International Journal of Security and Its Applications
Vol.9, No.1 (2015), pp.205-220
http://dx.doi.org/10.14257/ijsia.2015.9.1.21

$SBIS_{urban}$-Secure Urban Bus Information System based on Smart Devices

Donghyuk Park[1] and Hyunsung Kim[2*]

[1]*Dept. of Computer Engineering, Kyungil University*
[2]*Dept. of Cyber Security, Kyungil University*
[1]*eaeao@naver.com*, [2]*kim@kiu.ac.kr*

Abstract

Bus information system (BIS) has been developed for networking passengers with bus companies that provides public transportation services. The BIS, also denoted as $BIS_{generalized}$, supports a passenger with personalized and real time bus information services in all phases of a journey. Today's $BIS_{generalized}$ encompasses multiple technologies, including advanced visual displays, public address, emergency intercommunications, digital surveillance systems, IP networks, wireless networks, video streaming, coders, decoders and many more. These systems deliver real time bus information seamlessly on vehicles and in stations, while they are controlled and managed from a single control center. However, lots of small bus companies' services like urban city's bus company or small organization's bus could not afford to operate the profound services to the passenger due to the budget of the city, which requires complicated infrastructure. To provide the BIS services with cheap cost, this paper proposes a secure urban BIS, denoted by $SBIS_{urban}$, based on smart devices and explains the security issues related to the system operation. The $SBIS_{urban}$ is to reduce the cost and to ensure security and privacy from the $BIS_{generalized}$. The $SBIS_{urban}$ is secure from various attacks, provides privacy and has good properties compared with the other systems.

Keywords: *Bus information system, passenger service, communication security, authentication, privacy*

1. Introduction

With the advance of global positioning system (GPS) and the ubiquitous cellular network, real time vehicle tracking for better transport management has become possible. These technologies can be applied to public bus information system (BIS), also called passenger information system (PIS), which are not able to adhere to predefined timetables due to reasons like traffic jams, breakdowns etc. The BIS uses a variety of technologies to track the locations of bus in real time and uses this information to generate exact bus arrivals at stops along the route [1-4]. Passengers can spend their time efficiently with the information. This will make the public transport system competitive and passenger friendly.

Many people regularly use public transportation on their way to work, to meet other people, or to experience new places and landscapes. They are interested in reliable travel-related information, buying tickets without wasting time and a safe journey from the BIS [5]. The BIS is a complex and dynamic system requiring expertise from multiple disciplines. The BIS is a crucial part of any transport system that consumes land and exists within complex settings [2]. Journey planning involves traffic engineers modeling transport routes' network elements such as routes,

* Corresponding Author

ISSN: 1738-9976 IJSIA

services, together with timing and journey patterns. Good journey plans result in efficient public transport lines and stimulate the usage of sustainable modes of transport.

There are some researches for the BIS [6-14]. Researches that deal with the PIS mostly focus on technical aspects, such as the theoretical modeling and technical implementation of context information [6-7]. Others focus on the system description of certain applications [8-9]. Only a few researches regard PISs in relation to themes, such as user experience or user acceptance [10-14]. Lin and Zeng proposed a set of bus arrival time prediction algorithms for a transit traveler information system [10]. Four algorithms were introduced with different assumptions on input data and were shown to outperform several algorithms from the literature. However, their algorithms did not consider the effect of traffic congestion and dwell time at bus stations. Kidwell in [11] presented an algorithm for predicting bus arrival times based on real-time vehicle location. The algorithm worked by dividing each route into zones and recording the time that each bus passed through each zone. Predictions were based on the most recent observation of a bus passing through each zone. However, Kidwell's algorithm was not suitable for large cities where both travel time and dwell time could be subject to large variations. Zografos et al.'s research in [12] present an online PIS for delivering personalized multimodal trip planning services through the integration of wireless and web-based communication technologies. Foth and Schroeter in [13] introduce a research approach offering opportunities to enhance the experience of commuters in all aspects of their journey including planning, waiting at the bus stop, payment and the time after the journey.

It is possible to many typical BISs to permit unauthorized access relatively easily [15]. The most vehicle buses provide freely available documents for the format of possible bus messages, their respective structures and communication procedures. Conventional controllers are impossible to verify if an incoming message comes from an authorized sender at all. Above all, unauthorized vehicle modifications can compromise particularly the driving safety of the respective car and of all surrounding road users. Furthermore, today's BISs encompass multiple technologies, including advanced visual displays, public address, emergency intercom, digital surveillance systems, internet protocol (IP) networks, wireless networks, video streaming, coders, decoders and many more. These systems, denoted by $BIS_{generalized}$, deliver real time information seamlessly on-board vehicles and in stations, while controlled and managed from a single control center. Thereby, the cost of designing, implementing and operating the $BIS_{generalized}$ is not negligible as compared to the overall operational transportation costs.

The focus of this paper is on devising a secure BIS for urban, denoted by $SBIS_{urban}$, which does not require a complicated infrastructure and could not be afford to operate the profound services on the $BIS_{generalized}$ due to the budget limit of the city. To provide the BIS services with small cost, this paper introduces $SBIS_{urban}$ based on smart devices and explains the security issues related to the system operation. The $SBIS_{urban}$ could be used a basic building block to support the BIS for the urban and small company, efficiently.

The remainder of this paper consists of the following sections. Section 2 presents an overview of BISs focused on the generalized and urban. Section 3 provides the major security properties focused on the BIS and proposes the $SBIS_{urban}$. In Section 4, analyses are provided focused on the security and property. Section 5 concludes the work.

2. Overview of Bus Information System

This section gives an overview of the $BIS_{generalized}$ and points out it's problem [16]. Furthermore, this section reviews a previous implementation example focused on Cheorwon at Korea to understand basic requirement on urban BIS, denoted by BIS_{urban} [17].

2.1. Generalized BIS and It's Problem

The BIS has been developed for passengers to know where the bus is passing and when the bus is coming to its stop, which is also called as PIS [16]. The BIS is the key communications link between a bus company and their passengers. The BIS technology lets a bus company communicate with its passengers to provide them with real-time bus location and status updates, schedule data and timely announcements [18].

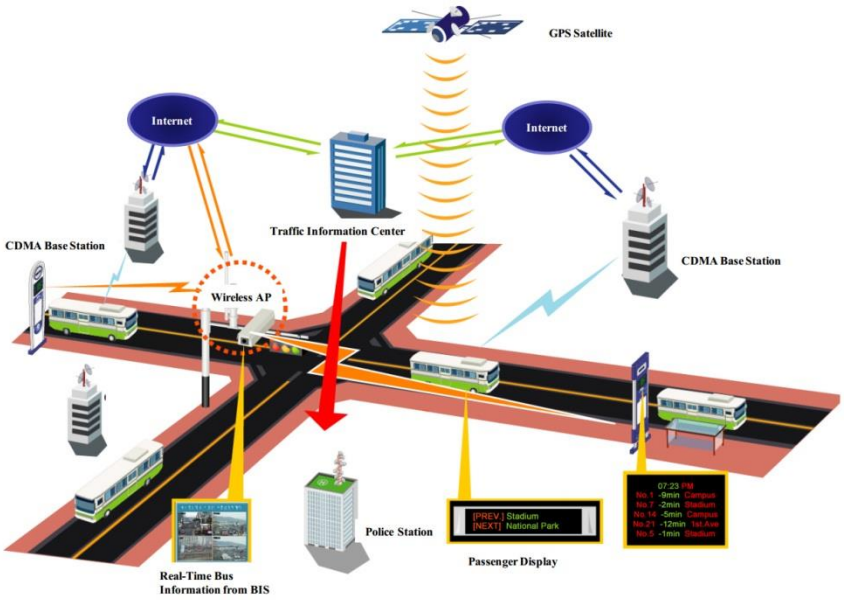

Figure 1. $BIS_{generalized}$ Environment [19]

For this to occur, all buses that wish to know the location must equipped with costly location device (as location beacon and GPS), and display should be equipped to show bus information on each bus stop. In addition, wireless network must be constructed according to the technology depending on the service company's network technology to communicate between the bus and its stops.

The $BIS_{generalized}$ is consisted with the systems that provide current position of the bus to server through mobile network and Internet by equipping location device and mobile communication device. Server processes passenger information after collecting information of location or route information from bus. After this process, server records history of the service for the bus, which could be used to monitor the situations of the bus. From this process, bus driver could keep the predefined arrival to the stop and passengers could use public transportation safely and easily. The bus company could establish business plan for the future by using the history information stored in the server such as location information, number of passengers, accident information, and service status.

A considerable amount of money needs to be investigated for IT-based applications such as real-time and at-stop displays on public transportation [20]. Likewise, a $BIS_{generalized}$ requires equipment of lots of expensive gadgets to operate the proper BIS. However, lots of urban bus companies like urban city's bus company or small organization's bus could not afford to operate the $BIS_{generalized}$ services to the passenger due to the budget of the city, which requires complicated infrastructure as shown in Figure 1.

To provide BIS services with cheap cost, this paper introduces $SBIS_{urban}$ based on smart-phone and explains the security issues related to the system operation [21].

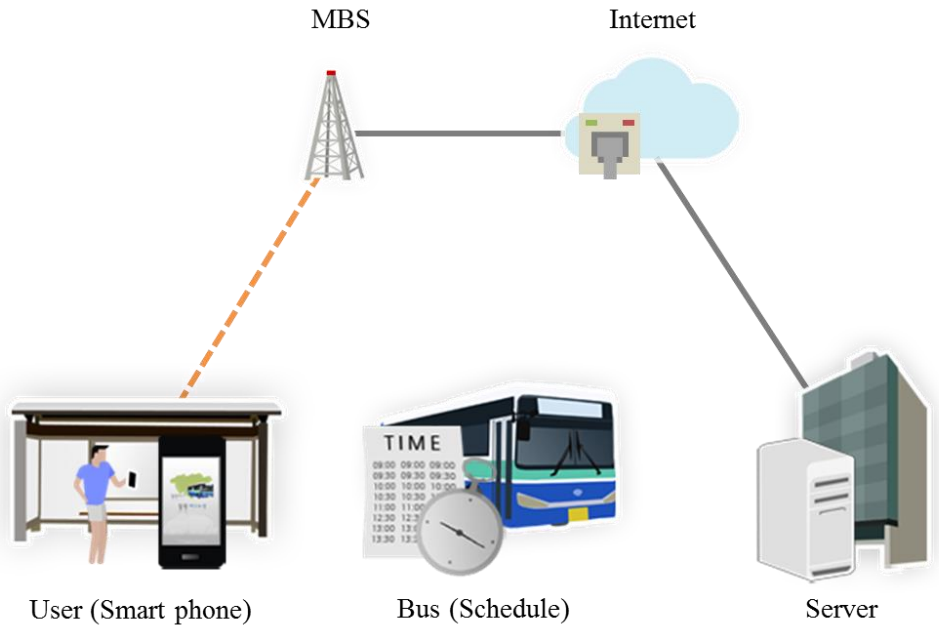

Figure 2. Cherwon City's BIS_{urban} Environment [17]

2.2. Urban BIS

We will review the case study for Cheorwon to withdraw the detailed BIS requirements focused on urban, named as BIS_{urban}, where the population is just 5,000 people corresponding to 1/2000 of Seoul's population with 10 million. The BIS_{urban} for Cheorwon is currently operating via Android app [17]. As shown in Figure 2, buses running at Cheorwon are not equipped with location device. Thereby, bus companies have been just providing static time schedules to the passengers, and could not provide exact arrival time information to them. Besides, the information are also merely static information for departure time, arrival time of each stop, and required time from source to destination stop for bus, which do not consider real situations of bus. It is not easy to many urban cities like Cheorwon to have a $BIS_{generalized}$ due to the following reasons.

- Scale of a market is less than metropolitan: The population has a direct impact to the business scale of bus company. Main route of bus is running with about 30 minutes interval, and the rest routes are running with 1 to 6 hours interval. That's why market of small scale than metropolitan is hard to equip with the expensive infrastructure such as for the $BIS_{generalized}$.
- Establishment of infrastructure and operation cost are huge: For the deployment of the $BIS_{generalized}$, all buses and stops should equip with many expensive gadgets. Furthermore, operating the BIS for various bus networks should require costs for wireless and wired communications. Besides, unlike in the metropolitan case, the government budget of urban is very small.
- Service improvement and maintenance are difficult: There is lack of companies to develop the BIS_{urban} and there are no local companies. Furthermore, the method, hardware, and

software used for each company are different from each other. So, update, modification, addition, and maintenance of the BIS services are not easy.

3. Secure BIS_{urban}

This section proposes a secure urban bus information system, denoted by $SBIS_{urban}$, to reduce the cost and to ensure security and privacy from the generalized BIS. First of all, we define a system environment for the $SBIS_{urban}$, which is a very important part to understand the necessity of our paper. The environment is focused on infrastructure-less configuration, which just uses smart phone like device from user not need to establish or supported by the BIS company. After define security services for the BIS, we will propose a $SBIS_{urban}$.

3.1. $SBIS_{urban}$ Configuration

The functionalities of the $SBIS_{urban}$ should be very the similar with the $BIS_{generalized}$, which requires the similar configuration but needs to be inexpensive. Thereby, the suggested environment has three main components, user, bus, and server. Because the proposed environment is focused on the infrastructure-less, we are focused on reducing the basic requirements for the user and bus, which uses mobile device such as smart phone, tablet PC, or other mobile devices. However, there is no difference for the server side system requirements but needs to be down grade if there is any requirement. It means that our environment for the $SBIS_{urban}$ does not require unified bus location device, costly display for bus stop, and excessive performance server. We assume that each mobile device is equipped with location device such as GPS with global navigation satellite system (GLONASS) and high-speed data communication method such as 3G or LTE.

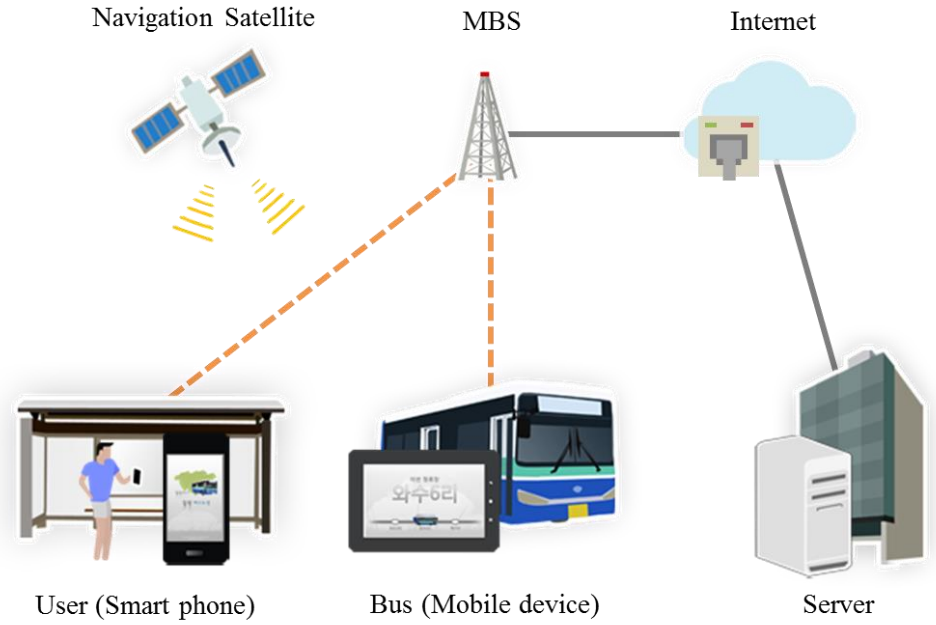

Figure 3. Proposed $SBIS_{urban}$ Environment

The basic functions of the $SBIS_{urban}$ are similar with the $BIS_{generalized}$. However, it is necessary to define roles for each component in the $SBIS_{urban}$ clearly as follows

- User (smart phone): User uses bus information from the server, which are arrival time, interval and route information for bus by sending queries to the server. He (she) should communicate only to the server to get any required information by using App. on his (her) device.
- Bus (mobile device): Bus needs to update its location information to server periodically, which is the top most important data in the $SBIS_{urban}$ and thereby should provide security and privacy. The server could compute the other bus related information including arrival time or delay based on the location information.
- Server: The main role of the server is to provide bus information to passengers by keeping and updating running information of buses in database. Since the information stored in the server is very important to the company, it is necessary to keep and provide security and privacy of the database to the other components. It provides bus information to mobile App. on user's device by using the format of extensible markup language (XML) or Javascript object notation (JSON) data format.

3.2. Security Properties

As the system configuration shown in Figure 3, each entity in the $SBIS_{urban}$ needs to communicate with each other via wireless or wired network, which requires security properties including authentication, confidentiality and integrity. Furthermore, privacy should be considered for the ubiquitous applications like the $SBIS_{urban}$.

A. Authentication

When mobile device needs to connect to a certain network, entity authentication could play a critical role to prevent misuse, abuse and attack. Authentication of all entities is necessary to assure that only valid entity is able to communicate within the BIS. All messages from unauthorized entities may then processed separately or just immediately discarded [15].

There are two ways of communications in authentication concern, which does require or does not require authentication. User device should get information from the $SBIS_{urban}$ server without authentication for the easy accessibility. However, bus driver's device should perform authentication first before it updates or inserts its changes into the database in the server. The data from the bus driver influences the system credibility very much. Furthermore, the device needs to use secure socket layer/transport layer security (SSL/TLS) between the bus and the server. SSL/TLS protocol is generally integrated into the application for protecting data sent via HTTP between clients and servers, which are also known as HTTP over TLS (HTTPS) [22].

B. Confidentiality and Integrity

A fundamental step to improve the BIS's security is applying the encryption of all service information to provide confidentiality. It is obligatory to guard data form disclosure. In passenger applications, sensitive data is sent through the open network. An attacker could overhear the critical information with no trouble [23]. Due to the particular constraints of the BIS, a combination of symmetric and asymmetric encryption meets the requirements on adequate security and high performance [15].

Integrity in information security is usually defined as the concept that an attacker should not be able to modify or tamper with the information without being noticed by the information owner. For company, it should be guaranteed so that the company can trust that information does not played by attacker [24].

To provide confidentiality and integrity, the $SBIS_{urban}$ needs to use advanced encryption standard (AES), Elliptic curve cryptosystem (ECC) and secure hash algorithm-2 (SHA2) as

symmetric key cryptosystem, public key cryptosystem and message authentication code, respectively. Those operations are applied only to security sensitive information in the $SBIS_{urban}$.

C. Privacy

Users need to regulate how applications access the private information that is stored on their phone. Their smart phones often store sensitive personal information including GPS, WiFi SSIDs, cellular tower information, and sensor data [25].

Especially, precise estimation of the patient's location is needed in most passenger applications. The lack of smart tracking mechanisms permits attacker to send erroneous reports concerning the passenger's location either by reporting fake signal strengths or by using rerun the signals [23]. Thereby, provision of privacy is one of very important aspects in the BIS.

3.3. Functional Properties

The $SBIS_{urban}$ should provide the overall functionalities from the $BIS_{generalized}$, as shown in Figure 4.

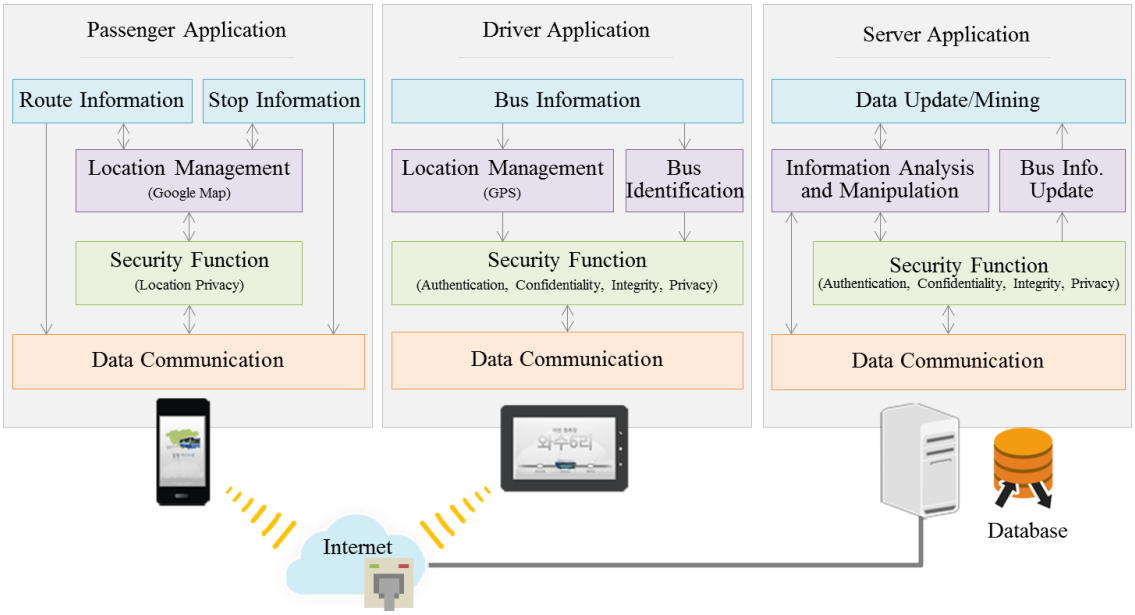

Figure 4. Overview of $SBIS_{urban}$'s Functional Properties

There are some modules for the $SBIS_{urban}$ in passenger's application, driver's application and server application. The functionalities of each application are listed as follows:

- Passenger's application: This app. has two important functions including route information and stop information. Route information is to provide information of a specific bus's operation route, shortest path, minimal required travel time and transit by using two inputs of source stop and destination stop. The current bus stop information could be used if passenger is at the bus stop. Stop information is for providing arrival time, interval and route information on buses for the stop.
- Driver's application: This app. is to provide current location, velocity, arrival time and delay based on the location information of a specific bus. The bus information is automatically submitted to the server at an interval of several seconds for the real-time information by establishing a secure channel between the bus and the server after authentication.

- Server: The module is provided in the form of a web server, which processes all the data from or to driver's applications and the passenger's applications. Whole information are kept on database in secure manner. It communicates with passengers to provide information including route information and stop information. Otherwise, it updates current location, velocity, arrival time and delay obtained from each bus.

The $SBIS_{urban}$ requires the following assumptions to support security functions. The server has a public-private key pair $\{PU_S, PR_S\}$ for the public-key cryptosystem and each user has the possibility to generate a session key SK to be used for encryption based on the symmetric-key cryptosystem. The server's public key PU_S is opened to user and its private key PR_S is kept in secret.

A. Passenger Application

Passenger application provides two queries, stop and route. For stop query, the current location information of user is provided to the server. Otherwise, user needs to input source and destination information. For the privacy, data could be encrypted and transferred to the server. The overall procedure of the passenger's application follows the steps

Step 1. User selects a function whether he or she requires the route information or the stop information.

Step 2. User's request is transmitted to the server through data communication module by applying encryption if it requires privacy support. The encrypted query message is formed as $\{E_{SK}(LOC||TS_U), E_{PUs}(SK||TS_U), MAC_{SK}(E_{SK}(LOC||TS_U))\}$ by using the server's public key PU_S and the current timestamp TS_U if it requires privacy. Otherwise, the message is transferred without applying encryption.

Step 3. When the server receives the query, it decrypts the message $E_{PUs}(SK||TS_U)$ by using it's private key PR_S to derive the session key SK' if the privacy function was applied to the message. Furthermore, it checks the integrity of the query by checking whether the computed $MAC_{SK'}(E_{SK}(LOC||TS_U))$ and the received $MAC_{SK}(E_{SK}(LOC||TS_U))$ are the same or not. After that, it checks the currency of TS_U. The server decrypts $E_{SK}(LOC||TS_U)$ with SK' only if the verifications are successful. After processing the query by using LOC from the user, the server returns back secured data by applying encryption and integrity with the session key SK'. The format of the message is as $\{E_{SK'}(M||TS_S), MAC_{SK'}(E_{SK'}(M||TS_S))\}$ if the query request is encrypted. Otherwise, the message is transferred in plaintext.

Step 4. After receiving the message, the passenger's application decrypts $E_{SK'}(M||TS_S)$ only if the validation of $MAC_{SK'}(E_{SK'}(M||TS_S))$ is successful.

Step 5. The passenger's application shows information by using the message M from the server.

B. Driver Application

Driver application is to keep updates for the specific bus information, i.e. bus identification (BID), current location (LOC), route information (ROU) and time (TS_D), to server's database. It uses the following steps to keep the current information of the bus

Step 1. The driver's application sends the bus information periodically to the server. Whenever a bus needs to connect to the server for the bus information update, it needs to be authenticated and establish a session key SK to the server by using one of the previous well known authenticated key agreement schemes in [26-28]. The application sends an encrypted message $\{E_{SK}(BID, TS_D, LOC), MAC_{SK}(E_{SK}(BID, TS_D, LOC))\}$ by using the session key SK, only after the authentication is successful.

Step 2. When the server receives the message from the bus, it checks the integrity of $MAC_{SK}(E_{SK}(BID, TS_D, LOC))$. It updates the bus information in the database by using the decrypted information from $E_{SK}(BID, TS_D, LOC)$ only if the integrity check is successful.

C. Server Application

Server application needs to communicate with the driver application or the passenger application. To support the driver application, it mainly updates the information, including location and time delay, related with buses after the authentication and the session key establishment. The whole information from buses are especially important to the $SBIS_{urban}$, which need to be encrypted based on the symmetric key cryptosystem. However, it just provides route or stop information to the user for the passenger application if user does not care about privacy or does not like overhead from the application. Otherwise, the communication channel could be secured by establishing session key based on the asymmetric key cryptosystem. The two functions are processed as follows:

- For the driver application, the server needs to authenticate the bus and establish a session key *SK* with the bus whenever a request $\{E_{SK}(BID, TS_D, LOC), MAC_{SK}(E_{SK}(BID, TS_D, LOC))\}$ from a bus arrives to it. It updates the information of the bus in the database only if the integrity of the message is successful. It means that the bus's information is successfully updated in the database. This update is repeated in an interval of several seconds until the bus finishes the service.
- If a query is received from a user, the server checks whether the query is encrypted or not, *i.e.*,$\{E_{SK}(LOC||TS_U), E_{PUs}(SK||TS_U)\}$ or $\{LOC||TS_U\}$. It decrypts the query first if it is encrypted by using the session key *SK*. After applying the query to the database, the server returns back the result to the passenger application. Before the transmission of the message, the data should form as $\{E_{SK}(M||TS_S), MAC_{SK}(E_{SK}(M||TS_S))\}$ by applying encryption and integrity check function.

4. Analyses

This section shows that the $SBIS_{urban}$ is secure against various security attacks and provides privacy. Furthermore, we will provide properties analyses.

4.1. Security Analysis

This section provides security analysis on the $SBIS_{urban}$, which are focused on replay attack, bus masquerading attack, server masquerading attack and session key agreement. Mathematical problems are discussed first that are used to the security analyses.

A. Mathematical Problems

Here, we discuss some mathematical problems, which form the basis of the security on the $SBIS_{urban}$. The $SBIS_{urban}$ is based on the discrete logarithm problem (DLP), the symmetric key cryptography (SKC) and the cryptographic hash function (CHF).

- DLP: Public key cryptography, also known as symmetric cryptography, is a class of cryptographic algorithms which requires two separate keys, one of which is secret or private and one of which is public. Although different, the two parts of this key pair are mathematically linked. The public key PU_S is used to encrypt plaintext or to verify a digital signature; whereas the private key PR_S is used to decrypt ciphertext or to create a digital signature. Public-key algorithms are based on mathematical problems which currently admit no efficient solution that are inherent in certain integer factorization, DLP,

and elliptic curve relationships. It is computationally easy for a user to generate their own public and private key-pair and to use them for encryption and decryption. The strength lies in the fact that it is impossible for a properly generated private key to be determined from its corresponding public key [29]. It is assumed that the public key cryptography used in the $SBIS_{urban}$ is based on the DLP.

- SKC : SKC is a class of algorithms for cryptography that use the same cryptographic keys for both encryption and decryption. The keys may be identical or there may be a simple transformation to go between the two keys. The keys represent a shared secret between two parties that can be used to maintain a private information link [30]. It is assumed that the SKC used in the $SBIS_{urban}$ is based on the advanced encryption standard (AES).
- CHF : A CHF is a hash function which is considered practically impossible to invert the input data from its hash value alone. The input data is often called the message, and the hash value is often called the message digest. The ideal cryptographic hash function has four main properties: it is easy to compute the hash value for any given message, it is infeasible to generate a message that has a given hash, it is infeasible to modify a message without changing the hash and it is infeasible to find two different messages with the same hash [31]. It is assumed that the CHF used in the $SBIS_{urban}$ is based on the hashed message authentication code (HMAC).

B. Replay Attack

The $SBIS_{urban}$ uses a session key based on a random numbers SK and a timestamp TS_U to cope with this attack. An attacker could intercept one of the messages $\{E_{SK}(LOC||TS_U), E_{PUs}(SK||TS_U), MAC_{SK}(E_{SK}(LOC||TS_U))\}$ from the user, $\{E_{SK}(BID, TS_D, LOC), MAC_{SK}(E_{SK}(BID, TS_D, LOC))\}$ from the driver and $\{E_{SK}(M||TS_S), MAC_{SK}(E_{SK}(M||TS_S))\}$ from the server. However, there is no way to the attacker to successfully replay the messages due to the validation check in each step of the function. So, the $SBIS_{urban}$ is secure against the replay attack due to the basic difficulties on the DLP, the SKC and the CHF.

C. Bus Masquerading Attack

The attacker cannot derive a bus's secret information from the eavesdropped message $\{E_{SK}(BID, TS_D, LOC), MAC_{SK}(E_{SK}(BID, TS_D, LOC))\}$ among the driver's application the server. The timestamp and session key prevent replay of the message, which could cope from masquerading attack. Because of using TS_D in $E_{SK}(BID, TS_D, LOC)$ and $MAC_{SK}(E_{SK}(BID, TS_D, LOC))$, the attacker cannot replay the driver application's message, which is based on the DLP, the SKC and the CHF.

D. Server Masquerading Attack

The attacker cannot derive a server's secret information from the eavesdropped message $\{E_{SK}(M||TS_S), MAC_{SK}(E_{SK}(M||TS_S))\}$ among the server and an entity among user or bus. To forge the message from the server, the attacker needs to know the private key PR_S from the public key PU_S. However, it is impossible due to the DLP. Furthermore, the attacker could not get any useful information from the intercepted message due to the SKC and the CHF.

E. Session Key Agreement

In order to protect the communication between two entities in the $SBIS_{urban}$, a session key needs to be established between them. The $SBIS_{urban}$ uses the combinations of the DLP and the SKC to establish a session key depending on the fresh session random number. By securing the exchange of SK based on the public key cryptography, two parties can share a common session key SK.

F. Privacy Support

The $SBIS_{urban}$ provides location privacy to the user by using the message $\{E_{SK}(LOC||TS_U), E_{PUs}(SK||TS_U), MAC_{SK}(E_{SK}(LOC||TS_U))\}$. User's location information is very important over ubiquitous computing environment. The privacy is based on the SKC and the DLP. Furthermore, the $SBIS_{urban}$ provides the bus privacy focused on the identification and location with the message $\{E_{SK}(BID, TS_D, LOC), MAC_{SK}(E_{SK}(BID, TS_D, LOC))\}$. Only the server with the proper private key could know the information in it. Thereby, we could argue that the $SBIS_{urban}$ supports privacy.

G. Security Comparison

Table 1 shows security comparisons among the BIS_{urban}, the $BIS_{generalized}$ and the $SBIS_{urban}$. The BIS_{urban} and the $BIS_{generalized}$ could not support privacy. However, the $SBIS_{urban}$ could provide all the necessary security properties as shown in Table 1.

Table 1. Security Comparisons

	BIS_{urban}	$BIS_{generalized}$	$SBIS_{urban}$
Security Aspects			
Confidentiality	No	Provide	Provide
Authentication	No	Provide	Provide
Integrity	No	Provide	Provide
Key agreement	No	Provide	Provide
Privacy	No	No	Provide

4.2. Property Analysis

The focus of this paper is on the cost efficient and the easy implement-ability of the BIS in urban or with infrastructure-less. This sub-section provides analyses on these two aspects with the comparisons among the BIS_{urban}, the $BIS_{generalized}$ and the $SBIS_{urban}$. It is only considered the GPS based $BIS_{generalized}$ for the simplicity even if there is the beacon based $BIS_{generalzied}$.

A. Easy Implement-ability

Easiness of implementation is one of the most important properties to realize the BIS. It needs to check and compare the GPS range, the updating interval of bus information, the map to be provided to passenger, the application development for bus and the performance and capacity of the server. Table 2 shows comparisons among the BIS_{urban}, the $BIS_{generalized}$ and the $SBIS_{urban}$.

The bus needs some devices for location information transmission to the server including GPS receiver and so on. The BIS_{urban} does not require any device because it is operated on the fixed bus schedule table. However, the $BIS_{generalized}$ requires GPS receiver, a communication device connected to the server, and some additional devices for the location information processing. Contrast with them, the $SBIS_{urban}$ requires only a smart phone, which naturally equips the communication module and GPS receiver based on GLONASS. The GLONASS receiver is 20 % faster than GPS.

For the concern on the exact location approximation, GPS and GLONASS have maximum 100*m* and 150*m* differences from the exact position, respectively. However, the smart phone based on GPS with GLONASS could reduce the differences to maximum 15*m*.

It is very important to provide correct information to passenger over the BIS. However, the BIS_{urban} only changes the schedule table and informs to passengers when the bus was crashed or is in bad traffic jam. Thereby, it is not easy to provide credible information to passenger from the BIS_{urban}. However, both of the $BIS_{generalized}$ and the $SBIS_{urban}$ updates the bus's information in real-time, i.e. about 3 to 5 seconds, and refreshes to the passengers, which could provide credible information.

Map based passenger interface is provided over the BIS, which shows the current position or the route information of the bus based on the bus's position stored in the server or source to destination information. The $BIS_{generalized}$ provides a customized map developed by the company or the 3rd party map by using position information from the location recognizer. However, the $SBIS_{urban}$ uses Google Map, which does not require any additional processing to know the position and matching.

On developing applications on the BIS, data communication is one of the most important parts on the security and overhead of the system. It needs to develop software to compatible with the operating system (OS) on the communication device on the $BIS_{generalized}$. Developing software on the popular OS like Windows CE or Linux is cheaper than on the rarely used OSs like a company's private OS. Furthermore, the developer could have much more overhead in the latter case. But, the $SBIS_{urban}$ is based on the smart phone, which is based on the well-known OSs and easy to developers due to the abundant resources, open sources, and good developer's networks.

For the server capacity, the BIS_{urban} only provides predefined bus information stored in the server to passengers. As a solution from the BIS_{urban}, the $BIS_{generalized}$ uses some servers for passengers. The servers on the $BIS_{generalized}$ are classified with their functionalities, which need the functions of communication, processing, analysis, store and data provision. However, the server on the $SBIS_{urban}$ requires only simple operations of store and provision of service because the bus driver's device could pre-process required operations, which only provides a function of Web server.

Table 2. Implement-ability Comparisons

	BIS_{urban}	$BIS_{generalized}$	$SBIS_{urban}$
Property			
Necessary devices on bus	Not support	GPS receiver, communication device	Smart phone
GPS range	Not support	GPS within 100m	GPS+GLONASS within 15m
Updating interval	On schedule change (On accidents or traffic jam)	3~5 seconds	3~5 seconds
Map	Not support	Necessity on map matching	Google Map
Application development	Not support	On dedicated Embedded device	APP. on Android
Server capacity	Web server to support bus schedule	Data analyzing server with communication support device	Web server to support GPS information

B. Budget Supportability

We will consider two budget factors, initial system set-up costs and maintenance costs, based on each service. This analysis could show how much the $SBIS_{urban}$ is efficient in budget with good performance by providing comparison in Table 3.

For the initial set-up of the BIS, the $BIS_{generalized}$ uses a typical GPS receiver with cheap cost but needs a dedicated communication device to the BIS, which is comparatively expensive. However, the $SBIS_{urban}$ could support services by just using passenger's used smart phone, which does not need any additional costs. Glaxy Note N7000 from Samsung and Optimus G E975 from LG are accompanied with 3G and LTE communication property and GPS with GLONASS. The $SBIS_{urban}$ could be operated over even to the second handed smart phone within 3 years of release.

The communication device from the $BIS_{generalized}$ needs to check compart-ability with GPS receiver depending on OS. Thereby, the cost of software development is depending on the developing company on the $BIS_{generalized}$. However, the cost of the $SBIS_{urban}$ should be cheaper than the other environment because it is based on Android as mentioned before, which has the abundant resources, open sources, and good developer's networks.

Currently, the BIS_{urban} does not have much traffic due to the simple information supports to passenger. However, the $BIS_{generalized}$ and the $SBIS_{urban}$ require many communications in every second to support real-time location based bus information. The good aspect in the $BIS_{generalized}$ is that of using smart phone, which has good communication module and high performance device. Thereby, it could partially preprocess data before the transmission to the server.

Table 3. Budget Comparisons

	BIS_{urban}	$BIS_{generalized}$	$SBIS_{urban}$
Property			
Initial device set-up	Not support	GPS receiver, Expensive dedicated communication device	User's smart phone
Bus software development	Not support	High (over dedicated embedded system)	Relatively low (App. over Android)
Server maintenance	A Web server (data service)	Two servers (Analysis server, Server for passenger)	A Web server (data service)
Approximation of total amount to system set-up	$*** (Some hundreds $)	$**,*** (Some ten thousands $)	$*** (Some hundreds $)

5. Conclusion

This paper has been proposed a secure bus information system for urban, denoted by $SBIS_{urban}$, which reduces the cost and ensures security and privacy from the $BIS_{generalized}$. It does not require a complicated infrastructure and could be affordable to operate to the budget limited city. First of all, we defined a system environment for the $SBIS_{urban}$, which is a very important part to understand the necessity of our system. The environment is focused on infrastructure-less configuration, which just uses smart phone like devices from user and does not need to establish or supported by the BIS company. Analyses showed that the $SBIS_{urban}$ is secure from various attacks, provides privacy and has good properties compared with the other systems.

Acknowledgements

This work was supported by the National Research Foundation of Korea Grant funded by the Korean Government (MEST) (NRF-2010-0021575).

References

[1] K. Ganesh, M. Thrivikraman, J. Kuri, H. Dagale, G. Sudhakar and S. Sanyal, "Implementation of a Real Time Passenger Information System", CoRR abs/1206.0447 **(2012)**.
[2] J.-P. Rodrigue, C. Comtois and B. Slack, "The Geography of Transport Systems", 2nd ed., Routledge, London/New York **(2009)**.
[3] V. Scinteie, "Implementing Passenger Information, Entertainment, and Security Systems in Light Rapid Transi"t, Transportation Research Circular E-C058:9th National Light Rail Transit Conference, **(2003)**, pp. 528-533.

[4] J. Hu and G. Li, "Design of City-Bus Intelligent Control System Framework", In Proc. of the 2006 IEEE International Conference on Mechatronics and Automation, **(2006)**, pp. 2307-2311.
[5] B. Caulfield and M. O'Mahony, "An examination of the public transport information requirements of users", IEEE Transactions on Intelligent Transportation Systems, vol. 8, no. 1, **(2007)**, pp. 21–30.
[6] G. Eichler, K. H. Luke and B. Reufenheuser, "Context information as enhancement for mobile solutions and services", in *Proc. 13th Int. Conf. Intell. Next Gen. Netw.* **(2009)**, pp. 1–5.
[7] A. Brossard, M. Abed and C. Kolski, "Taking context into account in conceptual models using a model driven engineering approach", *Inf. Softw. Technol.* **(2011)**, vol. 53, pp. 1349–1369.
[8] J. Liikka, J. Lahti, P. Alahuhta and M. Rosenberg, "KAMO: Mobile guide for the city traveller", *Proc. 4th Int. Conf. Intell. Environ.* [Online]. Available: http://digital-library.theiet.org/content/conferences/10.1049/cp_20081133 **(2008)**.
[9] C. R. Garcia, S. Candela, J. Ginory, A. Quesada-Arencibia and F. Alayon, "On route travel assistant for public transport based on android technology, in *Proc. 6th Int. Conf. Innovative Mobile Internet Services in Ubiquitous Comput.* **(2012)**, pp. 840–845.
[10] W.-H. Lin and J. Zeng, "An Experimental Study on Real Time Bus Arrival Time Prediction with GPS Data", Transportation Research Record, vol. 1666, **(1999)**, p. 101-109.
[11] B. Kidwell, "Predicting Transit Vehicle Arrival Times", GeoGraphics Laboratory, Bridgewater State College **(2001)**.
[12] K. G. Zografos, K. N. Androutsopoulos and V. Spitadakis, "Design and assessment of an online passenger information system for integrated multimodal trip planning", *Trans. Intell. Transport. Syst.* vol. 10, **(2009)**, pp. 311–323.
[13] M. Foth and R. Schroeter, "Enhancing the experience of public transport users with urban screens and mobile applications", in Proc. 14th Int. Academic MindTrek Conf.: Envisioning Future Media Environ., **(2010)**.
[14] J. Bargas-Avila and K. Hornbæk, "Old wine in new bottles or novel challenges: A critical analysis of empirical studies of user experience", in *Proc. Annu. Conf. Human Factors Comput. Syst.* **(2011)**, pp. 2689–2698.
[15] M. Wolf, A. Weimeskirch and C. Paar, "Security in Automotive Bus Systems", in Proc. Workshop on Embedded Security in Cars, **(2004)**.
[16] D. M. Bae, "An analysis on the efficiency of bus information systems in Bucheon city", Journal of Korean Society of Transportation, vol. 20, **(2002)**, no. 1, pp. 7-18.
[17] D. Park," Cheorwon Bus", **(2013)**.
[18] Mentor Eng. Inc., Passenger information systems: what transit agencies need to know **(2011)**.
[19] J. Lee, K. Hong, H. Lee, J. Lim and S. Kim, "Bus information system based on smart-phone Apps", in *Proc. of KSCI Winter Conference* **(2012)**, pp. 219-222.
[20] S. Chandurkar, S. Mugade, S. Sinha, M. Misal and P. Borekar, "Implementation of Real Time Bus Monitoring and Passenger Information System", International Journal of Scientific and Research Publications, vol. 3, no. 5, **(2013)**, pp. 1-5.
[21] S. Kim, "Security Augmenting Scheme for Bus Information System based on Smart Phone", International Journal of Security and Its Applications, vol. 7, no. 3, **(2013)**, pp. 337-345.
[22] M. L. Das and N. Samdaria, "On the security of SSL/TLS-enabled applications", Applied Computing and Informatics, vol. 10, **(2014)**, pp. 68-81.
[23] N. Fatema and R. Brad, "Security Requirements, Counterattacks and Projects in Healthcare Applications Using WSNs – A Review, International Journal of Computer Networking and Communication, vol. 2, no. 2, **(2014)**, pp. 1-9.
[24] F. Hansson, "System Integrity for Smartphones – A security evaluation of iOS and BlackBerry OS", Thesis, Linköping University, **(2011)**.
[25] S. Egelman, A. P. Felt and D. Wagner, "Choice Architecture and Smart phone Privacy: There's A Price for That", The Economics of Information Security and Privacy, **(2013)**, pp. 211-236.
[26] H. Kim, "P_PAKA: Privacy Preserving Authenticated Key Agreement Protocol in Smart Grid", International Journal of Security and its Applications, vol. 8, no. 5, **(2014)**.
[27] H. Kim, "Anonymous authentication protocol for mobile pay-TV system", Communications in Computer and Information Science, vol. 339, no. 5, **(2012)**, pp. 471-478.
[28] H. Kim, "End-to-end Authentication Protocols for Personal/Portable Devices over Cognitive Radio Networks", International Journal of Security and its Applications **(2014)**, Vol. 8, No. 4, pp. 123-138.
[29] http://en.wikipedia.org/wiki/Public-key_cryptography
[30] http://en.wikipedia.org/wiki/Symmetric-key_algorithm
[31] http://en.wikipedia.org/wiki/Cryptographic_hash_function

Authors

Donghyuk Park, He is a student at the Department of Computer Engineering, Kyungil University, Korea and works as a developer at REBOMBA Inc. His research interests include information security, passenger information system, social network service, cloud computing, cyber physical system and ubiquitous computing.

Hyunsung Kim, He is a professor at the Department of Cyber Security, Kyungil University, Korea from 2012. He received the M.S. and Ph.D. degrees in Computer Engineering from Kyungpook National University, Republic of Korea, in 1998 and 2002, respectively. From 2000 to 2002, he worked as a senior researcher at Ditto Technology. He had been an associate professor from 2002 to 2012 with the Department of Computer Engineering, Kyungil University. His research interests include cryptography, VLSI, authentication technologies, network security and ubiquitous computing security.