IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received October 6, 2018, accepted November 28, 2018, date of publication December 3, 2018,
date of current version December 31, 2018.

*Digital Object Identifier 10.1109/ACCESS.2018.2884488*

# Neutralizing BLE Beacon-Based Electronic Attendance System Using Signal Imitation Attack

**MOONBEOM KIM, JONGHO LEE, AND JEONGYEUP PAEK, (Senior Member, IEEE)**
School of Computer Science and Engineering, Chung-Ang University, Seoul 06974, South Korea

Corresponding author: Jeongyeup Paek (jpaek@cau.ac.kr)

This research was supported by the Chung-Ang University Graduate Research Scholarship in 2018 and in part by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education under Grant NRF-2017R1D1A1B03031348.

**ABSTRACT** Many emerging location- or proximity-based applications use Bluetooth low energy (BLE) beacons thanks to the increasing popularity of the technology in mobile systems. An outstanding example is the *BLE beacon-based electronic attendance system* (*BEAS*) used in many universities today to increase the efficiency of lectures. Despite its popularity and usefulness, however, *BEAS* has not been thoroughly analyzed for its potential vulnerabilities. In this paper, we neutralize a university's *BEAS* by maliciously cheating attendance (i.e., faking attendance while the subject is not physically present at the location) in various scenarios using signal imitation attack, and investigate its possible vulnerabilities. The *BEAS* exploited in this paper is a commercial system actually used in a well-known university. After the exploitation experiment, we analyze the system's weaknesses and present possible counter-measures. Furthermore, additional attack methods are shown to re-counteract those possible counter-measures and to discuss the fundamental challenges, deficiencies, and suggestions in electronic attendance systems using BLE beacons.

**INDEX TERMS** Proximity-based application, electronic attendance systems, Bluetooth low energy, BLE beacon, vulnerability analysis.

## I. INTRODUCTION AND RELATED WORK

Bluetooth Low Energy (BLE) [1], [2] has enjoyed increased attention and popularity in the recent years, especially for mobile systems. This led to a plethora of applications to be developed with the technology. One large body of those are various location or proximity detection based applications that use low-cost low-complexity BLE transmitters called *"BLE beacons"*. These applications include promotional activities for indoor shopping in department stores [3], [4], information services for exhibitions and museums [5]–[7], mobile financial transactions [8], [9], indoor guidance systems [10], [11], and child-loss prevention services [12], [13].

*BLE beacons* can also be used for automating attendance checks. Teaching time in large lecture classes tend to be cut short due to the lecturer calling out student names to check attendances. For this reason, many universities today adopted automated *BLE beacon-based electronic attendance system* (*BEAS*) to increase the efficiency of lectures [14]–[18]. BLE beacons placed in classrooms periodically broadcast beacon messages, and nearby smartphones scan the signal. Then, students can check-in for attendance by using a *BEAS* mobile app which receives the BLE beacon messages and sends them to the university's *BEAS* server. Upon receiving the message from the mobile app, server validates the attendance request and determines whether the subject student is present at the proper lecture (time- and location-wise) by checking its lecture and student database [19], [20]. *BEAS* not only decreases the time spent on calling names to check student attendance, but also aims to prevent illegal attendance of a student fake attending on behalf of his/her friend, which enforces university's honor policies. Several related commercial products already exist [21]–[26].

Despite its popularity and usefulness, however, *BEAS* has not been thoroughly analyzed for its potential vulnerabilities. For example, an obvious but noticeable one would be checking attendance from a nearby place (e.g., hallway, adjacent classroom) outside of the classroom. To overcome this problem, prior work has proposed methods to check

whether the student is inside the intended classroom by using RSSI values and trilateration techniques [27], [28]. Albeit a useful approach, however, signal strength from BLE beacons vary significantly in different environments and can lead to errors [29], [30]. There are related work that attempts to address the problem by enhancing the accuracy of localization [28], [31], [32]. However, most of prior work only focuses on preventing the attacker from exploiting *BEAS* from nearby locations and does not consider the possibility of the *attacker imitating BLE messages* to check attendance illegally.

In this paper, we neutralize a university's *BEAS* by maliciously cheating attendance (i.e. faking attendance while the subject is not physically present at the location) in various scenarios using *"signal imitation attack"*, and investigate its possible vulnerabilities. The *BEAS* exploited in this work is a commercial system actually being used at Chung-Ang University.[1] We exploit the system having no pre-acquired knowledge of its internal workings, and we do not manipulate the official mobile app used to check attendance. After the exploitation experiment, we analyze the system's weaknesses and present possible counter-measures. Furthermore, additional attack methods (of cheating attendance) such as *forwarding and replaying BLE beacon messages* from classrooms to attackers at distant locations (e.g., home, coffee shops) are shown to re-counteract those possible counter-measures and expose additional vulnerabilities. Through this investigation, we discuss the fundamental challenges, deficiencies, and suggestions in electronic attendance systems using BLE beacons.

The remainder of this paper is structured as follows: We first analyze each classroom's BLE beacon signals to explore the system's vulnerabilities in Section II. Then we exploit (i.e., illegal attendance) the system by *imitating the beacon signals* using *programmable BLE beacon (PBB)* in Section III. In Section IV, we propose various counter-measures to the vulnerabilities shown in Section II and III, and also present additional possible attack methods against the proposed counter-measures. We summarize the vulnerability analysis and attack methods of current *BEAS* in Section V, and conclude the paper in Section VI.

## II. *BEAS* BEACON SIGNAL COLLECTION AND ANALYSIS

Before the actual exploitation experiments can be designed, an investigation and analysis of the BLE electronic attendance system in Chung-Ang University is necessary. For this purpose, a simple *BLE beacon scanner software* is written and used to collect information from the BLE beacons in the attendance system. Information such as the number of beacons in a classroom, message contents, transmission periods, and RSSI values were obtained and examined to determine which vulnerabilities the system may possess.

We first use the scanner software to investigate whether the messages emitted from the BLE beacons change over time and lecture schedule. To accomplish this, we collected BLE beacon signals from 10 different classrooms twice a day over the course of three days. After collecting data from the scans, we were able to uncover that there are two BLE beacons (1A, 1B) per each normal-sized classroom and four BLE beacons (1A, 1B, 2A, 2B) per each large-sized ones for all classrooms that we have collected data from. Also, the messages emitted from each BLE beacon were consistent regardless of time or scheduled lecture (or lack thereof). In other words, a *BEAS* BLE beacon always broadcasted the same message regardless of time or lecture.

**TABLE 1. HW-names of *BEAS* BLE beacons installed in classrooms 618 and 728.**

| Building number | Class room | Beacon ID | HW-Name |
|---|---|---|---|
| 310 | 728 | 1A | CA00 **310** A0 **728** - **1A** |
| | | 1B | CA00 **310** A0 **728** - **1B** |
| | 618 | 1A | CA00 **310** A0 **618** - **1A** |
| | | 1B | CA00 **310** A0 **618** - **1B** |

Furthermore, *the beacon identifier (HW-name) and the contents of beacon messages connoted a predictable pattern of information*. First of all, TABLE 1 shows the hardware names of each BLE beacon in two classrooms. We were able to deduce that every BLE beacon in *BEAS* has its unique identifier (*HW-name*) that includes the building number (e.g., 310), classroom number (e.g., 728), and a distinguishing beacon ID (e.g., 1A, 1B) in plain text.

**TABLE 2. Message contents from *BEAS* BLE beacons installed in classrooms 618 and 728.**

| Data set \ Beacon | | 618 | | 728 | |
|---|---|---|---|---|---|
| | | 1A | 1B | 1A | 1B |
| Beacon Prefix | Adv Flags | 0x020102 | | | |
| | Adv Header | 0x0303 | | | |
| | Company ID | 0x0F18 | | | |
| | Beacon Type | 0x02 | | | |
| | Beacon Length | 0x0A | | | |
| UUID | | 0x0010094341 303033313041 303631382D | | 0x0010094341 303033313041 303732382D | |
| Major | | **0x3141** | **0x3142** | **0x3141** | **0x3142** |
| Minor | | 0x1009 | | | |
| TX-power | | 0x43 | | | |

Secondly, TABLE 2 shows the contents of the data packets emitted from BLE beacons in the attendance system. The BLE beacon packet format following the Bluetooth 4.0 standard is depicted in Figure 1 for reference. As shown in TABLE 2, *prefix*, *minor*, and *TX-power* values were the same across all beacons, but the *major* values were varying according to the in-room beacon ID. For example, if a beacon was assigned '1A' as an in-room ID, this particular beacon's *major* value will be $0 \times 3141$, the exact ASCII code value

[1] http://www.cau.ac.kr. Private university located in Seoul, ranked ∼8*th* in Republic of Korea, and enrolls ∼16000 undergraduate students.

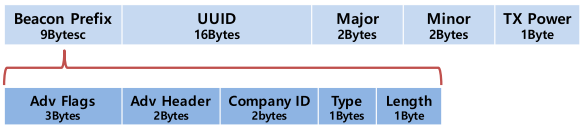


**FIGURE 1.** Packet format structure of a BLE beacon data packet.

of two-character string '1A'. Obviously, if the in-room ID is '1B', the beacon's *major* value will be $0 \times 3142$. Thus, the *major* values of all the BLE beacons can be predicted as follows: $2A = 0 \times 3241$, $2B = 0 \times 3242$, $3A = 0 \times 3341$, and so on.

| | Building number | | Class room | |
|---|---|---|---|---|
| 00100943413030 | **323033** | 4130 | **343035** | 2D |
| 00100943413030 | **323033** | 4130 | **333035** | 2D |
| 00100943413030 | **333033** | 4130 | **323034** | 2D |
| 00100943413030 | **333130** | 4130 | **363136** | 2D |
| 00100943413030 | **333130** | 4130 | **363138** | 2D |
| 00100943413030 | **333130** | 4130 | **373239** | 2D |
| 00100943413030 | **333130** | 4130 | **373330** | 2D |
| | (310) | | (730) | |

**FIGURE 2.** Analysis of UUIDs from each classroom BLE beacon.

Next, the UUID of each classroom beacon is analyzed. Figure 2 presents the consistent pattern in the UUID where the building numbers and classroom numbers are inherent in the UUID. UUID's $8^{th}$ to $10^{th}$ byte hide the building number of the classroom (e.g., 203, 303, 310), and the $13^{th}$ to $15^{th}$ byte connote beacon's classroom number (e.g., 405, 305, 204), both in ASCII code. For example, $0 \times 333130$ translates to "310", and $0 \times 373330$ equals "730". Thus, it can be deduced that the UUID's $8^{th}$ to $10^{th}$ and $13^{th}$ to $15^{th}$ byte values can be predicted by the building and classroom the beacon is placed in. All other bytes in the beacon messages had the same values regardless of the beacon as long as they are in the same *BEAS*.

Lastly, we examine the RSSI measurements from beacon messages. RSSI values were measured at various places in and around a classroom as shown in Figure 3, for 2 minutes at each location, and average values are presented for each measurement point {a, b, c, d, e, f, g, and h}. When measuring the values from the hallway, classroom doors were closed. Figure 4 displays the number of beacon messages received at each point. The measurement results show that the average RSSI values from within the classroom are approximately -75.75dBm, and -93.3dBm when measured outside. Although weaker, it was possible to receive beacon messages from outside the classrooms.

In summary, we discovered that the beacon packets' contents stayed consistent regardless of time. Also, the beacon signals had predictable data contents adhering to a specific rule, and if aware of the rule, one could imitate the messages effortlessly. We identify these as potential vulnerabilities and term them each *"temporal consistency of beacon information"* and *"predictable pattern of beacon information"*. Lastly, the RSSI values measured from within and around the classroom shows that although the signal strength is weaker, messages emitting from the beacons can still be received and thus attackers can still cheat attendance from outside of the classroom. This attack which exploits the *"leakage of beacon signal"* vulnerability is termed *"near classroom attack"*.

## III. *BEAS* EXPLOITATION AND VULNERABILITY ANALYSIS

Based on the findings in the previous section, this section focuses on the process of exploiting a commercial electronic attendance system by checking attendance even if the attacker is not physically present in the classroom. Twenty undergraduate students were enlisted for help with the experiments to prove whether the exploit is viable with different subjects. Experiments were conducted on actual lecture classes during a regular semester.

### A. BEACON SIGNAL IMITATION ATTACK

To neutralize the *BEAS*, we implemented a custom *programmable BLE beacon (PBB)* using Arduino UNO and BLE module CC41-A, which can generate beacon signals that imitate those of the electronic attendance system based on the rules and patterns we found in the previous section. A simple software was written to emit the imitated signal upon the attacker's request, and a separate *configuration script* was used to generate beacon signals based on the enrolled class schedule of the attacker (a mapping between classroom, class hour, and day of a week). Transmission power was configured to maximum, and the transmission interval was set to 100 milliseconds which is what we have observed from the beacons in *BEAS*. We term this first version as *PBB-v1*. Figure 5 shows the diagram of *PBB-v1* initiating the exploit. The attacker places *PBB-v1* device(s) near his/her smartphone, and attempts to cheat attendance by tricking the *BEAS* mobile app to think that the imitated signals are from the actual BLE beacons in the classroom.

Experiments were conducted under the following three scenarios. First, two *PBB-v1* devices were used to imitate the BLE beacons for a regular-sized classroom, one for beacon 1A and another for 1B. The attacker was in the same building as the classroom, but on a different floor to make sure that it only receives the signals from *PBB-v1* and not from the actual BLE beacons in the intended classroom. Second set of experiments were conducted at a classroom in a different building to examine whether other factors such as GPS or WiFi based positioning of the smartphone contribute to the attendance checking process. This experiment can uncover whether the building's WiFi APs or GPS location have a role in verifying attendance. Lastly, a series of additional experiments were conducted using only a single *PBB-v1* imitating only one of the 2 (or 4) *BEAS* beacons (i.e., beacon with identifier 1A or 1B). This is similar to Figure 5, but with only one PBB.

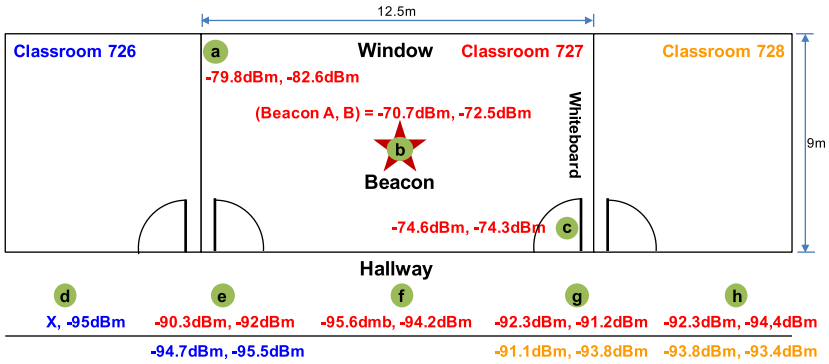


**FIGURE 3.** BLE beacon RSSI measurements at various locations in classroom 727.

| Location \ Classroom | | 726 | | 727 | | 728 | |
|---|---|---|---|---|---|---|---|
| | | A | B | A | B | A | B |
| Classroom | a | - | - | 77 | 74 | - | - |
| | b | - | - | 79 | 78 | - | - |
| | c | - | - | 78 | 70 | - | - |
| Hallway | d | - | 3 | - | - | - | - |
| | e | 15 | 4 | 55 | 36 | - | - |
| | f | - | - | 23 | 14 | - | - |
| | g | - | - | 49 | 52 | 41 | 27 |
| | h | - | - | 58 | 29 | 43 | 27 |

**FIGURE 4.** Number of received beacon packets at each location.

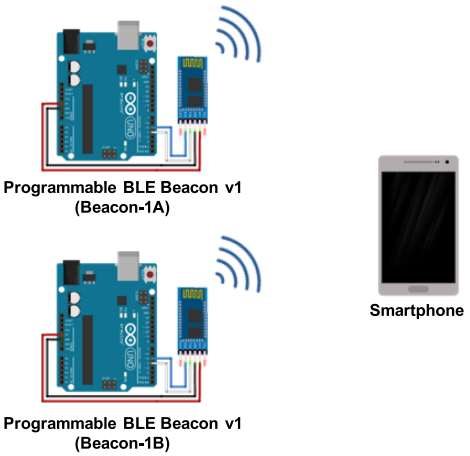


**FIGURE 5.** Diagram of beacon signal imitation attack experiment.

Illegal attendance was successful in all three scenarios, with a 100% success rate for all 20 actual undergrad students. This was true even if only one *PBB-v1* imitator was used for a classroom. Experimental results have shown that the university's electronic attendance system relies only on the BLE beacon signals (not on GPS or WiFi signals), and only one signal among multiple beacons in a classroom is sufficient to check-in for attendance. We term this *"single proximity vulnerability"* henceforth. Thus, it can be concluded that the electronic attendance system at Chung-Ang University can be easily exploited by imitating the BLE beacon signals alone.

### B. MULTIPLE CLASSROOM SIMULTANEOUS ATTACK

Next, we investigate whether a single *PBB* can be used to check attendance for multiple lectures simultaneously (e.g. ten students enrolled to ten different lectures at identical class time). We term this as *"multiple classroom simultaneous attack"*. For this purpose, we implemented *PBB-v2* which emits beacon signals of multiple classrooms (almost) simultaneously.

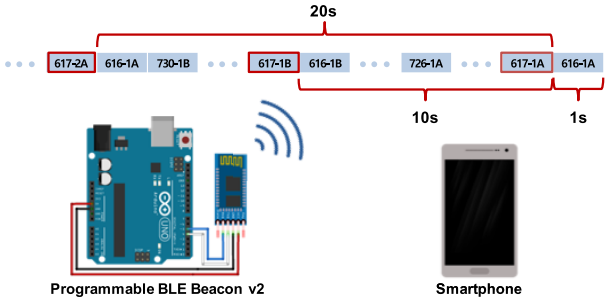


**FIGURE 6.** Diagram of the experiment which checks the time interval and delay using programmable BLE beacon v2.

Figure 6 shows the operation process. First, the attacker configures a total of $2N$ beacon information from $N$ classrooms in a configuration script. Then, *PBB-v2* creates timeslots for the beacon messages and assigns each one of $2N$ messages to a timeslot sequentially. *PBB-v2*'s transmission power and transmitting interval (between time slots) was configured the same as before. At every time slot, *PBB-v2* updates its beacon information according to the configuration script, and transmits the beacon message. This process is repeated for the duration of each class hour.

However, there was one challenge where a small reset delay was required every time we change the BLE module's configuration. This led to an occasional problem in which some beacon information was not updated when there isn't enough time for the modify command to take place. For this reason, fastest rate for *PBB-v2*'s information update is once per every 100ms. Also, to provide sufficient time for *PBB-v2* to emit its updated information at least a few times, a time

interval of 900ms was given after each re-configuration. In other words, *PBB-v2* updates the classroom information and emits its updated message every 1 second. If the configuration file holds $2N$ beacon information, it will take $2N$ seconds to emit all its beacon information. If we assume every classroom has 2 beacons (beacon-1A and 1B), it will take $N$ seconds to emit attendance signals of $N$ classrooms. Thus a student will receive his/her attendance signal every $N$ seconds. In our experiments, we used 10 different classrooms ($N = 10$).

Two variables must be taken into account in this scenario. First, a student's smartphone will be exposed to other classrooms' beacon signals. Second, there will be delays (of $N$ seconds) in and between receiving the student's correct lecture attendance signals. To see how much these two variables influence *"multiple classroom simultaneous attack"*, 20 undergraduate students' help was enlisted.

Experimental result was that 19 students out of 20 were able to check-in illegal attendance successfully, a 95% success ratio. This means that multiple students can cheat attendance simultaneously by creating a single custom built *PBB*. Receiving other beacon signals from unintended classrooms did not interfere with the attendance check as long as the beacon signal from the intended classroom can be received during a scanning interval. We name this vulnerability *"non-interference of other beacon signal"*.

Among the successful 19 students, however, some students took slightly longer than others. Also, iPhone users experienced unusual behavior where the mobile app alternated between displaying "`able to check attendance`" and "`unable to check attendance`" repeatedly. Although iPhone users were able to check attendance by clicking on the "`able to check attendance`" button before it alternated to displaying "`unable to check attendance`", the added delay is worth noting and we discuss them in Section III-C.

The interesting question was, "what's going on with the one student?". The one student that was unable to check attendance using *PBB-v2* was able to illegally check attendance with *PBB-v1*. We conjectured that BLE scanning intervals may differ across various smartphone manufacturers and operating system versions, and reducing the inter-beacon time (of intended messages) may resolve the problem. To verify, we additionally created a *PBB-v2.1* which can emit multiple beacon signals at a faster rate by using two CC41-A Bluetooth modules, each named 'A' and 'B'. *PBB-v2.1* attempts to overcome the aforementioned problem by making the additional Bluetooth module (module-B) repeat module-A's signal 5 seconds after module-A emits the signal, thus allowing students to receive their corresponding attendance signal every 5 seconds. Figure 7 depicts a diagram of *PBB-v2.1*'s operation, and we conducted experiments with another 20 undergraduate students. Unlike our expectation, however, one (out of 20) student was still unable to check attendance with *PBB v2.1* while other 19 students had no problem.

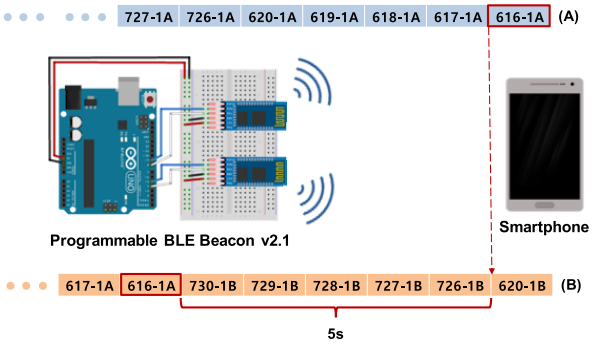


**FIGURE 7.** Diagram of the experiment which checks the time interval and delay using programmable BLE beacon v2.1.

### C. INFLUENCE OF BLE SCANNING BEHAVIOR

After investigation, we identified that the two students[2] who were unable to check attendance used older generations of smartphones (Samsung Galaxy Note 2 and a low-cost mobile phone). In particular, we found out that Samsung Galaxy Note 2's Android BLE scanning procedure pauses after scanning once for nearby Bluetooth devices. Thus, we conjectured that Bluetooth device scanning behavior differs across smartphone manufacturers and Android OS versions. To accurately analyze the problem, the following facts should be considered: our *PBB*'s BLE module is configured as *"connectable mode"*, and Samsung Galaxy Note 2 supports *Android version 4.1 to 4.4*.

*Why do Some Students Take More Time Than Others to Check Attendance?:* When a device scans a BLE beacon that is operating under *"connectable mode"*, the beacon must send scan responses to the scan request messages. Thus, the BLE beacons send advertising packets and scan responses (almost) simultaneously, and this occurs for several tens of devices (in our experiment, 20 students) resulting in collision and interference. This causes some devices that scan these beacons to not receive the beacon's information. In our experiments, it was because of this phenomenon that some students took more time to check attendance than others. We have verified this by reducing the number of contending students.

*Why Are Some Students Unable to Check Attendance?:* When smartphones with *Android version 4.3* scan for *"non-connectable mode"* beacons, they get multiple callbacks. When these smartphones attempt to scan *"connectable mode"* beacons, they get only one callback sequence per scanning cycle. On the other hand, Android smartphones with *versions 5.0 or above* can continuously get multiple callbacks regardless of BLE beacon mode. In our experiments, smartphones with Android version 4.3 or earlier cannot update the *PBB* information via scanning since they get only one callback per scanning cycle. Thus, students with lower Android versions may not be able to check attendance using *PBB-v2* and *v2.1* when their smartphones' scanning intervals

[2]Two different students, one from *PBB-v2* experiment and another from *PBB-v2.1* experiment.

do not coincide with the *PBB*'s emitting interval. If we switch the *PBB* to *"non-connectable mode"*, students with lower Android versions are able to check attendance.

In summary, multiple students can exploit the BLE beacon-based electronic system simultaneously by creating a single custom built *"non-connectable mode" PBB* that emits beacon signals imitating several beacons in multiple classrooms sequentially *("multiple classroom simultaneous attack")*. Receiving other beacon signals from unintended classrooms does not interfere with the attendance check process as long as the beacon signal from the intended classroom can be received during a scanning interval. We name this vulnerability *"non-interference of other beacon signal"*.

## IV. COUNTER-MEASURES AND ADDITIONAL EXPLOITS

In this section, we build upon the empirical results from Section II and Section III to devise counter-measures for checking illegal attendance. Furthermore, additional attack methods are shown to re-counteract those possible counter-measures and to discuss the fundamental challenges, deficiencies, and suggestions in electronic attendance systems using BLE beacons.

### A. INDOOR LOCATION-BASED EAS

There are prior work that proposes solutions based on indoor localization techniques, beyond simple proximity, to prevent cheating of electronic attendance [27], [28]. We label these methods as *"indoor location-based EAS (ILB-EAS)"*. Most of the *ILB-EAS* methods utilize RSSI values from carefully placed BLE beacons (and their pre-acquired locations) to localize the student checking attendance. If and only if the student is determined to be inside the intended room based on the localization result, the *BEAS* validates attendance for the student. This enforces the student to be physically present in the classroom while checking attendance, and thus, *ILB-EAS* methods can prevent *near classroom attack* and cover *single proximity vulnerability*.

However, since the student's smartphone itself scans for *BEAS* BLE beacons, simply using the same number of *PBB* devices as with the classroom BLE beacons and imitating them is sufficient to illegally check attendance. The only inconvenience and cost for the attacker is that now he/she must create multiple *PBB* devices and place them in a similar layout as with the classroom BLE beacons. Still, this cost to the attacker would be significantly less than the added cost and complexity of ILB-EAS itself compared to current *BEAS*.

Other positioning methods such as GPS or WiFi-based can be considered as well. However, obviously, *BEAS* cannot rely on GPS since *BEAS* targets indoors. Augmenting with WiFi-based positioning is a viable option, but will incur significant cost and complexity to the deployment and maintenance of the system. Furthermore, note that we assume no modification nor hacking of the official mobile app of the *BEAS*. If possible, one can simply fake the location within the app. In addition, through packet capture tools, we noticed that the attendance request messages sent from the official mobile app to the *BEAS* server are *"unencrypted"*. Thus, it is also possible to launch a *"man-in-the-middle attack"* where the attacker manipulates the information within the request packets.

### B. MAC ADDRESS VERIFICATION

A simple method to defend against attacker imitating BLE beacons may be to verify the *MAC address* of the scanned BLE beacons. This method enforces the attendance checking mobile app to send the scanned beacon's MAC address to the *BEAS* server, and the server validates it with the BLE beacon information database. Implementing the verification procedure and maintaining a MAC address database should not add significant cost to the *BEAS*. Thus, since each device should (ideally) have a unique MAC address, it seems to be a viable way to prevent imitation attacks.

However, not all BLE devices have unique MAC addresses. For example, in our previous exploitation efforts, CC41-A BLE modules were used which is relatively easy to acquire for students and has fixed MAC addresses. On the other hand, for example, *BLE Nano* [33] offers end-users freedom over multiple aspects including reconfigurable MAC addresses. To verify if an attacker can change the MAC address in a way to exploit the *BEAS*, we used the *Mbed's Bluetooth Low Energy API* [34] to change the MAC address of BLE Nano. Indeed, our experiments have confirmed that *MAC address verification* method can be disarmed by *"MAC imitation attack"* which uses MAC-reconfigurable devices to also imitate the MAC addresses of the system's BLE beacons. Thus, *MAC address verification* cannot deter dedicated attackers from checking illegal attendance.

### C. TIME-VARYING RANDOM VALUE

We propose using *"time-varying random value" (TVRV)* to overcome the vulnerabilities mentioned in the previous sections. An epitome of *TVRV* technique is the use of one-time passwords (OTP)[3] in various electronic financial transactions. If the BLE beacons can generate time-varying pseudo-random signal unpredictable by the attacker, then the *"temporal consistency of beacon information"* and *"predictable pattern of beacon information"* vulnerabilities are dismissed, and *"signal imitation attack"* can be neutralized to be no longer effective.

There are two possible representative ways in using *TVRV*. First method is to command the BLE beacons in each classroom to generate a random value per lecture-timeslot and use it to calculate its beacon information (e.g., UUID, major, minor) based on that time-varying random value. When a student's smartphone scans and receives the beacon signal, it sends the message to the *BEAS* server which can then verify whether the received information is valid. As long as the server knows the identity of the beacon (and time), it can reproduce the *TVRV*. However, every BLE beacon in

[3]One-time passwords (OTP) are created as a solution to vulnerabilities regarding static password-based authentication. These often use two-factor authentication by augmenting PINs with OTP calculators fitted with randomly generating values.

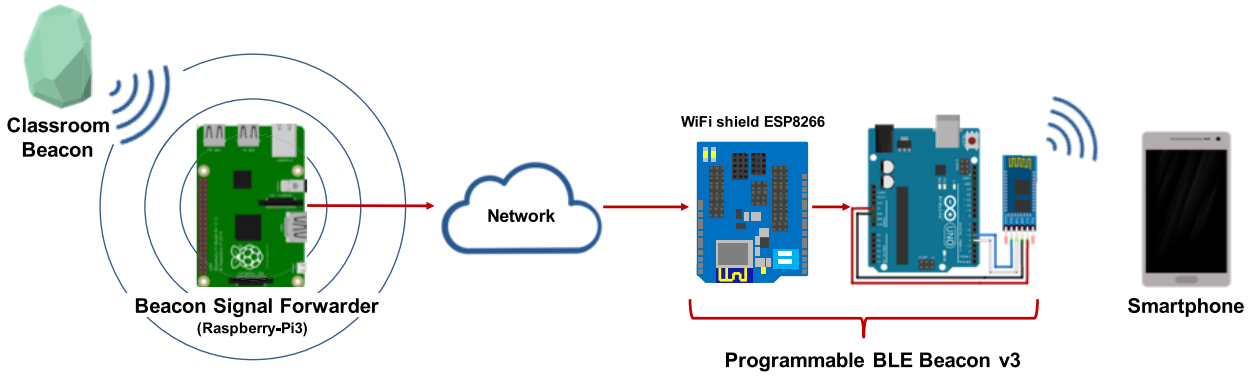


**FIGURE 8.** A plausible *"real-time beacon signal forwarding and replay"* attack using *beacon signal forwarder (BSF)* for counter-acting *"time-varying random value" (TVRV)* technique.

the system must be time-synchronized for the technique to be valid. This may compromise a significant advantage of the BLE beacons: its simplicity and cost-effectiveness. Also, the overall complexity of the *BEAS* will increase, which in turn increase the cost of maintenance.

Second *TVRV* method is to have the *BEAS* server create a random value per lecture timeslot and send it to the BLE beacons. BLE beacons can use the random value received from the server to modify its emitting signal. This method eliminates the need for clock synchronization. However, the major drawback is that the system's BLE beacons must be network-connected to the *BEAS* server, which may add significant installation cost not to mention IP addresses.

The two methods mentioned above follow the same fundamental principle of using randomly generated values per timeslot. Each beacon updates its emitting signal according to the generated value, and they are sent to the *BEAS* server for validation of attendance request. The following examines the vulnerabilities remaining in the system after adopting *TVRV* method from an attacker's standpoint.

An attacker seeking to check illegal attendance can no longer guess the time-varying pseudo-random message and will need to know what the current message is. A simple way to accomplish this is to acquire the current signal in that particular classroom at that specific time. For this purpose, an attacker can implement *beacon signal forwarder (BSF)* using a RaspberryPi-3 that can collect BLE beacon signals and forward it to the attacker at distant location in real time over the Internet. *BSF* can be placed in the intended classrooms since the attacker is a legitimate student who can have access to the university's WiFi and power outlet in the classroom. For the attacker to receive the beacon signal at a distant location over the Internet, *PBB* can be equipped with a WiFi interface. We term this PBB as *PBB-v3* and use it in a series of experiments to determine if this method is a viable way to exploit the attendance system.

Figure 8 illustrates *"real-time beacon signal forwarding and replay attack"* to neutralize *TVRV* techniques. A *BSF* is placed in a classroom, scans and collects BLE beacon signals in real-time, and forwards them to the attacker's *PBB-v3* over the Internet. When the *PBB-v3* receives the data, it replays (imitates) the attendance system's beacon signal based on the acquired/forwarded message. Overall, this exploitation technique disarms the *TVRV* method by relaying the current BLE beacon signals to the attacker, which then uses it to check attendance illegally. A drawback of this exploit is the fact that the attacker must build and place a number of *BSF*s in every classroom that he/she wants to check attendance for. Thus, this method is a costly attack compared to other previous techniques.

### D. MAJORITY VOTING

The *TVRV* method mentioned in subsection IV-C requires the BLE beacons to be either clock synchronized or connected to the network. This ultimately and significantly increases the cost and complexity of the *BEAS*. One way to circumvent this drawback is to adopt a *majority voting* scheme. It is based on the intuition that there are many students in a lecture and the majority will be legit. That is, attackers will be the minority.

To further illustrate, the beacons in a classroom creates a randomly generated value $X$ and emits it without any synchronization nor coordination. Then, all the students in the classroom will receive the same value $X$ and send it to the *BEAS* server for attendance check. When the server receives value $X$ from multiple students for a particular classroom during a particular classhour, it assumes that the beacon at that classroom has generated $X$ at that lecture timeslot. The *BEAS* then can positively check attendance for the students that sent value $X$ without having prior knowledge of the randomly generated value. If an attacker attempts to check attendance illegally by generating a different random value $Y$, *BEAS* can detect the exploitation attempt and ignore the attendance request.

This method can reduce the cost and complexity of the *BEAS*. However, it cannot prevent the attacker from exploiting the system by forwarding and replaying beacon signals in real-time (i.e., *real-time beacon signal forwarding and replay attack*). Also, if more than half of

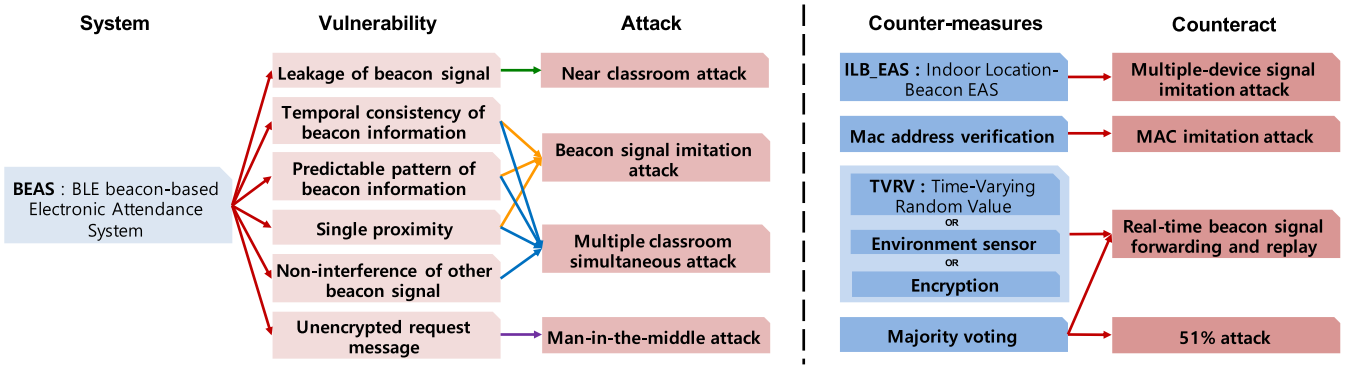


**FIGURE 9.** Vulnerabilities, attack methods, counter-measures, and additional counteracts for the BLE beacon-based electronic attendance system.

the students attending the lecture send a different random value $Y$ (a.k.a,*"51% attack"*), the *BEAS* server may mistakenly regard legitimate attendance requests as false requests (false negatives) and illegal requests as valid attendances (false positives).

### E. ENVIRONMENT INFORMATION SENSING

Another possible idea is to use the smartphone's sensors to read various information about its environment such as temperature, humidity, and lighting, and send those to the *BEAS* server. If the sensory data are consistent with those actually sensed in the classroom, attendance requests will be valid. This technique can prevent the *real-time beacon signal forwarding and replay* attack. However, the attacker can counter-act this defense by attaching additional sensors to the *BSF* and forwarding the sensory information along with the collected beacon signals to *PBB-v3*. The only challenge for the attacker would be to have prior knowledge of the type of sensors the *BEAS* requires. Furthermore, since the smartphones can be placed in pockets, bags, or on the desk, the environment sensor data can be different for even the legitimate students which will lead to high false negatives.

### F. OTHER POSSIBLE COUNTER-MEASURES

Other possible counter-measures that could be adopted are augmenting the *BEAS* with other technologies such as *QR code*, *NFC tag*, and *certification number*. There are multiple instances of universities, including Chung-Ang University, which uses one or more of these in their systems. *QR code* method requires students to scan the *QR code* displayed on small wall-mounted devices in classrooms to check attendance. *NFC tag* requires students to tag their ID card (or capable smartphone) to the card reader in the classrooms. Attendance by *certification number* requires the lecturer to call out a randomly selected number created during the lecture to the students, which in turn the students input to their *BEAS* mobile app to check attendance. Although orthogonal to *BEAS*, augmenting *BEAS* with the three mentioned techniques enforces the students to be physically present in the lecture room. However, they compromise the efficiency and convenience aspects of the BLE beacon-based electronic attendance system, which is the primary advantage and motivation of using such system.

Also, the presented technologies are susceptible to various out-of-band exploits. If the attendance system uses *NFC tags*, the attacker may enlist the help of a 3rd party person (e.g. a friend) to be present in the classroom and give the person his/her ID card to check attendance on their behalf. Similarly, *QR codes* can be captured by screenshots and sent to a 3rd party person to be scanned without the attacker being physically present in the classroom. *Certification numbers* can be relayed to a distant attacker with the help of a 3rd party person to cheat attendance. In conclusion, the mentioned technologies can augment existing electronic attendance systems, but can be exploited with the help of a 3rd party.

## V. VULNERABILITY ANALYSIS SUMMARY OF *BEAS*

This section summarizes the vulnerabilities, attack methods, counter-measures, and additional counteracts of BLE beacon-based electronic attendance system. Figure 9 concisely illustrates our summary.

Firstly, the vulnerabilities of *BEAS* and their corresponding attack methods are as follows.

*Leakage of beacon signal:*

Since beacon signal can be received from the vicinity (e.g., hallway, next classroom) of the designated classroom, an attacker can check attendance without being physically present in it $\Rightarrow$ ***Near classroom attack***.

*Predictable pattern of beacon information* +
*Temporal consistency of beacon information :*

An attacker can easily deduce the BLE beacon signal pattern by merely acquiring a small sample of beacon signals. Since each BLE beacon emits same signal regardless of time, the attacker then can use the rules to imitate such signals and cheat attendance using an unmodified *BEAS* mobile app $\Rightarrow$ ***Signal imitation attack***.

*Single proximity:*

Even though there are multiple BLE beacons in a classroom, signal from a single beacon is sufficient to cheat attendance ⇒ ***Single device signal imitation attack***.

*Non-interference of other beacon signal:*

Receiving multiple beacon signals other than the intended does not interference with the overall attendance verification process. Thus, a single device can be used to imitate signals of several beacons and launch an attack where multiple attackers can cheat attendance simultaneously ⇒ ***Multiple classroom simultaneous attack***.

*Unencrypted request message:*

Attendance check request messages from the *BEAS* mobile app to the server is unencrypted plain text. Thus, it is possible to manipulate the beacon information in that message and check attendance from a different classroom ⇒ ***Man-in-the-middle attack***.

Possible counter-measures and additional counteracts to disarm those counter-measures are as follows.

*ILB-EAS:*

Indoor localization based verification may protect *BEAS* to some extent by overcoming the *leakage of beacon signal* and *single proximity* vulnerabilities. However, it only increases the cost of the attack (by requiring more devices) without preventing it while adding significant cost and complexity to the defending system ⇒ ***Multiple-device signal imitation attack***.

*MAC address verification:*

Even if MAC address check is employed, it can be neutralized simply by using BLE modules that allow MAC address modification to imitate beacon's address ⇒ ***MAC imitation attack***.

*TVRV or environment sensor:*

Time-varying random value mechanism may be one of the strongest defense, but requires either time-synchronization or network connectivity which adds significant cost and complexity to the system. Even if some form of TVRV mechanism is adopted, the system is susceptible to attackers forwarding and replaying beacon signals at remote locations. Encryption is also susceptible to such attack, and utilizing environment sensors has the same problem with possibly more false negatives ⇒ ***Real-time beacon signal forwarding & replay attack***

*Majority voting:*

This can eliminate the time-sync or network connectivity cost of the system when using TVRV method, but is vulnerable when the attackers are the majority ⇒ ***51% attack***.

## VI. DISCUSSION AND CONCLUSION

In this work, we analyzed the vulnerabilities of a BLE beacon-based electronic attendance system (*BEAS*) and discussed its possible counter-measures. We neutralize a university's *BEAS* by maliciously faking attendance when the subject is not physically present at the intended location using various types of signal imitation attacks. For this purpose, we built several custom *programmable BLE beacon (PBB)* and *beacon signal forwarder (BSF)* devices which can imitate, forward to, and replay legitimate beacon signals at remote locations. After the experiments, we categorized various vulnerabilities the attendance system possesses, presented possible counter-measures to the problems, and discussed additional counter-acts that can disarm those counter-measures.

Our investigation have shown that there is no cost-effective way (yet) to defend against all possible attackers. There are ways to make the attack difficult and costly, but usually at the expense of added cost and complexity to the defending system as well. False negatives would cause significant frustration to legitimate students and the lecturer, and sacrificing the convenience aspect of *BEAS* is not an option since there would be no point in having the system in the first place. We believe that our work can provide a reference for future work intended to enhance and secure electronic attendance systems.

## REFERENCES

[1] *Bluetooth Core Specification Version 4.0, Specification of the Bluetooth System*, Bluetooth_SIG, Kirkland, WA, USA, 2010.

[2] C. Gomez, J. Oller, and J. Paradells, "Overview and evaluation of Bluetooth low energy: An emerging low-power wireless technology," *Sensors*, vol. 12, no. 9, pp. 11734–11753, 2012.

[3] Nemustech. (2018). *Indoor Location Tracking and Indoor Navigation Framework*. Accessed: Oct. 4, 2018. [Online]. Available: http://nemustech.com/business/solution/indoornow/

[4] Intellian_Systems. (2015). *Location Awareness O2O Solution Through That Applied the Beacon Technology, and Location Based Service Delivering the Advertisement and Information*. Accessed: Oct. 4, 2018. [Online]. Available: http://www.intelliansys.co.kr/LAB/lab-lbs.asp

[5] Z. He, B. Cui, W. Zhou, and S. Yokoi, "A proposal of interaction system between visitor and collection in museum hall by iBeacon," in *Proc. Int. Conf. Comput. Sci. Edu. (ICCSE)*, Jul. 2015, pp. 427–430.

[6] JejuNet. *Smart Docent Services*. Accessed: Oct. 4, 2018. [Online]. Available: http://jejunet.jejuns.com/docen/

[7] Y. Choi. (Jan. 2016). *Mobile App of National Museum of Korea That is Explain the Exhibit of Museum*. Accessed: Oct. 4, 2018. [Online]. Available: http://m.jungle.co.kr/magazine/articleView?searchBbsId=BBSMSTR_000000000001&searchNttId=23067

[8] H. Park. (Sep. 2013). *PayPal, Reveal the Bluetooth Mobile Payment Service*. Accessed: Oct. 4, 2018. [Online]. Available: http://www.zdnet.co.kr/news/news_view.asp?artice_id=20130910084454

[9] Y. Leem. (May 2016). *Beaconyx, Reveal the Slg-Money Which Easy-to-Use Payment System Using Beacon*. Accessed: Oct. 4, 2018. [Online]. Available: http://www.zdnet.co.kr/news/news_view.asp?artice_id=20160516114503

[10] L.-W. Chen, J.-J. Chung, and J.-X. Liu, "GoFAST: A group-based emergency guiding system with dedicated path planning for mobile users using smartphones," in *Proc. IEEE Int. Conf. Mobile Ad Hoc Sensor Syst. (MASS)*, Oct. 2015, pp. 467–468.

[11] G. Conte, M. De Marchi, A. A. Nacci, V. Rana, and D. Sciuto, "BlueSentinel: A first approach using iBeacon for an energy efficient occupancy detection system," in *Proc. ACM Conf. Embedded Syst. Energy-Efficient Buildings (BuildSys)*, 2014, pp. 11–19.

[12] S. Park. (Mar. 2015). *Missing Child Prevention, Beacon-Startup is Responsible*. Accessed: Apr. 11, 2018. [Online]. Available: http://www.zdnet.co.kr/news/news_view.asp?artice_id=20150320103954

[13] Lineable Inc. *Lineable Wearables*. Accessed: Oct. 4, 2018. [Online]. Available: https://www.lineable.net/

[14] Sookmyung_University. *Information the Smart Attendance(for Students)*. Accessed: Oct. 4, 2018. [Online]. Available: http://www.sookmyung.ac.kr/sookmyungkr/1229/subview.do

[15] Yonsei_University. *S-Campus Electronic Attendance System*. Accessed: Oct. 4, 2018. [Online]. Available: http://ibook.yonsei.ac.kr/Viewer/JODIF6GNK5A1
[16] Sogang_University. *Introduce the Electronic Attendance System*. Accessed: Oct. 4, 2018. [Online]. Available: https://www.sogang.ac.kr/smartsogang/m_card.html
[17] Sejong_University. *Electronic Attendance*. Accessed: Oct. 4, 2018. [Online]. Available: http://eng.sejong.ac.kr/contents/eng/cor/attendance.html
[18] Myongji_College. *Electronic Attendance System*. Accessed: Oct. 4, 2018. [Online]. Available: https://www.mjc.ac.kr/ibuilder.do?menu_idx=1944
[19] S.-W. Ahn, "Smart attendance checking system based on BLE using a beacon," *J. Korea Inst. Electron. Commun. Sci.*, vol. 11, no. 2, pp. 209–214, 2016.
[20] M.-Y. Bae and D.-J. Cho, "Design and implementation of automatic attendance check system using BLE beacon," *Int. J. Multimedia Ubiquitous Eng.*, vol. 10, no. 10, pp. 177–186, 2015.
[21] Beaconyx. *Efficient and Convenient Attendance Management Solution*. Accessed: Oct. 4, 2018. [Online]. Available: http://www.beaconyx.com/?page_id=535
[22] ABILITY_SYSTEMS. *Beacon Service (Indoor LBS)*. Accessed: Oct. 4, 2018. [Online]. Available: http://www.abilsys.com/sub02/?page_id=81
[23] Icerti. *University Solution Business*. Accessed: Oct. 4, 2018. [Online]. Available: http://www.icerti.com/02_business/business00.php?ptype=sub02_00
[24] Duoit. *Electronic Attendance*. Accessed: Oct. 4, 2018. [Online]. Available: http://duoit.co.kr/newhome/index.html
[25] Sitin. *Location Based UCheck Plus Attendance System*. Accessed: Oct. 4, 2018. [Online]. Available: http://www.sitin.kr
[26] SYMTRA. *U-Campus System*. Accessed: Oct. 4, 2018. [Online]. Available: http://www.symtra.co.kr/02_03_01_Ucampus.asp
[27] S. Noguchi, M. Niibori, E. Zhou, and M. Kamada, "Student attendance management system with Bluetooth low energy beacon and android devices," in *Proc. Int. Conf. Netw.-Based Inf. Syst. (NBiS)*, Sep. 2015, pp. 710–713.
[28] J. Paek, J. Ko, and H. Shin, "A measurement study of BLE iBeacon and geometric adjustment scheme for indoor location-based mobile applications," *Mobile Inf. Syst.*, vol. 2016, Oct. 2016, Art. no. 8367638.
[29] J. Fürst, K. Chen, H.-S. Kim, and P. Bonnet, "Evaluating Bluetooth low energy for IoT," in *Proc. 1st Workshop Benchmarking Cyber-Phys. Netw. Syst. (CPSBench)*, Apr. 2018, pp. 1–6.
[30] M. S. Aman, H. Jiang, C. Quint, K. Yelamarthi, and A. Abdelgawad, "Reliability evaluation of iBeacon for micro-localization," in *Proc. IEEE Annu. Ubiquitous Comput., Electron. Mobile Commun. Conf. (UEMCON)*, Oct. 2016, pp. 1–5.
[31] Y. Wang, X. Yang, Y. Zhao, Y. Liu, and L. Cuthbert, "Bluetooth positioning using RSSI and triangulation methods," in *Proc. IEEE Consum. Commun. Netw. Conf. (CCNC)*, Jan. 2013, pp. 837–842.
[32] P. Kriz, F. Maly, and T. Kozel, "Improving indoor localization using Bluetooth low energy beacons," *Mobile Inf. Syst.*, vol. 2016, Mar. 2016, 2083094.
[33] Redbearlab. *BLE Nano and MK20 USB BOARD*. Accessed: Oct. 4, 2018. [Online]. Available: http://redbearlab.com/blenano/
[34] Y. Pyo. (Jan. 2013). *Mbed Basic Lecture: 01. Introduction of Mbed*. Accessed: Oct. 4, 2018. [Online]. Available: https://os.mbed.com/users/passionvirus/notebook/basic1

**MOONBEOM KIM** received the B.S. degree in computer and information communications engineering from Hongik University in 2018. He is currently pursuing the master's degree in computer science and engineering, Chung-Ang University, Seoul, South Korea. He is also a Research Assistant at the Networked Systems Laboratory led by Dr. J. Paek.

**JONGHO LEE** received the B.S. degree in computer science and engineering from Chung-Ang University in 2018. He is currently pursuing the M.S. degree with the University of California at Irvine, Irvine, USA. He was a Research Assistant at the Networked Systems Laboratory, Chung-Ang University, led by Dr. J. Paek.

**JEONGYEUP PAEK** (SM'14) received the B.S. degree in electrical engineering from Seoul National University in 2003, and the M.S. degree in electrical engineering and the Ph.D. degree in computer science from the University of Southern California in 2005 and 2010, respectively. He was a member of the Networked Systems Laboratory led by Dr. R. Govindan. He was with Deutsche Telekom, Inc., R&D Labs, USA, as a Research Intern, in 2010, and then joined Cisco Systems, Inc., in 2011, where he was a Technical Leader with the Internet of Things Group, Connected Energy Networks Business Unit (formerly the Smart Grid BU). At Cisco, he was one of the lead engineers for CG-Mesh system and WPAN software. In 2014, he was with the Department of Computer Information Communication, Hongik University, as an Assistant Professor. He is currently an Associate Professor at the School of Computer Science and Engineering, Chung-Ang University, Seoul, South Korea.