Order (SO) and its length is described by the Superframe Duration (SD). The SD is equal to $aBaseSuperframeDuration \times 2^{SO}$ symbols for $0 \leq SO \leq BO \leq 14$. The active portion is further divided into a Contention Access Period (CAP) and Contention Free Period (CFP). In the CAP, devices contend for the transmission of data using a slotted version of the CSMA/CA algorithm. Time slots are formed by multiple *backoff periods* (1 backoff period is equivalent to 20 symbols). Operations within the CAP always occur on the boundary of a backoff period. The CFP is an optional part of the active period but if it is used, it must always be located at the end of the active period. The CFP is divided into Guaranteed Time Slots (GTS), which are assigned to specific devices for transmission without contention. A maximum of 7 GTS can be assigned. Their length directly depends on the maximum size of the CFP and the total number of GTS assigned.

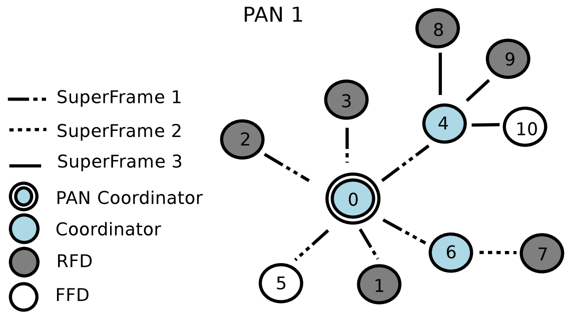


Fig. 2: IEEE 802.15.4 Semi-mesh topology in single PAN.

One aspect often overlooked by official IEEE 802.15.4 standard documents and researchers is the beacon-enabled function in semi-mesh topologies (full-mesh or mesh is only achievable by implementation on higher layers). While the standard states that this configuration is possible, little to no details are provided on the means to achieve this in multiple revisions. Figure 2 presents an example of the ways of achieving a semi-mesh topology. While only one PAN coordinator exists in a star topology PAN, it is possible to have extra coordinators to create a semi-mesh network (tree topology). PAN coordinators differ from coordinators in the sense that only PAN coordinators can initialize the network (association process) and give commands to other coordinators for administering the network. Each coordinator transmits its own beacons that

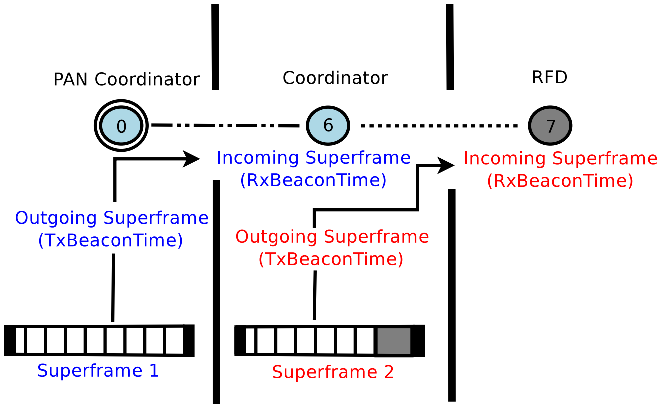

PAN Coordinator
Coordinator
RFD
0
6
7
Incoming Superframe (RxBeaconTime)
Incoming Superframe (RxBeaconTime)
Outgoing Superframe (TxBeaconTime)
Outgoing Superframe (TxBeaconTime)
Superframe 1
Superframe 2

Fig. 3: Outgoing and Incoming superframe relationship in a semi-mesh Network.

contain the information of its superframe. The transmitted superframe helps synchronize data transmissions between a coordinator and its associated devices. In a semi-mesh topology, a PAN coordinator transmits a superframe to its associated devices, but also, one or more of these devices can act as coordinators and therefore, transmit another superframe to its own associated devices. The transmitted superframe is known as the outgoing superframe and the received superframe is known as incoming superframe. In Figure 3, it is possible to observe this superframe relationship for one segment of the semi-mesh network previously presented in Figure 2. When the coordinator 6 wishes to transmit data to its PAN coordinator 0, the coordinator 6 uses the incoming superframe information (superframe 1). Similarly, if the coordinator 6 wishes to transmit data to its associated device node 7, it will use the outgoing superframe information that originated from itself (superframe 2). An incoming superframe uses the beacon reception time from its coordinator (RxBeaconTime) as a reference to the beginning of the superframe. An outgoing superframe uses its beacon transmission time (TxBeaconTime) as a reference to the beginning of the superframe.

B. IEEE 802.15.4 (2006)

The 2006 revision [4] was the first revision after the standard was introduced in 2003. In this revision, a field in the Frame Control Field (FCF) of the MAC Header was added to easily verify the version in use. The biggest changes in this revision are in the physical layer. The 2003 original 868/915 MHz bands employed a BPSK modulation. Optionally, an Amplitude Shift Keying (ASK) modulation on the 868/915 MHz bands can be used in this revision. This modulation effectively increases the offered data rate to 250 kb/s for both bands. The same data rate could only be achieved on the 2450 MHz band in the 2003 revision. In addition to the 868/915 MHz bands BPSK and ASK modulations, an O-QPSK modulation was added. This modulation offers an increased data rate of 100 kb/s and 250 kb/s, respectively, when compared to the original BPSK modulation. O-QPSK modulation was only possible on the 2450 MHz band in the 2003 revision. As for MAC layer enhancements, the 2006 revision enables specification beacons start times via a parameter in the MAC layer primitives. Pre-establishing the start time helps reduce beacon collisions among PAN coordinators.

C. IEEE 802.15.4a (2007) - Amendment 1

IEEE 802.15.4a [5] is the first amendment to the 2006 revision. It introduces two new PHYs: the Ultra-wide Band (UWB) and the Chirp Spread Spectrum (CSS). UWB operates at frequencies of 3 GHz, 5 GHz, 6 GHz to 10 GHz, and less than 1 GHz (16 channels). UWB has a maximum over-the-air data rate of 851 kb/s with optional data rates of 110 kb/s, 6.81 Mb/s, and 27.24 Mb/s using a combined modulation of Burst Position Modulation (BPM) and BPSK. On the other hand, CSS operates in the PHY 2450 MHz with supports for data rates of 1000 kb/s or 250 kb/s. The UWB enables the use of precision ranging (calculation of the distance between two devices) using the Two-Way Ranging (TWR) protocol that enables ranging calculation without a common time reference.

D. IEEE 802.15.4c (2009) - Amendment 2

The second amendment [6] to the 2006 revision adds two extensions to the physical layer: One 780 MHz PHY with the O-QPSK modulation and another 780MHz PHY with the new modulation M-ary Phase Shift Keying (MPSK). Both these additions are meant to be used in China and have a maximum data rate of 250 kb/s, regardless of the modulation used.

E. IEEE 802.15.4d (2009) - Amendment 3

Similar to 2nd, the 3rd amendment to the 2006 revision [7] adds extensions to the physical layer exclusively for Japan. These extensions include two additional PHY: a PHY in the 950 MHz band with a Gaussian Frequency-Shift Keying (GFSK) modulation with a maximum data rate of 100 kb/s and a PHY in the 950 MHz band using the BPSK modulation with a data rate of 20 kb/s.

F. IEEE 802.15.4 (2011)

The 2011 revision [8] compiles all changes made in the last 3 amendments after the 2006 revision into a single document. In this revision, the standard dropped the concept of Service Specific Convergence Sublayer (SSCS) and instead exclusively focuses on PHY and MAC layer topics. Because of the lack of a flexible MAC layer, the 2011 revision gave birth to numerous alternative MAC layer proposals that satisfy the requirements of different types of applications. In time, the standard addressed these concerns and officially introduced variants to the MAC layers in the form of *MAC behaviors* in subsequent amendments.

G. IEEE 802.15.4e (2012) - Amendment 1

While most amendments prior to this one focus on PHY layer additions, IEEE 802.15.4e [9] proposed significant changes to the MAC layer. These changes impacted the standard in 2 ways. First, it relegated the previous MAC layer to an all-purpose legacy status. Second, it reworked the MAC layer to a modular and specialized design in the form of

MAC behaviors. These MAC behaviors introduce a level of flexibility never present in the previous versions and, therefore, include a point of interest often surveyed and evaluated by researchers [10]. IEEE 802.15.4e describe 5 MAC behaviors:

RFID. The standard specifies the MAC behavior called BLINK, which is a specific kind of Radio Frequency Identification (RFID) [11]. RFID BLINK transmits encrypted data and is well suited for applications that involve sensitive information, which is the reason for its wide use in contactless credit card transactions and transportation systems worldwide. Devices connecting with RFID do not require prior association or acknowledgement.

AMCA. The Asynchronous Multichannel Adaptation MAC behavior is designed to work in environments with low channel quality because of noise or the presence of a large number of devices in a non-beacon enabled network. These problems can cause link asymmetry, which leads to a rapid degradation in communication. To combat this, during an active scan, AMCA tests the link quality on all available channels through requests made by the coordinator. This way, AMCA selects the channel with the highest link quality for either listening or transmitting at any given time.

DSME. The Deterministic Synchronous Multichannel Extension MAC behavior is targeted at applications that require high levels of reliability or deterministic latency. Examples include applications in industrial automation in which the loss of data represents a serious problem and applications in health monitoring where a guaranteed timely response is necessary. Simultaneously, DSME can also handle densely populated networks such as sensor networks. Similar to the beacon-enabled mode in the legacy MAC, synchronized transmissions are performed using *superframes* structures, but these superframes are contained in *multiframes* structures. DSME multi-superframe structures are described in Figure 4. Like before, a superframe is formed by a CAP and a CFP. In DSME, a single channel is used for the association process, which involves the transmission of Enhanced Beacons (EB) and transmissions during the CAP. The EB is a new addition to the standard and is composed of Information Elements (IE). IE are introduced for the first time in this amendment but are also used in other standards such as the IEEE 802.11. IE enables a more flexible use of the fields because they possess variable sizes, greatly extending the functionality of the frame that uses them. Different from the legacy MAC beacon-enabled, the CFP in DSM is capable of allocating up to 7 GTS for each available channel (16 channels). Alternatively, the slots can be assigned to perform Group Acknowledgment (GACK). With a GACK, it is possible to combine several acknowledgments to be sent to all devices communicating within the same superframe. This feature helps reduce latency and energy consumption.

Another unique feature of DSME is CAP reduction. Except for the first superframe CAP in the multi-frame, DSME can completely eliminate subsequent CAPs in the multi-frame and use the time gained to effectively increase the time for exclusive transmissions in CFP operations. DSME Beacon Interval (BI) is equal to $aBaseSuperframeDuration$ x 2^{BO} symbols where $aBaseSuperframeDuration$ is equal to 960 symbols and the Beacon Order (BO) is an integer between 0 and 14. The superframe duration (SD) is equivalent to $aBaseSuperframeDuration$ x 2^{SO} symbols, where SO is the superframe order and is related to the BO in $0 \leq SO \leq BO \leq 14$. Likewise, the Multi-superframe Duration (MD) is the result of $aBaseSuperframeDuration$ x 2^{MO} symbols where MO is the Multi-superframe Order and relates to both SO and BO in $0 \leq SO \leq MO \leq BO \leq 14$. To overcome interference as a result of noise present in a given channel, DSMA can check the link quality and use *channel adaptation* to switch a GTS (assigned to a specific device) to a different channel in a consecutive time slot. On the other hand, *channel hopping*, a well-known technique, can be used to set a predefined sequence to hop between channels during the whole frame transmission.

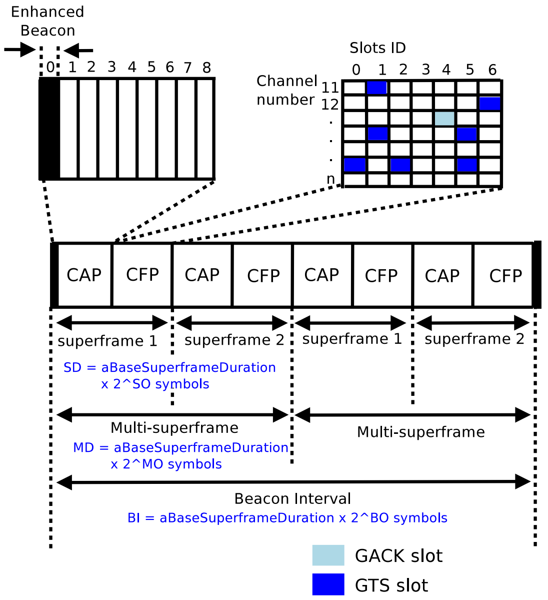


Fig. 4: DSME multi-superframe structure.

LLDN. The Low Latency Deterministic Networks MAC behavior was specifically designed for factory automation or implementations with similar requirements and limitations. LLDN is exclusive used in centralized networks (star topology) that require latencies as low as 10 ms for more than 100 devices connected to a single coordinator. Examples of LLDN applications include, but are not limited to robots, airport logistics, conveyors, automatic packing, cargo, etc.

In LLDN there can be two types of devices; devices that can only send data to the coordinator (uplink capable) or devices that can do both, send and receive data from the coordinator (uplink and downlink capable). LLDN has a *superframe* structure in which the first time slot is assigned to the beacon and the remaining slots of equal size are assigned to specific devices in the network. Multiple devices can be assigned to a single slot and they contend for the medium using CSMA/CA. In LLDN, superframe time slots have a specific order and purpose: a) The *beacon timeslot* which is always present. b) The *management timeslots*: *downlink* and *uplink* timeslots. The existence of management slots is optional and depends on whether or not the *macLLDNmgmtTS* flag is set

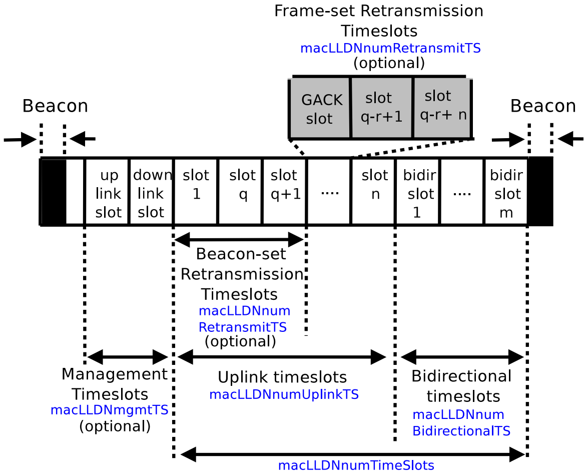


Fig. 5: LLDN superframe structure.

true. c) The *uplink timeslots* are used for transmissions from the devices to the coordinator. In addition, the first uplink slots can be used for re-transmissions if specified by the Group Acknowledgment (GACK) field in the beacon. Alternatively, re-transmissions can also be set using an LL-Acknowledgment frame (command frame) sent in the *bidirectional timeslots*. d) *Bidirectional timeslots* are used for multi-link communication between the coordinator and its devices. The slot size and number of slots for each usage are indicated by the *macLLDN* attributes, as shown in Figure 5.

TSCH. The Time Slotted Channel Hopping MAC behavior was created for robustness. TSCH applications include the oil and gas industry, chemical and pharmaceutical production, or applications prone to collisions caused by the saturation of the network. TSCH considers a deterministic response as the most important aspect of communication. Different to DSME, TSCH support semi-mesh and star topologies. In TSCH, *superframes* are replaced with *slotframes*. Slotframes repeat cyclically and are formed by a sequence of *timeslots*. Each timeslot has an incremental Absolute Slot Number (ASN) that indicates the total number timeslots elapsed since the beginning of the network. Transmissions inside these timeslots can occur with or without contention. In addition, in TSCH, it is possible to use concurrent slotframes, each with independent timeslot configurations. However, all slotframes are aligned to the same timeslot boundaries. Unlike the channel diversity used in DSME, TSCH relies on a channel hopping mechanism to achieve communication. The frequency f used in a transmission between two nodes is defined by $f = F[(ASN + channelOffset)\%NChannels]$ where *channel Offset* is an integer between 0 and 15, *NChannels* is the hopping sequence length, and F denotes a lookup table. In this manner, a different frequency is obtained for the same link in different time slots. TSCH behavior is summarized in Figure 6.

H. IEEE 802.15.4f (2012) - Amendment 2

The 2nd amendment [12] to the 2011 revision has two new PHY. First, the Low-rate PRF Ultra-Wide Band (LRP UWB) optimized for low complexity RFID transmitters (tags) exhibits a level of interoperability only present with the UWB PHY in previous revisions. LRP UWB offers 3 modes: a) *Base mode* with an On-Off-Keying (OOK) modulation and a bit rate of 1000 kb/s. b) *Extended mode* with an OOK modulation and a bit rate of 250 kb/s. c) *Long-range mode* with a Manchester Pulse Position Modulation (PPM) and a maximum bit rate of 31.25 kb/s.

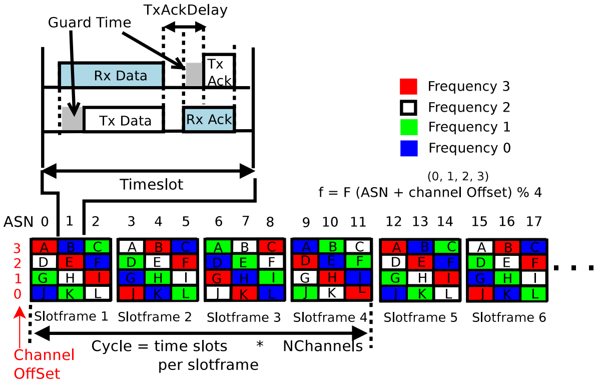


Fig. 6: TSCH frequency hopping mechanism.

The second PHY is a 2450 MHz band PHY with a Minimum Shift Keying (MSK) modulation and a maximum bit rate of 250 kb/s for RFID applications. The 2450 MHz band is the Industrial, Scientific and Medical (ISM) band and therefore, multiple standards operate on this band (e.g. Wifi, Lr-Wpan, etc). Moreover, small unused gaps in the spectrum on the edges of these frequencies tend to exist. MSK 2450MHz PHY takes advantage of those spaces and is capable of using up to 42 possible narrowband channels that fall on these unused gaps, gracefully coexisting with existing devices using the same band. Alternatively, MSK can operate on the much less saturated 433 MHz band with bit rates of 31.25, 100 or 250 kb/s.

I. IEEE 802.15.4g (2012) - Amendment 3

IEEE 802.15.4g [13], known as the Smart Utility Networks (SUN) standard, was created to be used in the emerging Smart Grids (SG). SGs are electrical grids capable of bidirectional energy flow and communication [14]. SUN PHYs are often used in smart metering applications with long-range, low-power requirements. This amendment introduces three PHY with multiple data rates to choose from. The PHY names are described by its modulation names: a) Frequency Shift Keying (FSK). b)Offset Quadrature Phase-Shift Keying (O-QPSK), which extends the frequency ranges of the 2011 modulation O-QPSK. c) The Orthogonal Frequency Division Multiplexing (OFDM), which uses DSSS and MDSSS. All of these PHY are designed to be used with Multiple data rates and in multiple regions (MR). However, smart-metering applications tend to use the internationally agreed *920 Mhz band* (frequencies 902 Mhz to 928Mhz) with a 2FSK and 50 kbps as the most common modulation and data rate choice [15]. While FSK and O-QPSK are well known modulations techniques used in multiple standards, OFDM is generally reserved for more specialized systems, and it was until 2012 that was adapted to the IEEE 802.15.4 standard to be used on low powered devices. OFDM purpose is to offer higher data rates over longer distances and combat multi-path fading. Multi-path fading occurs when transmitted signals bouncing off obstacles take different paths and arrive to the receiver at slightly different times. As a result, the overall received signal becomes the sum of these reflections which can be interpreted by the receiver as interference [16]. To combat multi-path fading, OFDM divides a frequency band into multiple sets of frequencies called subcarriers. Subcarriers are far apart enough from each other to avoid interfering with one another. Each subcarrier is modulated according to a *Modulation and Coding Scheme* (MCS): BPSK, QPSK or 16-QAM. Additionally, subcarriers must be grouped in one of four different ways formally called *options*. In other words, the transmitted OFDM symbol is the result of the combination of multiple modulated subcarriers grouped by an option. Each one of these subcarries carries pieces of the transmitted information. With this technique OFDM can achieve data rates as high as a high order modulation. A complete list of OFDM data rates according to the option and MCS can be found on Table III. Furthermore, OFDM can recover lost data using *Forward Error Correction* (FEC) or reducing the amount of lost data with *Frequency repetition* on some MCS (More than two subcarriers transmit the same information as a redundancy measure) [17].

Vendors often offer a SUN PHY paired with a portion of the IEEE 802.15.4e for its MAC implementation (TSCH behavior).

Some of the SUN PHY frequencies established in this amendment have been updated or discarded in later amendments.

J. IEEE 802.15.4j (2013) - Amendment 4

This amendment [18] introduces a single PHY for the 2380 MHz band with a maximum bit-rate of 250 kb/s. Its use is restricted to transmission data (no voice) in devices for monitoring, diagnosing, and treating of patients. These devices must be compliant with the Federal Communications Commission (FCC) rules for Medical Body Area Networks (MBAN).

K. IEEE 802.15.4k (2013) - Amendment 5

This amendment added 2 more PHYs: a) A DSSS PHY with either BPSK or O-QPSK modulation schemes. b) A FSK PHY with 3 possible modulations; a Gaussian FSK (GFSK), Position-based FSK (P-FSK), and Position-based Gaussian FSK (P-GFSK). These PHY are designed for Low Energy, Critical Infrastructure Monitoring (LECIM) applications. Different to its IEEE 802.15.4 PHY counterparts, LECIM PHY are designed to operate with extremly low energy because they are required to last with the original battery supply for many years (in the order of 20 years or more). To achieve this, LECIM uses low data rates but favors long range operations. LECIM can use a wide range of low data rates using either BPSK or O-QPSK modulations (Table II). LECIM data rates are calculated using the Equation 1 [19, pp. 58-61].

$$DataRate = FEC * \frac{ModulationRate * ChipPerSymbol}{SpreadFactor} \tag{1}$$

In the Equation 1, BPSK modulation is used when $ChipPerSymbol = 1$ and O-QPSK modulation is used when $ChipPerSymbol = 2$. The Forward Error Correction (FEC) is equal to 0.5. With the combination of the available $ModulationRates$ and $SpreadFactors$ LECIM datarates can be obtained. For example, the lowest possible O-QPSK data rate with a $ModulationRate$ of 200 ksym/s and the largest $SpreadFactor$ of 32768 would be 3 b/s. Usage of particular data rates or restrictions of specific bands depend on local regulations. One of the main features introduced in the 802.15.4k MAC layer is the ability to use *priority channel access* (PCA). PCA enables the allocation of high-priority messages in the CAP period of the superframe structure. Experiments performed by Gebremedhin et al. [20] demonstrated that under some conditions, PCA messages can greatly improve the latency of emergency messages while slightly affecting the performance of normal messages.

L. IEEE 802.15.4m (2014) - Amendment 6

The IEEE 802.15.4m amendment [21] objective was to re-purpose the unused frequency space left by some TV channels in the VHF and UHF TV broadcast bands. Originally, some space occupied by some TV channels was left unused to prevent TV channels from interfering with one or in some cases TV channels were left unused to comply with local regulations. These empty spaces are known as TV White Spaces (TVWS) and its value depends on its wide availability, uniformity among regions and its potential for longer range communications. A 2.4 Ghz signal might travel several kilometers in the right conditions, but UHF (470 - 698 MHz) can travel for many miles. Such characteristics make it an attractive cost-effective solution to be use in rural areas. However, it is worth noting that in urban areas, the existing TVWS (i.e. 600 - 700 MHz) are increasingly becoming unavailable because of a high demand in cellular frequencies and other wireless services. The IEEE 802.15.4m TVWS PHY support multiple data rates in bands ranging from 54 MHz to 862 MHz, aided by 3 modulation schemes: FSK (2FSK and 4FSK), OFDM (BPSK, QPSK, 16-QAM), and NB-OFDM (BPSK,QAM,16-QAM,64-QAM). The availability of TVWS channels change from region to region as well as channel usage and the TV channel length. In the US, Canada, Japan and other countries that comply with the FCC (Federal Communications Commission) rules, the TV channels length is 6 MHz while in UK and Europe channels length is 8 MHz. The US use both, VHF as well as UHF TV broadcast bands (37 possible channels of 6 Mhz), however, most countries use TVWS in the UHF TV band exclusively, each one with their particular channelization and regional rules. For example, UK and Europe both use the UHF band from 470 to 790 MHz (40 possible TV channels of 8 Mhz) while Japan [22] uses the UHF band from 470 to 710 MHz (40 possible TV channels of 6 Mhz). The coexistence of IEEE 802.15.4m with other standards using TVWS such as IEEE 802.11af and 802.22b have been explored in [23]. IEEE 802.15.4m MAC layer supports a superframe variant called TMCTP (TVWS Multichannel Cluster Tree PAN). The TMCTP superframe (Figure 7) is a modified version of the superframe first introduced in the IEEE 802.15.4-2003 [1] (Section II-A). The main difference to the original superframe is that this version includes a Beacon Only Period (BOP) in the last part of the superframe Active Period. BOPs are subdivided into Dedicated Beacon Slots (DBS) one of which is allocated to each PAN coordinator connected to a Super PAN Coordinator (SPC). DBSs are formed by a different number of Base Slots as required for each PAN. Using the BOP, a SPC maintain exclusive communication with other PAN coordinators to keep synchronization among multiple PANs (Figure 8).

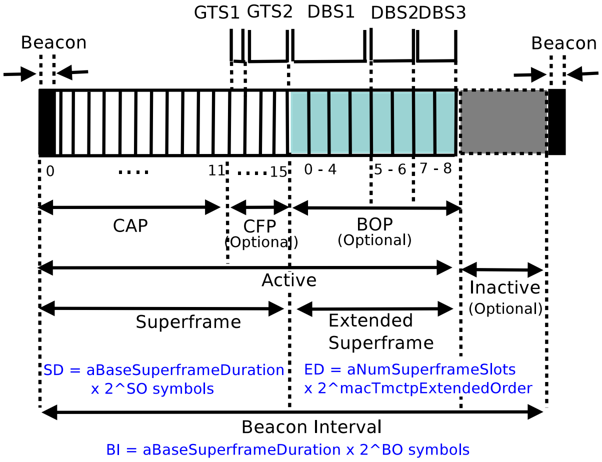


Fig. 7: TMCTP Superframe.

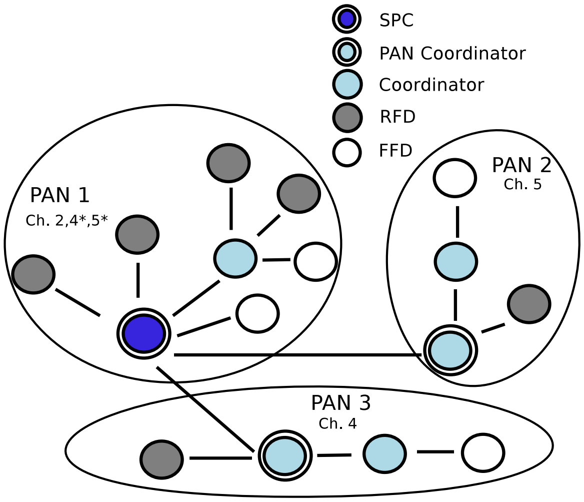


Fig. 8: TVWS Multichannel Cluster Tree PAN (TMCTP).

M. IEEE 802.15.4p (2014) - Amendment 7

This amendment [24] addressed the need for a communication standard in Rail Communications Control (RCC) systems. Previous to this standard, there were no IEEE 802 standards specifically designed for vehicles capable of moving up to 600 km/h. IEEE 802.15.4p devices are deployed on locomotives, base stations, railyard locations and can be useful to vehicular networks in general. This standard enable data rates of up to 1 Mbit/s over frequencies in the narrow bands VHF, UHF, and SHF bands (161, 216, 217, 220, 450, 770, 896, 915, 928, 2450, 4965, 5800 MHz) operating in contiguous and non-contiguous channel bandwidths as narrow as 12.5 kHz and as wide as 2Mhz [25, pp. 386]. The standard includes multiple modulation technique options: GMSK, QPSK, and DPSK among others. A full list of the frequencies and modulations introduced for this amendment can be found in Table I. Railroads and transit authorities around the globe often use proprietary protocols and communication systems, the adoption of the IEEE 802.15.4p standard allows these authorities to overcome these systems interoperability challenges plan for flexible and scalable future railroad communication networks.

N. IEEE 802.15.4 (2015)

IEEE 802.15.4-2015 [25] is the third revision of the standard. As its predecessors, this combines all the PHYs additions and MAC enhancements since the 2011 revision in a single document. Additional corrections to the document are editorial in nature.

O. IEEE 802.15.4n (2016) - Amendment 1

The first amendment [26] to the 2016 revision present another PHY alternative for the transmission of medical information in China. The China Medical Band (CMB) defines the 174-216 MHz, 407-425 MHz, and 608-630 MHz bands. The standard restricts the use of these bands for voice applications.

P. IEEE 802.15.4q (2016) - Amendment 2

IEEE 802.15.4q [27] introduced two PHY for 2.4 GHz and multiple sub-gigahertz bands with data rates up to 1 Mb/s. These PHYs were designed for ultra low-cost (low complexity) and ultra-low power applications. To achieve this, the standard used two new modulations: the Rate Switch Gaussian Frequency Shift Keying (RS-GFSK) and the Ternary Amplitude Shift Keying (TASK). TASK use a ternary sequence spreading followed by an ASK modulation.

IEEE 802.15.4q RS-GFSK modulation uses a simple but ingenious way to combine 2GFSK and 4GFSK during the transmission of the Physical Protocol Data Unit (PPDU) also known as frame. RS-GFSK main characteristic is that the combined resulting modulation bandwidth is close to identical. RS-GFSK switching rate mode is optional and must use 2GFSK modulation when disabled. However, when enable (indicated by the *Rate Switch* bit in the PHR) the frame's synchronization Header (SHR) and PHY header (PHR) shall be transmitted using 2GFSK while the PHY Service Data Unit (PSDU) shall be transmitted using 4GFSK with the same symbol rate used by the 2GFSK transmission of the SHR and PHR (Figure 9). Nodes communicating with sufficient link budget can use Rate Switch to reduce the active time for transmitting and receiving and therefore, save energy. The highest data rate specified in in RS-GFSK modulation is 2.5 times higher than the available SUN FSK PHYs with the added advantage of lower interference due to the use of the Gaussian filter, resulting in fewer collisions and retransmissions. Furthermore, IEEE 802.15.4q utilize shorter preambles. Therefore, is more energy efficient than standards IEEE 802.15.4f, 802.15.4g and 802.15.4k.

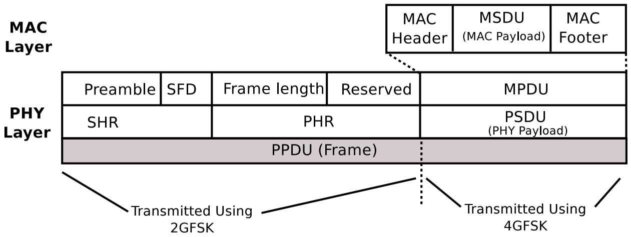


Fig. 9: PPDU (frame) to be transmitted using RS-GFSK with rate switching option enabled.

RS-GFSK provided options to interoperate with existing SUN FSK PHYs. Consequently, smart metering, smart irrigation, and home network applications benefit from these PHYs.

Q. IEEE 802.15.4u (2016) - Amendment 3

The third amendment to the 2015 revision [28] brought the 866 Mhz PHY to India. This PHY defined the 865-867 MHz band with an option for multiple bit-rates to choose from and 3 possible modulations: SUN FSK, OFDM, O-QPSK.

R. IEEE 802.15.4t (2017) - Amendment 4

A new PHY was introduced in this amendment [29], which was designed to operate on devices that require a short burst of information at high speeds (up to 2 Mb/s) followed by long sleep periods, contributing to extended battery life. This amendment uses the same 2400-483.5 MHz frequencies occupied by the O-QPSK PHY in place of MSK modulation.

S. IEEE 802.15.4v (2017) - Amendment 5

This amendment [30] changed multiple SUN PHY frequency ranges, including their channel ranges. The changes conceded the use of the 870-876 MHz and the 915-921 Mhz in Europe, the 902-928 MHz in Mexico, the 902-907.5 in Brazil and the 915-928 MHz in Australia, Brazil, and New Zealand. In addition, frequency range changes are made to the LECIM and TVWS PHYs.

T. IEEE 802.15.4s (2018) - Amendment 6

In this amendment [31], several MAC layer primitives and commands were added as part of the Spectrum Resource Measurements (SRM) toolkit. These changes are the most significant additions to the MAC layer since 802.15.4e-2012. SRM enables the measure, transmission, and request of information concerning the state of the channel. The MAC layer can report this information to higher layers for its usage. For example, SRM information can be used to create more precise and cost effective routing protocols in upper layers. Some of the SRM introduced features include:

- *Failed Transmissions measurement.* It estimates the propagation quality of specific links as part of the channel selection algorithm.
- *Deferred Transmissions measurement.* It helps to determine the level of congestion in the channel caused by other coexisting networks.
- *Retry Histogram.* It provides a histogram with the number of retries from a single transmission during a determinate space of time.
- *Noise Histogram.* Reports the noise power of non-IEEE 802.15 devices in a specific channel during a specific period of time.
- *Channel Usage.* Display the total Channel time used during a sequence of Rx and Tx frames during a period of time.
- *Received Signal Strength Indicator (RSSI)* Measurement of the Radio Frequency power received. While RSSI is a common management function in other standards, it was first introduced to the IEEE 802.15.4 in this amendment.
- *Energy Detection (ED).* The ability of the receiver to detect energy level present on the current channel from other transceivers or ambient energy.

U. IEEE 802.15.4x (2019) - Amendment 7

IEEE 802.15.4x [32] is the last amendment to date. Similar to the IEEE 802.15.4v-2017 standard, this amendment further extends the SUN PHYs (first introduced in IEEE 802.15.4g-2012). New 2FSK modulation data rates to be use in narrow bands are added as well as the extension of the SUN OFDM PHY with a data rates up to 2.4 Mb/s and SUN O-QPSK with additional data rate options in multiple regions.

III. IEEE 802.15.4 IMPLEMENTATIONS

At times, the accuracy of simulation results can be questionable; however, without the simulation results, large scale and costly experiments cannot be performed. The IEEE 802.15.4 is a popular protocol with multiple revisions. Despite its popularity, new revisions are gradually being adopted. By far, the 2003 and 2006 revisions are the most implemented. 2012 revisions or later, brought highly specialized PHYs and MAC behaviors limited to specific industries and applications. Their implementation in simulations is somehow rare in comparison to the legacy standard. Examples of popular IEEE 802.15.4 implementations include the following:

The Ns-2 WPAN module [33] is among the first simulations of the standard. Its latest version (2.35) completely supports the IEEE 802.15.4-2003 protocol, and is to date, one of the most complete implementations of the standard with beacon and non-beacon support for semi-mesh and star topologies (No support for inactive periods). Unfortunately, it exhibits certain disadvantages that were inherited from ns-2; lack of documentation and coding standards, unrealistic packet formats, unnecessary overhead, and lack of maintenance. Its modules are coded in C++ while scenarios require OTcl scripting language.

Castalia (v3.3) [34] is an OMNET++ based simulator. In addition to the basic 802.15.4-2006 MAC standard, Castalia supports 3 more MAC layers: TunableMac, TMAC, and IEEE 802.15.6. Castalia only supports beacon-enabled modes in star topologies with the optional GTS (No support for non-beacon, Indirect-transfers or semi-mesh topology). Castalia supports PHYs modulations QPSK, BPSK, PSK, and FSK, unlike the 2006 revision of the standard. C++ and NED languages are used in OMNET++ modules.

Ns-3 [35] is a simulator with an active community that develops new modules. Some of these modules even include emulation and hardware integration support. The latest version of the Ns-3 (V3.29) LR-WPAN module supports a full PHY IEEE 802-15.4-2006 set with a non-beacon mode MAC for a star topology PAN (No association or beacon-enabled mode MAC options). The module exhibits promising performance; however, the module still has several limitations compared to other simulators. Its code base is C++ and it supports Python bindings.

The OPNET simulator provides an IEEE 802.15.4-2003 model [36] that supports beacon-enabled modes in star typologies (No support for association, Non beacon-enabled mode or semi-mesh topology). Similar to OMNET++, OPNET provides a robust GUI. Modules are build using Proto-C, C, or C++. A major drawback of OPNET is the requirement of a license.

OpenZB [37] is an open source, real hardware implementation of the IEEE 802.15.4-2003 with beacon-enabled modes for star and mesh topologies on CrossBow MICAz and TelosB motes. TinyOs, as its name implies is an operative system specifically designed to create easy modules for microcontrollers. Some of the most popular modules are created for microcontrollers commonly used in Wireless Sensor Networks (WSN). OpenZB is completely programmed using the nesC language (as required by TinyOS). OpenZB is not the only implementation of the IEEE 802.15.4 on TinyOS. In fact, other authors have documented [38], [39] their experiences implementing parts of the IEEE 802.15.4 standard for TinyOS.

Zigbee [40], used by the industry and hobbyist alike is arguably the most popular implementation of the IEEE 802.15.4 standard. A common misconception is that IEEE 802.15.4 is Zigbee. Zigbee includes IEEE 802.15.4 PHY and some of its MAC layers but it also includes upper layers (routing, security, applications, etc). In other words, Zigbee is a full-stack solution. Zigbee is developed by the Zigbee Alliance which is formed by various groups (manufacturers, users, etc) with the objective of solving IEEE 802.15.4 interoperability problems and ensure that products from different vendors that use the Zigbee stack are compatible with one another. Its latest revision (Zigbee V3.0) includes a 2011 revision of the IEEE 802.15.4 standard. Additionally, the PHY IEEE 802.15.4g bundle with the IEEE 802.15.4e TSCH MAC behavior can be found in the Zigbee product formally named ”JupiterMesh”. Zigbee mayor drawback is that its a closed source solution and none of its conforming layers can be modified in any way.

IV. Conclusions

In this paper, we presented a complete and uptodate compendium of the IEEE 802.15.4 standard. The standard was initially envisioned for applications with low range and low energy consumption requirements. In recent years, the standard have evolved to handle an extensive range of application operating on multiple bands and modulations. While monitoring and medical were the most common implementations when the standard was first introduced, its focus have now turned to grid networks and smart metering applications in recent revisions. Vendors and users alike, however, have not be able to keep pace with the changes. Most of the standard introduced features are little known by most users. Likewise, simulations and hardware implementations of the standard are rarely complete and even popular simulators are significantly behind from the latest revisions of the standard. It is the wish of the authors that the current document help users to navigate these differences and better understanding each one of the standard specifications for any given situation. Future networks performance will depend on the standard choice and the ability of these standards to support smooth coexistence with other protocols. With, literally, thousands of possible combinations to choose from, network specialists will have to depend more on simulations and a deep understanding of the available standards.

Appendix

Table I list all IEEE 802.15.4 PHY with their modulations and data rates, sorted by year of introduction. Channeling specifications and regional restrictions are not specified in this Table.

Amendments v-2007 and x-2009 are extensions on the IEEE 802.15.4g-2012 and for this reason, in Table I are included in the SUN PHYs differentiated by their font color.

Table II list all the LECIM data rates used for narrow bands while Table III list all possible data rate combinations for the OFDM modulation in the standard (IEEE 802.15.4x OFDM data rates additions are indicated with different font color).

In the Table I, IEEE 802.15.4q RS-GFSK modulation data rates are described in pairs (2GFSK, 4GFSK). For example, the band 901 can transmit its PPDU with modulation RS-GFSK (rate switch enabled) with either the data rate pair [4.8 (2GFSK), 9.6 (4FSK)] or the pair [9.6 (2GFSK), 19.2 (4GFSK)]. If the rate switch is not enabled only the 2GFSK data rate is used (see Section II-P).

TABLE I
IEEE 802.15.4 PHY evolution.

PHY Band Name	**Frequencies (MHz)**	**Modulation - Spread Spectrum**	**Bit-Rate (kb/s)**	**Symbol Rate (ksym/s)**
IEEE 802.15.4-2003 2450 (World Wide)	2400-2483.5	O-QPSK *DSSS	250	62.5
915 (US)	902-928	BPSK *DSSS	40	40
868 (EUR)	868-868.6		20	20
IEEE 802.15.4-2006	902-928	ASK*PSS	250	50
915 (US)		O-QPSK*DSSS	250	62.5
868 (EUR)	868-868.6	ASK*PSS	250	12.5
		O-QPSK*DSSS	100	25
IEEE 802.15.4a-2007 2450	2400-2483.5	DQPSK → DQCSK *CSS	250 / 1000	166.667 / 166.667
UWB sub-Ghz	250-750		110/850	0.12/0.98(Mhz)
UWB low	3244-4742	BPM-BPSK	6810	7.80(Mhz)
UWB high	5944-10234		27240	15.60(Mhz)
IEEE 802.15.4c-2009	779-787	O-QPSK	250	62.5
780 (China)		MPSK	250	62.5
IEEE 802.15.4d-2009	950-956	2GFSK	100	100
950 (Japan)		BPSK *DSSS	20	20
IEEE 802.15.4f-2012				
433	433.05-434.79	MSK	31.25/100/250	31.25/100/250
2450	2400-2483		250	250
LRP UWB	6289.6-9185.6	PPM	31.25	31.25
		OOK	250/1000	250/1000
IEEE 802.15.4g-2012 **IEEE 802.15.4v-2017** **IEEE 802.15.4x-2019**				
SUN	169.400-169.475	2FSK	2.4 / 4.8	2.4/4.8
169 (EUR)		4FSK	9.6	4.8
450 (US)	450-470	2FSK	4.8	4.8
		4FSK	9.6	4.8
470 (China)	470-510	2FSK	10/20/50/100	10/2050/100
		~~4FSK~~ 2FSK	~~200~~ 150	~~100~~ 150
		O-QPSK	6.25-50	1.56-12.5
		OFDM(Opt. 4)	Table III	N/A
780 (China)	779-787	2FSK	10/20/50/100	10/20/50/100
		4FSK	200	100
		O-QPSK	31.25-500 6.25-50	7.8125-125 1.56-12.5
		OFDM	Table III	N/A
863 (EUR)	863-870	2FSK	10/20/50/100	10/20/50/100
		~~4FSK~~ 2FSK	~~200~~ 150	~~100~~ 150
		OFDM (Opt. 4)	Table III	N/A
867 (Singapore)	866-869	2FSK	10/20/50/100 150/200/300	10/20/50/100 150/200/300
		OFDM (Opt. 3,4)	Table III	N/A
		O-QPSK	6.25-50	1.56-12.5
870 (EUR)	870-876	2FSK	10/20 50/100/150	10/20 50/100/150
		OFDM (Opt. 4)	Table III	N/A
		O-QPSK	6.25-50	1.56-12.5
896 (US)	896-901	2FSK	10/20/40	10/20/40
901 (US)	901-902	2FSK	10/20/40	10/20/40

TABLE I a
(Continued) IEEE 802.15.4 PHY evolution.

PHY Band Name	**Frequencies (MHz)**	**Modulation - Spread Spectrum**	**Bit-Rate (kb/s)**	**Symbol Rate (ksym/s)**
915-a (Mexico/US)	902-928	2FSK	10/20 150/200/300	10/20 150/200/300
915-b (Brazil)	902-907.5	OFDM (Opt. 1-4)	Table III	N/A
	915-928	O-QPSK	31.25-500	7.8125-125
915-c (AU/NZ)	915-928		6.25-50	1.56-12.5
915-d (EUR)	915-921	2FSK	10/20	10/20
915-e (Philipines)	915-918		150/200/300	150/200/300
	902-907.5	OFDM (Opt. 3,4)(Opt. 1-4)	Table III	N/A
		O-QPSK	6.25-50	1.56-12.5
915 (US)	902-928	2FSK	10/20 50/100/200	10/20 50/100/200
917 (Korea)	917-923.5	O-QPSK	31.25-500 6.25-50	7.8125-125 1.56-12.5
		OFDM(Opt. 1-4)	Table III	N/A
919 (Malaysia)	919-923	2FSK	10/20 150/200/300	10/20 150/200/300
		OFDM (Opt. 1-4)	Table III	N/A
		O-QPSK	6.25-50	1.56-12.5
920 (Japan)	920-928	2FSK	50/100/200	50/100/200
		4FSK	400	200
		O-QPSK	6.25-50	1.5625-12.5
		OFDM	Table III	N/A
920-a (China)	920.5-924.5	2FSK	10/20 50/100/150	10/20 50/100/150
		OFDM (Opt.4)(Opt. 1-4)	Table III	N/A
920-b (H.K, Sing. Thailand,Vietnam)	920-925	O-QPSK	6.25-50	1.56-12.5
928 (US)	928-960	2FSK	10/20/40	10/20/40
950 (Japan)	950-958	2FSK	10/20 50/100/200	10/20 50/100/200
		4FSK	400	200
		O-QPSK	6.25-50	1.5625-12.5
		OFDM	Table III	N/A
1427 (US)	1427-1518	2FSK	10/20/40	10/20/40
2450 (World Wide)	2400-2483	2FSK	50/150/200	50/150/200
		O-QPSK	31.25-500	7.8125-125
		OFDM	Table III	N/A
IEEE 802.15.4j-2013 2380	2360-2400	O-QPSK *DSSS	250	62.5
IEEE 802.15.4k-2013 **LECIM** 169	169.400-169.475	2FSK/P-FSK 2GFSK/P-GFSK	25/12.5	25/12.5
433	433.050-434.790	2FSK/P-FSK 2GFSK/P-GFSK	37.5/25/ 12.5	37.5/25/ 12.5
470	470-510	2FSK/P-FSK 2GFSK/P-GFSK	37.5/25/ 12.5	37.5/25/ 12.5
780	779-787			
863	863-870	BPSK/O-QPSK	Table II	-
915	902-928			
922	915-928			
917	917.1-963.5			
920	920-928			
921	921-928			
2450	2400-2483.5	BPSK/O-QPSK	Table II	-

TABLE I b
(Continued) IEEE 802.15.4 PHY evolution.

PHY Band Name	Frequencies (MHz)	Modulation - Spread Spectrum	Bit-Rate (kb/s)	Symbol Rate (ksym/s)
IEEE 802.15.4m-2014				
TVWS		2FSK	50/100/200/300	50/100/200/300
CH.2 (US/Canada)	54-60	4FSK	400	200
CH.5-6 (US/Canada)	76-88	OFDM (BPSK)	390.625/1562.5	N/A
CH.7-13 (US/Canada)	174-216	OFDM (QPSK)	781.250/3125	
CH.14-20 (US/Canada)	470-512	OFDM (16-QAM)	1562.5/6250	
CH.21-36 (US/Canada)	512-608	NB-OFDM (BPSK)	156/234	
CH.38-51 (US/Canada)	614-698	NB-OFDM (QAM)	312/468	
CH.21-60 (UK/Europe)	470-790	NB-OFDM (16-QAM)	624/936	
(others)	790-862	NB-OFDM (64-QAM)	936/1404/1638	
IEEE 802.15.4p-2014				
RCC		GMSK	9.6/19.2	9.6/19.2
161	160.170-161.580	C4FM	9.6/19.2/38.4	4.8/9.6/19.2
216	216-217	QPSK	16/32	8/16
217	217-220	Pi/4 DQPSK	16/32/36	8/16/18
220	220-222			
450	450-470			
770	769-775			
800	799-805			
806	806-821			
	851-866			
896	896-901			
	935-940			
915	902-928	GMSK	9.6/19.2	9.6/19.2
		C4FM	9.6/19.2/38.4	4.8/9.6/19.2
		QPSK	16/32	8/16
		Pi/4 DQPSK	16/32/36	8/16/18
		DPSK*DSSS	[24]	-
		BPSK*DSSS	40	40
928	928-960	GMSK	9.6/19.2	9.6/19.2
		C4FM	9.6/19.2/38.4	4.8/9.6/19.2
		QPSK	16/32	8/16
		Pi/4 DQPSK	16/32/36	8/16/18
2450	2400-2483.5	BPSK*DSSS	40	40
4965	4940-4990	DPSK*DSSS	[24]	-
		BPSK*DSSS	40	40
5800	5725-5850	DPSK*DSSS	[24]	-
		BPSK*DSSS	40	40
IEEE 802.15.4q-2016				
169	169.400-169.475	RS-GFSK	(4.8,9.6)	4.8
			(9.6,19.2)	9.6
433	433.050-434.790	RS-GFSK	(4.8,9.6)	4.8
			(9.6,19.2)	9.6
			(50,100)	50
		TASK	202.38/101.19 75.89/31.62	-
450	450-470	RS-GFSK	(4.8,9.6)	4.8
			(9.6,19.2)	9.6
			(50,100)	50
			(150,300)	150
			(500,1000)	500
			250	250
			1000	1000

TABLE I c
(Continued) IEEE 802.15.4 PHY evolution.

PHY Band Name	Frequencies (MHz)	Modulation - Spread Spectrum	Bit-Rate (kb/s)	Symbol Rate (ksym/s)
470	470-510	RS-GFSK	(9.6,19.2)	9.6
			(50,100)	50
			(150,300)	150
			(500,1000)	500
			250	250
			1000	1000
		TASK	202.38/101.19 75.89/31.62	-
780	779-787	RS-GFSK	(50,100)	50
			(150,300)	150
			(500,1000)	500
			250	250
		TASK	485.71/242.85 182.14/75.89	-
863	863-876	RS-FSK	(50,100)	50
			(150,300)	150
			(500,1000)	500
			1000	1000
			500	500
		TASK	485.71/242.85 182.14/75.89	-
896	896-901	RS-GFSK	(4.8,9.6)	4.8
			(9.6,19.2)	9.6
			(50,100)	50
901	901-902	RS-GFSK	(4.8,9.6)	9.6
			(9.6,19.2)	9.6
915	902-928	RS-GFSK	(50,100)	50
			(150,300)	150
			(500,1000)	500
			250	250
			1000	1000
		TASK	485.71/242.85 182.14/75.89	-
918	915-921	RS-GFSK		
917	917-923.5	RS-GFSK	(50,100)	50
			(150,300)	150
			250	250
928	928-960	RS-GFSK	(4.8,9.6)	4.8
			(9.6,19.2)	9.6
1427	1427-1518			
2450	2400-2483.5	RS-GFSK	(50,100)	50
			(150,300)	150
			(500,1000)	500
			250	250
			1000	1000
		TASK	809.5/404.76 303.57/126.48	-
IEEE 802.15.4n-2016				
195 (China)	174-216	2GFSK	50/100/200	50/100/200
416 (China)	407-425			
619 (China)	608-630	O-QPSK	250/500	62.5/125
IEEE 802.15.4u-2016		2FSK	10/20	10/20
866 (India)	865-867		50/100/150	50/100/150
		OFDM (Opt. 4)	Table III	N/A
		O-QPSK	6.25-50	1.56-12.5
IEEE 802.15.4t-2017 2450	2400-2483.5	MSK	2000	250

TABLE II
IEEE 802.15.4k LECIM BPSK and O-QPSK data rates (kbps).

Spreading Factor	**Modulation Rate (ksym/s)**				
	200	**400**	**600**	**800**	**1000**
16	6.25 / 12.5 kbps	12.5 / 25 kbps	18.75 / 37.5 kbps	25 / 50 kbps	31.25 / 62.5 kbps
32	3.125 / 6.25 kbps	6.25 / 12.5 kbps	9.375 / 18.75 kbps	12.5 / 25 kbps	15.625 / 31.25 kbps
64	1.5625 / 3.125 kbps	3.125 / 6.25 kbps	4.6875 / 9.375 kbps	6.25 / 12.5 kbps	7.8125 / 15.625 kbps
128	0.7813 / 1.5625 kbps	1.5625 / 3.125 kbps	2.3438 / 4.6875 kbps	3.125 / 6.25 kbps	3.9063 / 7.8125 kbps
256	0.3906 / 0.7813 kbps	0.7813 / 1.5625 kbps	1.1719 / 2.3438 kbps	1.5625 / 3.125 kbps	1.9531 / 3.9063 kbps
512	0.1953 / 0.3906 kbps	0.3906 / 0.7813 kbps	0.5859 / 1.1719 kbps	0.7813 / 1.5625 kbps	0.9766 / 1.9531 kbps
1024	0.0977 / 0.1953 kbps	0.1953 / 0.3906 kbps	0.293 / 0.5859 kbps	0.3906 / 0.7813 kbps	0.4883 / 0.9766 kbps
2048	0.0488 / 0.0977 kbps	0.0977 / 0.1953 kbps	0.1465 / 0.293 kbps	0.1953 / 0.3906 kbps	0.2441 / 0.4883 kbps
4096	0.0244 / 0.0488 kbps	0.0488 / 0.0977 kbps	0.0732 / 0.1465 kbps	0.0977 / 0.1953 kbps	0.1221 / 0.2441 kbps
8192	0.0122 / 0.0244 kbps	0.0244 / 0.0488 kbps	0.0366 / 0.0732 kbps	0.0488 / 0.0977 kbps	0.061 / 0.1221 kbps
16384	0.0061 / 0.0122 kbps	0.0122 / 0.0244 kbps	0.0183 / 0.0366 kbps	0.0244 / 0.0488 kbps	0.0305 / 0.061 kbps
32768	0.0031 / 0.0061 kbps	0.0061 / 0.0122 kbps	0.0092 / 0.0183 kbps	0.0122 / 0.0244 kbps	0.0153 / 0.0305 kbps

TABLE III
OFDM datarates according to the MCS and option selected.

	option 1	**option 2**	**option 3**	**option 4**
MCS 0 BPSK (*Fq. Rep.)	100 kbps	50 kbps	25 kbps	12.5 kbps
MCS 1 BPSK (*Fq. Rep.)	200 kbps	100 kbps	50 kbps	25 kbps
MCS 2 QPSK (*Fq. Rep.)	400 kbps	200 kbps	100 kbps	50 kbps
MCS 3 QPSK	800 kbps	400 kbps	200 kbps	100 kbps
MCS 4 QPSK	1200 kbps	600 kbps	300 kbps	150 kbps
MCS 5 16-QAM	1600 kbps	800 kbps	400 kbps	200 kbps
MCS 6 16-QAM	2400 kbps	1200 kbps	600 kbps	300 kbps

References

[1] "IEEE standard for information technology - telecommunications and information exchange between systems - local and metropolitan area networks specific requirements part 15.4: Wireless medium access control (mac) and physical layer (phy) specifications for low-rate wireless personal area networks (lr-wpans)," *IEEE Std 802.15.4-2003*, pp. 1–670, 2003.

[2] A. G. Ramonet and T. Noguchi, "Ieee 802.15.4 historical evolution and trends," in *2019 21st International Conference on Advanced Communication Technology (ICACT)*, Feb 2019, pp. 351–359.

[3] *NXP ZigBee 3.0 Stack User Guide*.

[4] "IEEE standard for information technology– local and metropolitan area networks– specific requirements– part 15.4: Wireless medium access control (mac) and physical layer (phy) specifications for low rate wireless personal area networks (wpans)," *IEEE Std 802.15.4-2006 (Revision of IEEE Std 802.15.4-2003)*, pp. 1–320, Sept 2006.

[5] "IEEE standard for information technology - telecommunications and information exchange between systems - local and metropolitan area networks - specific requirement part 15.4: Wireless medium access control (mac) and physical layer (phy) specifications for low-rate wireless personal area networks (wpans)," *IEEE Std 802.15.4a-2007 (Amendment to IEEE Std 802.15.4-2006)*, pp. 1–203, 2007.

[6] "IEEE standard for information technology-telecommunications and information exchange between systems-local and metropolitan area networks-specific requirements part 15.4: Wireless medium access control (mac) and physical layer (phy) specifications for low-rate wireless personal area networks (wpans) amendment 2: Alternative physical layer extension to support one or more of the chinese 314-316 mhz, 430-434 mhz, and 779-787 mhz bands," *IEEE Std 802.15.4c-2009 (Amendment to IEEE Std 802.15.4-2006)*, pp. 1–21, April 2009.

[7] "IEEE standard for information technology-telecommunications and information exchange between systems-local and metropolitan area networks-specific requirements part 15.4: Wireless medium access control (mac) and physical layer (phy) specifications for low-rate wireless personal area networks (wpans) amendment 3: Alternative physical layer extension to support the japanese 950 mhz bands," *IEEE Std 802.15.4d-2009 (Amendment to IEEE Std 802.15.4-2006)*, pp. 1–27, April 2009.

[8] "IEEE standard for local and metropolitan area networks–part 15.4: Low-rate wireless personal area networks (lr-wpans)," *IEEE Std 802.15.4-2011 (Revision of IEEE Std 802.15.4-2006)*, pp. 1–314, Sept 2011.

[9] "IEEE standard for local and metropolitan area networks–part 15.4: Low-rate wireless personal area networks (lr-wpans) amendment 1: Mac sublayer," *IEEE Std 802.15.4e-2012 (Amendment to IEEE Std 802.15.4-2011)*, pp. 1–225, April 2012.

[10] H. Kurunathan, R. Severino, A. Koubaa, and E. Tovar, "IEEE 802.15.4e in a nutshell: Survey and performance evaluation," *IEEE Communications Surveys Tutorials*, vol. 20, no. 3, pp. 1989–2010, thirdquarter 2018.

[11] *Identification cards - Contactless integrated circuit cards - Proximity cards*, ISO 14 443-1, 2008.

[12] "IEEE standard for local and metropolitan area networks– part 15.4: Low-rate wireless personal area networks (lr-wpans) amendment 2: Active radio frequency identification (rfid) system physical layer (phy)," *IEEE Std 802.15.4f-2012 (Amendment to IEEE Std 802.15.4-2011)*, pp. 1–72, April 2012.

[13] "IEEE standard for local and metropolitan area networks–part 15.4: Low-rate wireless personal area networks (lr-wpans) amendment 3: Physical layer (phy) specifications for low-data-rate, wireless, smart metering utility networks," *IEEE Std 802.15.4g-2012 (Amendment to IEEE Std 802.15.4-2011)*, pp. 1–252, April 2012.

[14] Y. Kabalci, "A survey on smart metering and smart grid communication," *Renewable and Sustainable Energy Reviews*, vol. 57, pp. 302 – 318, 2016.

[15] *Anritsu MS2830A Signal Analyzer Product Introduction*.

[16] J. Muoz, T. Chang, X. Vilajosana, and T. Watteyne, "Evaluation of ieee802.15.4g for environmental observations," *Sensors*, vol. 18, no. 10, 2018. [Online]. Available: http://www.mdpi.com/1424-8220/18/10/3468

[17] J. Muoz, E. Riou, X. Vilajosana, P. Muhlethaler, and T. Watteyne, "Overview of ieee802.15.4g ofdm and its applicability to smart building applications," in *2018 Wireless Days (WD)*, April 2018, pp. 123–130.

[18] "IEEE standard for local and metropolitan area networks - part 15.4: Low-rate wireless personal area networks (lr-wpans) amendment 4: Alternative physical layer extension to support medical body area network (mban) services operating in the 2360 mhz - 2400 mhz band," *IEEE Std 802.15.4j-2013 (Amendment to IEEE Std 802.15.4-2011 as amended by IEEE Std 802.15.4e-2012, IEEE Std 802.15.4f-2012, and IEEE Std 802.15.4g-2012)*, pp. 1–24, Feb 2013.

[19] "IEEE standard for local and metropolitan area networks– part 15.4: Low-rate wireless personal area networks (lr-wpans)–amendment 5: Physical layer specifications for low energy, critical infrastructure monitoring networks." *IEEE Std 802.15.4k-2013 (Amendment to IEEE Std 802.15.4-2011 as amended by IEEE Std 802.15.4e-2012, IEEE Std 802.15.4f-2012, IEEE Std 802.15.4g-2012, and IEEE Std 802.15.4j-2013)*, pp. 1–149, Aug 2013.

[20] B. G. Gebremedhin, J. Haapola, and J. Iinatti, "Performance evaluation of ieee 802.15.4k priority channel access with dsss phy," in *Proceedings of European Wireless 2015; 21th European Wireless Conference*, May 2015, pp. 1–6.

[21] "Ieee standard for local and metropolitan area networks - part 15.4: Low-rate wireless personal area networks (lr-wpans) - amendment 6:

Tv white space between 54 mhz and 862 mhz physical layer," *IEEE Std 802.15.4m-2014 (Amendment to IEEE Std 802.15.4-2011 as amended by IEEE Std 802.15.4e-2012, IEEE Std 802.15.4f-2012, IEEE Std 802.15.4g-2012, IEEE Std 802.15.4j-2013, and IEEE Std 802.15.4k-2013)*, pp. 1–118, April 2014.

[22] T. Shimomura, T. Oyama, and H. Seki, "Analysis of tv white space availability in japan," in *2012 IEEE Vehicular Technology Conference (VTC Fall)*, Sep. 2012, pp. 1–5.

[23] C. Sum, M. Zhou, L. Lu, F. Kojima, and H. Harada, "Performance and coexistence analysis of multiple ieee 802 wpan/wlan/wran systems operating in tv white space," in *2014 IEEE International Symposium on Dynamic Spectrum Access Networks (DYSPAN)*, April 2014, pp. 145–148.

[24] "Ieee standard for local and metropolitan area networks - part 15.4: Low-rate wireless personal area networks (lr-wpans) - amendment 7: Physical layer for rail communications and control (rcc)," *IEEE Std 802.15.4p-2014 (Amendment to IEEE Std 802.15.4-2011 as amended by IEEE Std 802.15.4e-2012, IEEE Std 802.15.4f-2012, IEEE Std 802.15.4g-2012, IEEE Std 802.15.4j-2013, IEEE Std 802.15.4k-2013, and IEEE Std 802.15.4m-2014)*, pp. 1–45, May 2014.

[25] "IEEE standard for low-rate wireless networks," *IEEE Std 802.15.4-2015 (Revision of IEEE Std 802.15.4-2011)*, pp. 1–709, April 2016.

[26] "IEEE standard for low-rate wireless networks – amendment 1: Physical layer utilizing china medical bands," *IEEE Std 802.15.4n-2016 (Amendment to IEEE Std 802.15.4-2015)*, pp. 1–27, April 2016.

[27] "IEEE standard for low-rate wireless networks –amendment 2: Ultra-low power physical layer," *IEEE Std 802.15.4q-2016 (Amendment to IEEE Std 802.15.4-2015 as amended by IEEE Std 802.15.4n-2016)*, pp. 1–52, April 2016.

[28] "IEEE standard for low-rate wireless networks–amendment 3: Use of the 865 mhz to 867 mhz band in india," *IEEE Std 802.15.4u-2016 (Amendment to IEEE Std 802.15.4-2015 as amended by IEEE Std 802.15.4n-2016 and IEEE Std 802.15.4q-2016)*, pp. 1–18, Feb 2017.

[29] "IEEE standard for low-rate wireless networks–amendment 4: Higher rate (2 mb/s) physical (phy) layer," *IEEE Std 802.15.4t-2017 (Amendment to IEEE Std 802.15.4-2015 as amended by IEEE Std 802.15.4n-2016, IEEE Std 802.15.4q-2016, and IEEE Std 802.15.4u-2016*, pp. 1–25, April 2017.

[30] "IEEE standard for low-rate wireless networks - amendment 5: Enabling/updating the use of regional sub-ghz bands," *IEEE Std 802.15.4v-2017 (Amendment to IEEE Std 802.15.4-2015, as amended by IEEE Std 802.15.4n-2016, IEEE Std 802.15.4q-2016, IEEE Std 802.15.4u-2016, and IEEE Std 802.15.4t-2017)*, pp. 1–35, June 2017.

[31] "Ieee standard for low-rate wireless networks amendment 6: Enabling spectrum resource measurement capability," *IEEE Std 802.15.4s-2018 (Amendment to IEEE Std 802.15.4-2015 as amended by IEEE Std 802.15.4n-2016, IEEE Std 802.15.4q-2016, IEEE Std 802.15.4u-2016, IEEE Std 802.15.4t-2017, IEEE Std 802.15.4v-2017, and IEEE Std 802.15.4-2015/Cor 1-2018)*, pp. 1–51, June 2018.

[32] "Ieee standard for low-rate wireless networks - amendment 7: Defining enhancements to the smart utility network (sun) physical layers (phys) supporting up to 2.4 mb/s data rates," *IEEE Std 802.15.4x-2019 (Amendment to IEEE 802.15.4-2015 as amended by IEEE 802.15.4n-2016, IEEE 802.15.4q-2016, IEEE 802.15.4u-2016, IEEE 802.15.4t-2017, IEEE 802.15.4v-2017, IEEE 802.15.4s-2018, and IEEE 802.15.4-2015/Cor. 1-2018)*, pp. 1–30, April 2019.

[33] J. Zheng and M. J. Lee, "A comprehensive performance study of ieee 802.15. 4," *Sensor network operations*, vol. 4, pp. 218–237, 2006.

[34] A. Boulis, "Castalia userś manual v3.2," *NICTA*, 2011.

[35] Nsam, "Ns-3 discrete event simulator," http://www.nsnam.org, accessed Jan. 07. 2017.

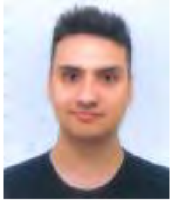
[36] P. Jurčík and A. Koubâa, "The ieee 802.15.4 opnet simulation model:reference guide v2.0," *IPP-HURRAY Technical Report, HURRAY-TR-070509*, 2007.

[37] A. Cunha, A. Koubaa, R. Severino, and M. Alves, "Open-zb: an open-source implementation of the ieee 802.15.4/zigbee protocol stack on tinyos," in *2007 IEEE International Conference on Mobile Adhoc and Sensor Systems*, Oct 2007, pp. 1–12.

[38] J. Flora and P. Bonnet, "Never mind the standard here is the tinyos 802.15. 4 stack," *University of Copenhagen, Technical Report*, vol. 6, no. 10, 2006.

[39] J.-H. Hauer, "Tkn15. 4: An ieee 802.15. 4 mac implementation for tinyos," 2009.

[40] Zigbee Alliance, "Zigbee 3.0," https://www.zigbee.org/, accessed May. 15. 2019.



Alberto Gallegos Received his B.E. degree in computer science from Guadalajara University, Jalisco, Mexico in 2005. He later received his M.S. and PH.D. degrees in Engineering from Ritsumeikan University, Shiga, Japan in 2014 and 2018 respectively. He joined the College of Information Science and Engineering at Ritsumeikan University in 2018, where he is currently Assistant Professor. His current research interests include but are not limited to Wireless Sensor Networks and routing protocols.

Taku Noguchi Received his B.E., M.E. and Ph.D. degrees in communications engineering from Osaka University, Osaka, Japan in 2000, 2002 and 2004, respectively. He joined College of Information Science and Engineering at Ritsumeikan University in 2004, where he is currently a Professor. His research interests include performance analysis and the design of computer networks and wireless networks. He is a member of IEEE, IEICE and IPSJ.

Classify and Analyze the Security Issues and Challenges in Mobile banking in Uzbekistan

Azamjon Abdullaev *, Mohammed Abdulhakim Al-Absi *, Ahmed Abdulhakim Al-Absi **, Mangal Sain*, Hoon Jae Lee *

** Dongseo University, Busan, Republic of Korea*

*** Kyungdong University Gangwon-do, Republic of Korea*

azamjon.a.sobirovich@gmail.com, mohammed.a.absi@gmail.com, absiahmed@kduniv.ac.kr, mangalsain1@gmail.com, hjlee@dongseo.ac.kr

***Abstract*—Due to advancement and growth in mobile technology, mobile banking is now included in our lives. in Uzbekistan, Mobile banking is a subset of Mobile-services where all banks provide Internet banking service uses SSL encryption of data transmitted from the user's computer to the bank system and vice versa. Security measure allows the users to exclude a previously common type of fraud. The security in crowded enterprise architecture is a concern that encompasses user's mobile clients, web applications, mobile devices, back -end applications and networks. All systems interfaces can undergo a form of attacks and it needs to be secured. The main objective of this work is to classify and analyze the Security issues and challenges in Mobile banking in Uzbekistan.**

***Keyword*—Internet banking, Mobile Banking, Challenges Mobile Banking in Uzbekistan, Security Issue.**

I. INTRODUCTION

THE internet has both the attributes and advantages that can transcend the limits of space and distance facilitating the delivery of service "anywhere at any time" from any internet-enabled device. These technological advances have enabled consumers to avail of banking services without the need to physically visit a bank. Financial institutions have also identified the opportunities these technological advances present to attract new customers, develop and maintain current customer relationships, cross-selling of products and develop new innovative service offerings.

For today, online banking is one of the modern tools, which allow banks to increase their profitability and increase their profitability client base. This article examines the world-wide issues and challenges online banking as well as an overview of the current status of online banking in Uzbekistan.

A mobile phone is a device that widespread technology that turns into a part of every person in the information era. Mobile banking is a framework that permits clients of a monetary organization to direct various budgetary exchanges through a cell phone, for example, cell phone or personal digital assistant. Mobile Banking indicates to arrangement and benefits of saving money and monetary administrations with the assistance of mobile telecommunication devices. Banking is one of the big financial foundations that explore the opportunity of technology where this technology allowed the services to have the best customer experience and comfort. Technologies perform a significant role in the banking sector. The development of mobile devices nowadays, mobile banking is one of the important strategies in the banking industry. Mobile banking is a mobile computing application which supports customers with mobile banking service. Whenever and what they want, the users be able to mobile banks such as short messages. Mobile banking [1] has emerged as a popular mode of banking in many developed and developing countries. Access to mobile data services can be a distinct part depending on technology or performance type. The current population of Uzbekistan is 32,520,015 as of Tuesday, November 6, 2018, based on the latest United Nations estimates.

Depend on the International Telecommunication Union, the number of mobile users in 2017 [2] exceeds more than 7 billion. In 2000, their number was estimated to be 1 billion. In turn; the number of Internet users reached 4.2 billion. The number of mobile subscribers in Uzbekistan has increased by 1.4 million in 2017 compared to 2016 and amounted to 22.8 million people in January 2018.

Nowadays, internet banking helps the users and customers.

Manuscript received on Jan. 1, 2019. This work was supported by the Institute for Information and Communications Technology Promotion (Grant Number: 2018-0-00245) and it was also supported by the Basic Science Research Program through the National Research Foundation of Korea funded by the Ministry of Education, Science, and Technology (Grant Number: NRF2016R1D1A1B01011908), and a follow-up of the invited journal to the accepted & presented paper entitled "Security Challenge and Issue of Mobile Banking in Republic of Uzbekistan: A State of Art Survey" of the 21th International Conference on Advanced Communication Technology (ICACT2019).

Azamjon Abdullaev. Currently, he is a Master student in the Department of Computer Engineering at Dongseo University, South Korea. (e-mail: azamjon.a.sobirovich@gmail.com)

Mohammed Abdulhakim Al-Absi. Currently, he is a Ph.D. student in the Department of Computer Engineering at Dongseo University, South Korea. (e-mail: mohammed.a.absi@gmail.com)

Ahmed Abdulhakim Al-Absi. Author is an assistant professor and head of smart computing department at Kyungdong University - Global Campus in South Korea. (e-mail: absiahmed@kduniv.ac.kr)

Mangal Sain. Author is an Assistant Professor in the Department of Computer Engineering, Dongseo University, South Korea. (e-mail: mangalsain1@gmail.com)

Hoon Jae Lee. Currently, he is a professor in the Department of Information Communication Engineering at Dongseo University, South Korea (corresponding author, phone: +82-10-2801-3735, email: hjlee@dongseo.ac.kr)

Customers can money transfer, check out their account details, get their bank account statements and pay money sitting in the comfort of their offices and at home. On the other hand, the biggest limitation of internet banking needs a personal computer and internet connection. And this is a little problem in developing countries if we consider most developing countries especially in Uzbekistan. Despite various initiatives, the level of internet connection in Uzbekistan is still relatively low. Mobile banking can solve this problem as it reduces the user's requirement to just their mobile phones.

Payments for all mobile services in Uzbekistan (Ucell, UzMobile CDMA, UzMobile GSM, UMS, Beeline, Perfectum); Natural gas and electricity payments; Internet access charges (Sarkor Telecom, Uzonline, EVO, TPS); Payments for fixed telephony; Payments for IPTV; Payments for cable television (UzDigital TV, Stars TV); [3] Payments within the system, Customers can transfer funds from plastic card through the special account opened to them by transferring funds from other plastic cards to the mobile bank's special number, i.e. non-cash Payments; Individuals Monthly payments for loans received from Bank branches; One - time payments for goods and services purchased.

II. MOBILE PAYMENT CHARACTERISTICS

In developing countries for example in Uzbekistan, mobile banking providers rely on agents to acquire customers and manage liquidity. They reach sensitive customer information such as the mobile number, user name, and other credentials used for authentication and identification purpose. These factors are not well equipped to keep customer sensitive information and can be easily lead to information leakage. The failure of a service provider to protect or control sensitive information is a serious threat to business processes and potential customer security.

There are some conditions for the mobile payment service to be acceptable as a market payment service:

- Universality: where the mobile banking should give transactions services among Business to Businesses (B2B), Customer to Customer (C2C), and Businesses to Customer (B2C)
- Interoperability: combining technologies as one system based on standards
- Security, Privacy and Trust: customers go to the bank and give their personal information and also depositing their money. However, there should be trust between the customer and the bank so the customer can trust the mobile banking payment service and make sure that his personal information not be misused.
- Simplicity and Usability: mobile banking payment services should able to fit the customer's convenience.
- Cross border payments: mobile banking should be widely accepted in the word-wide
- Cost and Speed: where speed it's very important in the mobile payment that convenience merchants and customers.

III. BANKING SYSTEM AND MOBILE BANKING IN UZBEKISTAN

Uzbekistan has 29 commercial banks, including 5 state-owned banks, 13 state-owned banks, 5 foreign banks, and 6 private banks. There are 8,610 credit institutions nationwide, including microfinance institutions and commercial bank branches. The Uzbek banking system remains under State control through a series of regulatory measures, legislation, declarations and complex practices. Most bank assets are still in state-owned or state-controlled banks, and most of the loans are directed by the government or directed to develop a pre-determined industrial sector. By limiting the role of banks as a financial intermediary to reform the slow financial system, it limits the ability of citizens and private companies to access credit and other financial services [21].

Mobile banking in Uzbekistan, primarily by Hamkorbank and its international financial corporation and the Asian Development Bank, was developed by a hamkormobile platform in May 2009 [4]. It was an independent platform allowing operators to save, receive, transfer, withdraw money, as well as buy goods and services.

Remote service for individuals - this is a system that allows you to control your bank account from anywhere using a mobile phone or the Internet browser [5].

IV. SYSTEM OPPORTUNITIES

Payments for cellular operators and fixed telephony, Internet providers and digital television services, Utility payments, Single-time payments for Consumer Goods and Services, and other payments, payments for consumer and mortgage loans, seeing and replenishing of account status, obtaining information on deposit balances and interest accrued, online Smart Visa balances and its get information about turnover [6]. Payments to the budget, transfer of bonus cards from card to card, online conversion, connecting Visa and Union Pay cards and checking account status and more.

We can see from Table I [20], three banks controlled 59.9% of the total assets banking in 2018 compared to 86.9% in 2001. The National Bank of Uzbekistan controlled 76% of the banking sector in 2001 where 30.9% in January 2018. The national bank of Uzbekistan controlling 19.5% and 18.5% of the deposit and market loan shares in 2018. The foreign ownership controlled 7.7% of the sector in 2018. However, there is 0.8% of the share of the bank with no state ownership is increased in 2001 to 13% in 2018.

TABLE I
UZBEKISTAN'S BANKING SYSTEM OWNERSHIP AND CONCENTRATION

Market Share (Percentage of Banking Assets)				
	2001	2014	2016	2018
Market share of the top three banks	86.6	50.6	49.7	59.9
Market share of the top five banks	91.3	63.7	62.9	71.8
State-owned banks	82.2	41.2	41.4	48.8

Shareholding banks with indirect state ownership	6.1	35.5	33.7	33.2
Banks with foreign ownership	0.9	8.7	9.9	7.7

The main provider mobile platform in Uzbekistan CLICK was founded in November 2011. The activity of the company is the development of software products for commercial banks, organizations, individuals, their adaptation to various hardware and software complexes and further improvement. software products are protected by the current legislation of the Republic of Uzbekistan [7]. "CLICK" system is a mobile banking system that allows mobile operators to pay for services of cellular operators, Internet providers and other companies; traditional and internet-shop purchases, card-to-card transfers, and more. Key features of the CLICK system:

- transfer from card to card
- "CLICK Terminal" service
- Manage the accounts you have sent to you
- Auto payment service
- View payment history
- An online check of account balances
- Repayment of received loans
- SMS notifications

The advantages of the click system are as follows; Hammerliness: Usage of a USSD-request on a negative balance and without the use of the Internet, even if the user's number is blocked, can pay at any time from his bank account. In order to use the system, you do not need to install any software on the phone: USSD-request can be sent from any mobile phone [8].

Proximity: Opportunity to replenish the balance and manage your bank account, without having to go to the bank branches and paying for the recent payment receipt or payment acceptance and payment system locations opportunity to pay without leaving home. The entire payment system is in the pocket of each subscriber.

In order to connect to the system, it is not required to open special accounts in the bank and deposit funds to another deposit. Our system allows you to "bind" your number to any existing account of an individual.

V. SECURITY ISSUES AND CHALLENGES IN MOBILE BANKING

Mobile banking has become a big challenge for banks because of the fast development of mobile technologies such as 1G, 2G, 3G, 4G, and 5G. In Uzbekistan, most of people use the ATM machine as well as online banking services. However, they are afraid of mobile banking due to the theft of mobile handset and misuse.

A. Security issues and Mobile banking with Wireless Application Protocol

New technology has made people access to the internet much easier. Users connect their mobile devices to WAP and GPRS, access various banking services, such as transferring money from one account to another and paying the cost of items purchased. In Uzbekistan, mobile devices have become widespread and are becoming necessary for consumers, entrepreneurs and business people alike. Although these devices are relatively small and inexpensive but have multiple features. Portable devices have built-in special devices, such as accelerometers, cameras, removable media readers and GPS receivers. It also integrates many wireless technologies such as Wireless Fidelity (Wi-Fi), Bluetooth, Near Field Connection (NFC) and Mobile Interface (CDMA or GSM). The interconnect network is connected to the world. At the same time, security and convenience are important factors in the growth of mobile banking and mobile device trading.

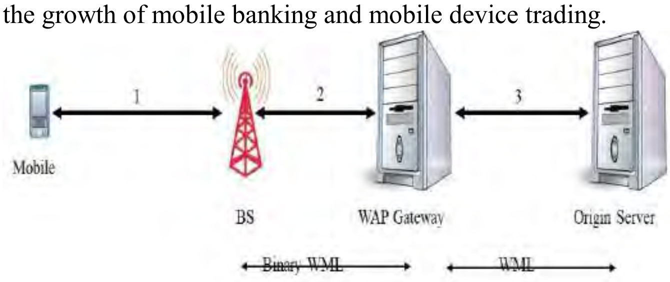


Fig. 1. Security aspect in the WAP architecture

Wireless Application Protocol is used for communication among devices where the customer uses it to realize the functionality of internet banking. For secure and successful transmission between the customer and bank, the encryption data process has been used but this is not good enough to secure the sensitive data among the customer and bank. The transmission needs to be more security methods with high memory storage capacity. We are unable to apply a complex cryptographic systems due to the mobiles have a low computational capacity [9]. Table II shows the Security threads for mobile banking.

Because of the technology development is increasing day by day, it is important to provide very good end-to-end security Fig. 1. However, it is very difficult to provide security using WAP because at the gateway the data is not encrypted while switching of protocol process [10]

There are two technologies are using for mobile banking namely Wireless Internet Gateway (WIG) (short message service) and Wireless Application Protocol (WAP). Security is very important before you provide the services [11]

TABLE II
SECURITY THREADS FOR MOBILE BANKING

Danger Identification regarding Mobile banking	
Security threads for mobile banking	Security issues and Mobile banking with Wireless Application Protocol
	Transaction and massage transmission Using mobile Banking
	Third-party identification password
	Identification of password

Recently in Uzbekistan that banks had a chance long enough to communicate with customer's mobile banking applications so and with their performers - the developers, so they are able to look at problems from different positions. Often there are organizational problems when in their technical assignments for customers. The problem of data storage, Mobile devices can be easily lost or just lose sight for a while. Meanwhile, they can say about their owners much more than their board "brothers". Therefore, the problem of data storage on mobile devices is one of the most important. When analyzing the security of mobile applications banking often observes critical information in open form, which is either simply stored in the application, or unconsciously "falls" in cache network requests, logs, crash dumps, screenshots. An attacker when getting physical access, the device can download these critical files. Another equally important issue is to work in an untrusted environment. Often users put themselves their devices are at risk getting root access on their Android device or installing jailbreak on iOS devices. However, they often do not understand that when you receive various free "bonuses" The OS's built-in security mechanisms are partially or completely disabled. This increases the probability of infection of the device with malicious code and implements a successful attack by an attacker. Worth noting is the problem of application distribution. It concerns only mobile operating systems with many app stores, and first of all, the Android OS. For Android, there is a huge number of stores (Google Play, Samsung Apps, Yandex market, Amazon mobile app distribution, Slide Me, etc.). Some of them are installed by default. As a result, one store may contain the legitimate application, and in another - its modified version with malicious functionality.

There are also unofficial applications for banks that often represent "Wrappers" over Internet sites. We recommend use only official apps, but banks need to monitor store applications to detect fakes.

Code deobfuscation occurs in Android applications. In IOS, it is absolutely missing. The situation is similar with anti-debug technicians as for channel security data transfer. This is a problem for mobile banking. But mobile devices are good that provides freedom of movement and choosing a place to connect to the network on your own.

B. *Authentication Risks and Issues*

The people like to use the mobile phone anywhere they go so they use the mobile banking application while they are moving and in any situation. The Security mechanism can be done by identifying the customer's pin number, phone number etc.

Authentication Model: two kinds of services are provided to the customer's one is the direct bank services to the customer and the second one is the bank will share the services to the third-party provider.

C. *Bank provides the service directly to the customer Architecture*

If a customer wants to transfer money using mobile banking he has to authenticate himself to the bank sever using a firewall then the server will verify the customer security password and pin number then the bank will allow him to complete the process for money transfer[12]. This method has security issues for instance system crash, server failure and malevolent intrusion [13]. However, banks don't prefer using this method Fig. 2.

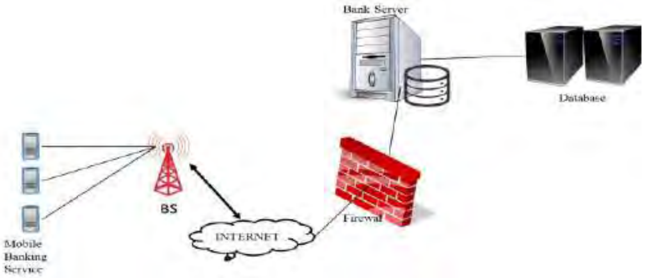


Fig. 2. Service directly to customer Architecture

D. *SMS Spoofing Attack*

The spoofing attack is the most serious attack in SMS mobile banking where the attacker can send a message to the sender number so most of the organism doesn't use mobile banking using SMS [14]

E. *Mobile banking virus attacks*

There are many types of viruses, Trojan and malicious internet program [15]. For instance, Trojan can get the password from the web easily and from the operating system cached information. Zeus Trojan is used for stealing the password and the authentication number for the mobile banking transactions [16]

VI. Mobile Payment Security Framework

In fact, mobile phone payments can be divided into payments close to the field and remote payments. Near-field payments include an RFID-based mobile payment framework and an NFC-based mobile payment framework. Payment is not yet popular and is limited. In the case of a request, the protection of unencrypted information is not yet effective. In addition, some attackers convert NFC-enabled mobile phones to point-of-sale (POS) devices for non-contact card transactions as well as point-of-sale (POS) frauds in Portuguese phone mode.

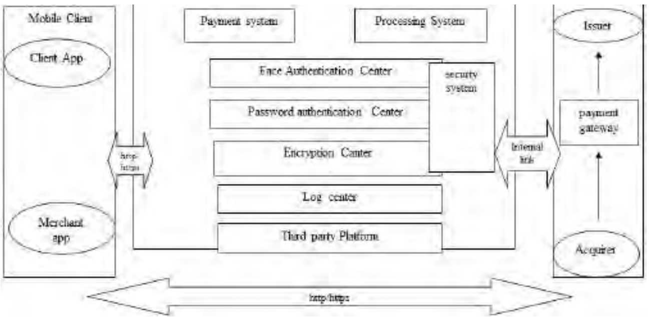


Fig. 3. The framework consists of three parts: a transaction interface, a server-side and a mobile client.

Mobile Client: The application appears in the client application and sales application in Fig. 3 because the application needs to complete the user's work. The two applications use the same program structure as they are used to perform the payment.

VII. Interfaces Design and Mobile Payment Security Processes

This frame adds the idea of face recognition to secure user accounts. At the same time, a third-party regulatory body has been added to manage the user's assets. If the user logs on to the system using Uname and Psd, the payment process is as follows Fig. 4:

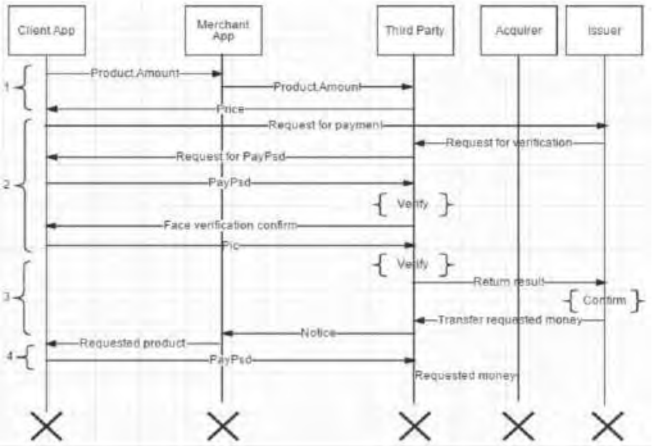


Fig. 4. Mobile Payment Security Processes and Interfaces Design

1) Find what you need and confirm the order with the dealer. Once the merchant receives the customer's request, they must send the request to a third-party regulatory agency, which includes the product name, unit price, amount, etc. The total price is sent after your third party certificate.

2) You need to provide a PayPal password after the customer has received and confirmed the total price. When a third party confirms the payment password, a request is sent to an external image to the client.

3) Once verification of identity and password has been completed, the issuing institution transfers the amount necessary for the transaction to the third-party account. He then sends the seller a notice of receipt to inform the customer of the third-party vendor that the goods will be delivered.

4) The customer needs to confirm it to the third party that receives the goods online. After that, the amount of payment necessary to the third party is transferred to the acquirer. At this point, the deal is over.

In this case, four request APIs are displayed in Table III to facilitate access to their mobile phone applications and identity technology.

TABLE III
NECESSARY FOR THE FACE AUTHENTICATION

API Name	Function Description
Face Detection API	Detect human face in images, then the detected face will be marked
PCA Processing API	Do 2DPCA to existing data
Face Matching API	Compare two processed face images
Grayscale Conversion API	Put color image convert into gray images

VIII. SECURING MOBILE BANKING ON ANDROID WITH SSL CERTIFICATE PINNING

Let's say you want to exchange some sensitive data between your application and a server. SSL should do the trick, but in many cases, you'll have to send sensitive data between your application and server. Take mobile banking applications for example. The last thing you want is a malicious hacker to steal someone's bank account info – or worse, their money [18].

Security is crucial for a mobile banking solution, so you'll be using SSL to keep that data safe and secret. But there's a catch. The app has no relationship with the trust store of the device to enforce security using static SSL certificates. It's not easy to destroy fixed-coded stores in your app. The app must be compiled, edited, and reassembled, and cannot sign the same Android activation key used by the original developer of the app. Table IV shows the present Uzbekistan mobile banking implementation solutions.

TABLE IV
UZBEKISTAN MOBILE BANKING IMPLEMENTATIONS SOLUTIONS

IX. MOBILE BANKING ANALYSIS

Central Bank of Uzbekistan Tashkent, [17] on 1 April 2013

	WAP	SMS &USSD	SMS &WIG
Transmission Speed	The transfer rate of any mobile banking solution depends on several factors. This depends on the signal strength received by the user's mobile phone. Thus, this depends on the user's location, network traffic, the number of base station towers around the user's mobile device, etc. All these factors affect the transfer rate and you cannot do real experiments.		
Cost for Bank Server	GPRS is generally cheaper than SMS.	One SMS message for reply	Multiple SMS reply messages required.
Usability	Mobile phone WAP browser interface.	It requires no menu. The user interface depends on how the users interact with their mobile phones to send SMS messages.	Menu-based user interface.
Compatibility	Requires mobile phone to be WAP capable and GPRS, EDGE or 3G enabled.	Any mobile phone that can support USSD and SMS can use this service.	Requires mobile phone to be SIM Application Toolkit (SAT) compatible. It is SIM card dependent.
Security	Standard WTLS protocol. No End to End encryption.	USSD String sent in plaintext. Authentication relies on IMEI.	USSD string and SMS message transmitted in plaintext.
Cost for Customer	It depends on the amount of data required to be sent.	USSD is for free. One SMS message required	Multiple SMS messages required.

the number of users of distance banking services in Uzbekistan made up over 149,000, the central bank noted that the number of SMS-banking and mobile banking services made up 106,925 units and internet banking 42,098 units as of 1 April 2013.

Compared to 1 January 2013, the number of users of SMS banking and mobile banking service rose by 37,600 and internet banking – by 2,930 units Fig. 5.

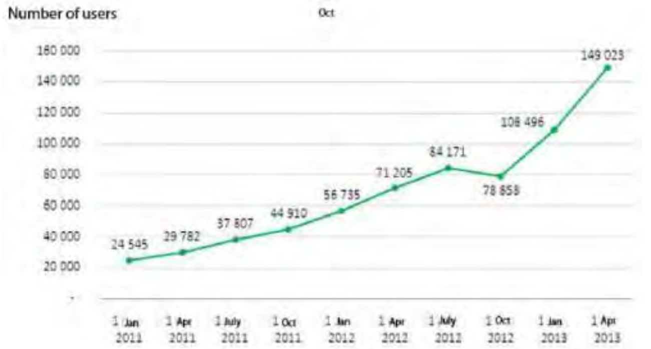


Fig. 5. Number of users of distance banking services

According to the central bank, the National Bank of Uzbekistan (34,300 users), Ipoteka Bank (30,314 units) and Microcreditbank (15,477 units) are leading on a number of users of distance banking services as showing in the Fig. 6 and Table V.

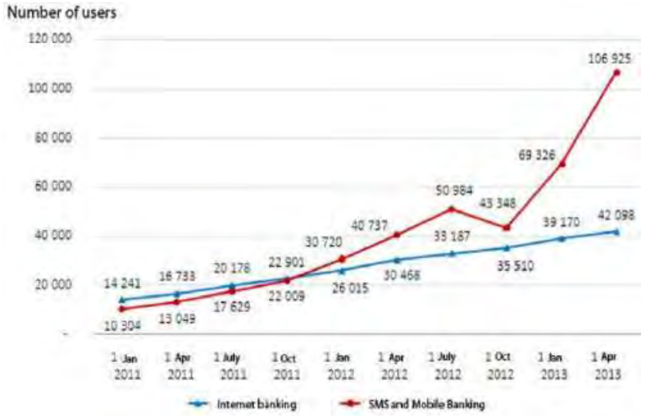


Fig. 6. Number of users of distance banking services by type of system

TABLE V
MOBILE BANKING SERVICES OFFERED BY SOME OF THE BANKS IN UZBEKISTAN

No	Name of the Bank	Internet banking Users	SMS-banking and mobile banking users	Total
1	National Bank of Uzbekistan	4227	30071	34298
2	Uzpromstroybank	2042	1348	3390
3	Agrobank	1765	749	2514
4	Ipoteka-Bank	3158	27255	30413
5	Microcreditbank	2385	13062	15447
6	People's Bank	1204	-	1204
7	Savdogarbank	459	-	459
8	Qishloq Qurilish Bank	1239	8692	9931
9	Turon Bank	981	613	1594
10	Hamkor Bank	4147	4767	8914
11	Asaka Bank	1503	8513	10106
12	Ipak Yoli Bank	3229	2042	5271
13	Uzbek-Turkish Bank	177	128	305
14	Trust Bank	1352	970	2322
15	Aloqabank	1226	1789	3015
16	KDB Bank Uzbekistan	217	498	715
17	Turkiston bank	227	25	252
18	Sederat Iran	11	12	236
19	Samarkand Bank	6302	429	6731
20	Universalbank	258	425	683
21	Kapitalbank	2803	3907	6710
22	Ravnaq Bank	64	33	97
23	Davr-Bank	704	-	704
24	Credit Standard Bank	34	215	249
25	Invest Finance Bank	1028	431	1459
26	Amirbank	52	38	90
27	Asia Alliance Bank	610	329	939
28	Hi-Tech Bank	298	82	380
29	Orien Finans Bank	396	502	898
	TOTAL	**42098**	**106925**	**149023**

Fig. 7 shows [19], [20], the number of ATMs and information terminals for 100,000 adults have so fast grown; the development of non-cash bank payment system was not silky. However, the growth rate of bank cards on an annual basis is much faster than the initial increase in ATM cards.

In general, Uzbekistan's prudent and cautious approach seems to have achieved its goal. It helps to avoid the double crises faced by most economies in transition, thereby protecting social stability and reducing the negative impact of structural reforms on employment and economic growth. The change in state ownership, the introduction of credit bureaux and mortgage registration, and the rapid development of non-cash payment methods show that the banking industry is gradually being integrated into market-based systems.

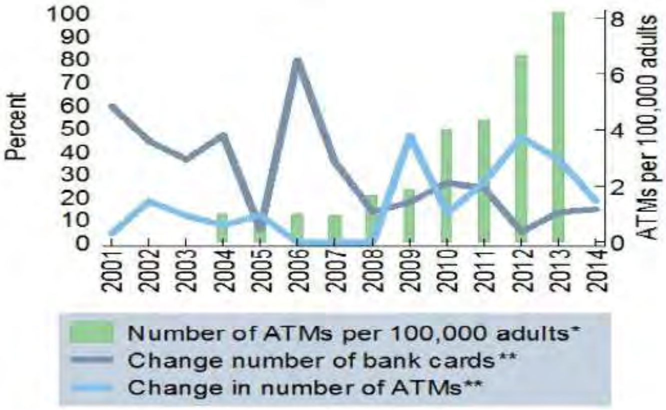


Fig. 7. Bank Cards and ATMs

X. CONCLUSION

For today, online banking is one of the modern tools, which allow banks to increase their profitability and increase their profitability client base. This article examines the world-wide issues and challenges online banking as well as an overview of the current state of online banking in Uzbekistan. The Uzbek banking system remains under State control through a series of regulatory measures, legislation, declarations and complex practices. Most bank assets are still in state-owned or state-controlled banks, and most of the loans are directed by the government or directed to develop a pre-determined industrial sector. By limiting the role of banks as a financial intermediary to reform the slow financial system, it limits the ability of citizens and private companies to access credit and other financial services

This work is to classify and analyze the Security issues and challenges in Mobile banking in Uzbekistan. The majority of the customers in Uzbekistan are using online banking or ATM. However, around 40 % of customers are using mobile banking where the remaining people 60% are not using this technology.

ACKNOWLEDGMENT

This work was supported by the Institute for Information and Communications Technology Promotion (IITP) grant funded by the Korea government (MSIT) (No.2018-0-00245), And it was also supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science, and Technology (grant number: NRF2016R1D1A1B01011908).

REFERENCES

[1] Customer adoption of banking technology: the case of uzbekistan . *International Journal of Bank Marketing* vol.pp.15-25

[2] A. D. Bank, "Technical assistance to the Republic of Uzbekistan for Development of the capital market Uzbekistan, Manila: *ADB*, 2017.

[3] A.V. Akimov, and B. Dollery. "Uzbekistan's Financial System. An Evaluation of Twelve Years of Transition." *Problems of Economic Transition* 48, no. 12, pp. 6–31, 2017

[4] K.D. Ghosh, S.C Ruziev. "Analysis of Mobile banking Economic Performance in Uzbekistan" vol 26.no.1, pp. 7-30

[5] https://m.hamkorbank.uz/en.The History of the Banks in Uzbekistan

[6] I.A.BOQIYEV, "Research on Security Payment Technology Based on Mobile Phones" , pp. 1-4, 2017

[7] Click system in Uzbekistan in 2011-2018. Annual report of central bank in Uzbekistan . https://click.uz/, http://www.gov.uz/government/cbu/cbu_0.htm

[8] A.V.Vahobov "Public key infrastructure for mobile banking security" vol 66.no.2, pp 12-20, 2015

[9]. J. Nie and X. Hu. "Mobile Banking Information Security and Protection Methods", *International Conference of Computer Science and Software Engineering*, , pp. 587-590, 2008.

[10] C. Narendiran, S. Albert Rabara, and N. Rajendran. Public key infrastructure for mobile banking security, *Global Mobile Congress*, pp. 1-6,2009.

[11] I. Brown, Z. Cajee, D. Davies, and S. Stroebel, "Cell phone banking: predictors of adoption in South Africa--an exploratory study, *International Journal of Information Management*,Vol.23, pp. 381-394, Oct.2003.

[12] D. Y. Liou, "Four - scenario analysis for mobile banking development contextualized to Taiwan", *Management of Engineering & Technology, PICMET*, pp. 2634-2642, 2008.

[13]. H. Wu, A. Burt, and R. Thurimella. Making secure TCP connections resistant to server failures, *Computer Security Applications Conference*, Proceedings. 19th Annual, pp. 197-206,2003.

[14]. H. Harb, H. Farahat, and M. Ezz. SecureSMSPay "Secure SMS Mobile Payment model", *Anti - counterfeiting, Security and Identification ASID*, pp. 11- 17,2008.

[15] T. Wilson, ― Malicious mobile ode, ‖ Internet Business, pp. 52-3, Feb.1999.

[16] T. Holz, M.Engelberth, F. Freiling," Learning More about the Underground Economy", *ESORICS*, LNCS 5789, pp. 1–18, 2009

[17] Tashkent, Uzbekistan, April, 2013 "Over 149,000 users use distance banking services " https://www.uzdaily.com/articles-id-22798.htm

[18] I. Kušt., "Securing mobile banking on Android with SSL certificate pinning" March 12th, 2014 https://infinum.co/the-capsized-eight/securing-mobile-banking-on-android-with-ssl-certificate-pinning

[19] M.Ahunov.,"Uzbek banking system: some history and current state" July 26,2015,
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2636002

[20] A. Abdullaev, M. A. Al-Absi, A. A. Al-absi, M. Sain, H. J. Lee" Security Challenge and Issue of Mobile Banking in Republic of Uzbekistan: A State of Art Survey" *International Conference on Advanced Communications Technology (ICACT)* February 17 ~ 20, 2019

[21] Uzbekistan-bankingsystems
https://www.export.gov/article?id=Uzbekistan-Banking-Systems/ 2019

AZamjon Abdullaev was born in Uzbekistan 1992, received his BS degree in finance from Tashkent financial Institute in Uzbekistan 2011-2015. Currently, he is a Master candidate student in the Department of Computer Engineering at Dongseo University, Korea. His research interests include Mobile Banking, Wireless Sensor Networks, Cryptography, and Network Security.

Mohammed Abdulhakim Alabsi was born in Yemen 1987, received his BS in Computer Application from Bangalore University in India. He earned his (MS) degree at Dongseo University, South Korea in 2018. Currently, he is a PhD. student in the Department of Information and Communication Engineering at Dongseo University, South Korea. His research interests include IoT, VANET, UAV, artificial intelligence, cryptology, network security, computer networks and digital communications.

Ahmed Abdulhakim Al-Absi was born in Yemen 1984, he is an Assistant Professor and Head of Smart Computing Department at Kyungdong University – Global Campus in South Korea. He earned his PhD in Ubiquitous Computing at Dongseo University, South Korea in 2016. His research interests include database systems, big data, hadoop, cloud computing, distributed systems, parallel computing, high-performance computing, VANET, and bioinformatics. He received a Master of Science (MS) degree in Information Technology at University Utara Malaysia, Malaysia in 2011 and a Bachelor of Science (BS) degree in Computer Applications at Bangalore University, India in 2008.

Mangal Sain was born in India 1979, received the M.Sc. degree in computer application from India in 2003 and the Ph.D. degree in computer science in 2011. Since 2012, he has been an Assistant Professor with the Department of Computer Engineering, Dongseo University, South Korea. His research interest includes wireless sensor network, cloud computing, Internet of Things, embedded systems, and middleware. He has authored over 50 international publications including journals and international conferences. He is a member of TIIS and a TPC member of more than ten international conferences.

HoonJae Lee was born in Korea 1962, received his BS, MS, and Ph.D. degrees in electronic engineering from Kyungpook National University, Daegu, Rep. of Korea, in 1985, 1987, and 1998, respectively. He is currently a professor in the Department of Information Communication Engineering at Dongseo University. His current research interests include Password Theory, Network Security, Side-Channel Attack, and Information Communication/Information Network.

Volume 8 Issue 3, May. 2019, ISSN: 2288-0003

ICACT-TACT JOURNAL

GIRI
Global IT Research Institute

1713 Obelisk, 216 Seohyunno, Bundang-gu, Sungnam Kyunggi-do, Republic of Korea 13591
Business Licence Number : 220-82-07506, Contact: tact@icact.org Tel: +82-70-4146-4991