A Secure Public Transport Multimedia on Demand System for VANET

Chin-Ling Chen1,2, Ming-Shaw Lu3, Jian-Wei Li4, Changqing Gong5 and Liang Zhao6
1Department of Computer Science and Information Engineering, Chaoyang University of Technology, Taiwan (R.O.C.)
2College of Information, Changchun University of Technology, Jilin Province, China
clc@mail.cytu.edu.tw
3Department of Information Management, Chaoyang University of Technology, Taiwan (R.O.C.)
shawming2001@gmail.com
4Department of Information and Communication Engineering, Chaoyang University of Technology, Taiwan (R.O.C.)
lijw@cyut.edu.tw
5,6 School of Computer Science, Shenyang Aerospace University, Liaoning Province, China
gongchangqing.zhao@sau.edu.cn

Abstract

In recent years, multimedia has been widely applied in various situations. Due to the fact that piracy is rampant, the issue of how to provide public transport passengers with a protected copyright multimedia entertainment service has become important. In this paper, a secure public transport multimedia on demand (MoD) system is proposed for Vehicular Ad-Hoc Networks (VANET) that not only protects the transmission of copyrighted multimedia data, but also provides passengers with a more enjoyable set of multimedia services during long travel. The proposed scheme satisfies the security requirements, such as defends against known attacks, authenticity, confidentiality and integrity issues. Our scheme is realistic and can enhance the competitiveness of the public transport companies.

Keywords: MoD, Multimedia service, VANET, Public transport

1 Introduction

1.1 Background

Recently, vehicle early warning systems [1-5] which are mainly applied to detect road conditions have become an important issue in intelligent transportation systems (ITS). However, the concept of green energy has gradually turned people’s attention toward public transportation (trains, airplanes, etc.) as a more viable transportation option. With public transportation, passengers may rest, chat or enjoy multimedia content such as music or video played by a transportation system administrator. On an airplane, a multimedia entertainment system [6] such as audio-video on demand (AVOD) or video on demand (VOD) is provided for passengers, who can choose their favorite multimedia content via a set-top box device. In contrast, the driver/conductor of a land-based public transportation system, not the passengers, chooses the multimedia content for broadcasting. Moreover, the copyright of the digital media need to be protected. However, using a value-added service via Vehicular Ad-Hoc Networks (VANET) is another worth researching issue. Thus, determining how to provide a public transport passenger with various services has become a practical issue[7-9]. In this paper, we propose a multimedia on demand (MoD) payment system in VANET and use a personal trusted device to protect the passenger’s sensitive information such that the passenger can enjoy the multimedia during travel.

1.2 Requirements

Many scholars [2,4-5,10-15] have presented infrastructures based on the public key infrastructure (PKI) to protect data security in vehicular communication, and some with possible solutions for security issues [3,12-13,16-17]. In 2010, researchers [18-21] analyzed encryption algorithms for images and indicated that the security of multimedia entrainment services cannot be ensured when applied to these algorithms, which also cannot protect copyrighted multimedia data or avoid inappropriate material for VANET.

With respect to the design requirements in VANET, the usual requirements regarding conventional cryptography should also be applied to the design of vehicular communication to ensure the security of vehicular communication systems and prevent attacks wherever possible, a hard problem with a broad range of challenges. Without security, users will be vulnerable to the malicious behavior in VANET services. The high speed real-time interaction and ample source of battery power are specific vehicle characteristics. All security services need to meet strict time constraints or they will become void. The following security issues occur with VANET.
Table 1 Comparison of WiMax, Wi-Fi and DSRC Technologies [13, 16]

<table>
<thead>
<tr>
<th></th>
<th>WiMax</th>
<th>Wi-Fi</th>
<th>DSRC</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Mobility</strong></td>
<td>&gt;60 km/h</td>
<td>&gt;5 km/h</td>
<td>&gt;60 km/h</td>
</tr>
<tr>
<td><strong>Range</strong></td>
<td>40 miles</td>
<td>400 meters</td>
<td>1000 meters</td>
</tr>
<tr>
<td><strong>Data rate</strong></td>
<td>2~70 Mbps</td>
<td>6~54 Mbps</td>
<td>3~27 Mbps</td>
</tr>
<tr>
<td><strong>Bandwidth</strong></td>
<td>&lt; 10 MHz</td>
<td>20 MHz</td>
<td>10/20 MHz</td>
</tr>
<tr>
<td><strong>Spectrum</strong></td>
<td>2.5 GHz</td>
<td>2.4 GHz, 5 GHz</td>
<td>5.86~5.926 GHz</td>
</tr>
<tr>
<td><strong>Standard</strong></td>
<td>802.16d/e</td>
<td>802.11n</td>
<td>802.11p/1609</td>
</tr>
</tbody>
</table>

(1) Authentication: The task of ensuring that the communication is authentic by identifying the sender; the vehicle should only react to messages generated by legitimate senders[22].

(2) Integrity: The integrity service deals with the consistency of a stream of messages. It ensures that the received messages are the same as those sent without modification, insertion, reordering, or replays.

(3) Non-repudiation: This service prevents either the sender or receiver from denying transmitted messages. This service may be crucial in determining the correct sequence and content of messages exchanged before an accident.

(4) Confidentiality: This issue has been defined by the International Organization for Standardization (ISO) in ISO-17799 [23] as "ensuring that information is accessible only to those authorized to have access" and is one of the cornerstones of information security. Confidentiality is one of the design goals for many cryptosystems, made possible by the techniques of modern cryptography.

In addition, faultless VANET protocol can also rule out possible malfeasance (for example, replay attack, impersonation attack, hijacking attack, etc.). In this paper, we present a secure MoD system for passengers to choose their favorite multimedia services on public transportation. The proposed scheme uses WiMax technology to transmit multimedia data. We use a certificate, a symmetric encryption, and a one-way hash function to protect confidential messages during the authentication and handoff phases. Chang et al.’s scheme [24] is adopted to protect the transmission of multimedia lists (passengers’ multimedia demands) and copyrighted multimedia content. Thus, a secure public transport MoD system can meet passengers’ requirements and enhance the competitiveness of the public transport companies. Our scheme can meet the following goals:

- Prevent an impersonation public transport (PT) attack
- Prevent a replay attack
- Prevent a hijacking attack
- Prevent a Denial of Service (DoS) attack
- Mutual authentication
- Confidentiality
- Integrity
- Handoff

The rest of this paper is organized as follows. Section 2 introduces related works. The proposed scheme is described in Section 3. In Section 4, we present a security analysis and discussions. Finally, conclusions are given in Section 5.

2 Background works

Many researchers [1-5] have used Worldwide Interoperability for Microwave Access (WiMax), Wireless Fidelity (Wi-Fi), Dedicated Short-Range communications (DSRC) to implement car-to-car communication, car-to-roadside facilities, Internet connectivity; much of the public infrastructure is authenticated using the X.509 certificate. In addition, the Chang et al.’s scheme [24] to protect copyrighted multimedia data is also adopted in our scheme. The related techniques will be introduced as follows.

2.1 WiMax versus Wi-Fi and DSRC

WiMax is defined in IEEE 802.16 standards and with increased market recognition such that it will result in lower cost products based on open standards. WiMax is a wireless communications system for economically delivering broadband access services to individual and commercial customers. It will transform the world of mobile broadband by enabling the cost-effective deployment of metropolitan area networks based on the IEEE 802.16e standard to support notebook PC and mobile services while moving. WiMax is not designed to clash with Wi-Fi, but rather to coexist with it. DSRC [25] is a short to medium range communications service that supports both public safety and private operations in roadside to vehicle and vehicle to vehicle communication environments. We make a comparison of the wireless communications among the three types, as shown in Table 1.

The WiMax standards describe a sophisticated media access control (MAC) protocol that can share a radio channel among hundreds of users while providing quality of service (QoS) [26]. The transmission range and rate on WiMax are better than the other types, as seen in Table 1. Therefore, WiMax is suitable as a communication platform in our scheme.

2.2 Review Chang et al.’s scheme
In 2005, Chang et al. [24] proposed digital signatures with message recovery using self-certified public keys without a trustworthy system authority. Chang et al.’s scheme has the following characteristics: (1) Transmits larger messages, and (2) Only allows the specified receiver to verify and recover the message. It is suitable to transmit multimedia data with copyright to a designated receiver, so we use it to recover multimedia from a hidden signature and encryption messages after compression [27-29] and division. In 2005, Zhang et al. [30] proposed an improved scheme to fix the loopholes in Chang Next, we briefly introduce Zhang et al. and Chang et al.’s scheme.

2.2.1 Chang et al.’s and Zhang et al.’s notations

d_i: The i’s identity
M_j: The i th message
h(·): A one-way hash function
A 2 B: Compare whether A is equal to B
x_i: The secret key of the user i
y, k: The random numbers
r_i, t, s: The digital signatures, for i = 1, 2, 3, …, m
r: The hash value, where
r = h(r_1 || r_2 || ··· || r_m)

2.2.2 Chang et al.’s core mechanism

The signature and encryption of a larger message (M_1, M_2, ···, M_m) are sent by sender P_1 to specified receiver P_r. First, P_r chooses a random number k and computes. Afterwards, P_r sends (r, s, σ, r_1, r_2, ···, r_m) as the signature of message M to specified receiver P_r. After receiving (r, s, σ, r_1, r_2, ···, r_m), specified receiver P_j recovers message (M_1, M_2, ···, M_m) and verifies the signature of message without the private key of recipient. They improved those weaknesses of Chang et al.’s scheme. We utilize Zhang et al.’s mechanism to protect the multimedia copyright in the communication phase.

3 The proposed scheme

This section presents the cardinal roles/components in our proposed scheme:

(1) The public transit (PT, for example: bus or train) is provided by a company that operates a fleet of vehicles for transit.
(2) The base station (BS) is a transmitter at an accurately-known fixed location which is used to derive correction information for nearby portable receivers.
(3) The passenger (P) requests MoD service.
(4) The multimedia on demand service server (MoDSS) supplies multimedia service (example: movie and music).
(5) An on-board unit (OBU) is a device application unit (AU) embedded into a seat in front of the passenger.
(6) Communication server (CS) is a device deployed on PT which uses an application unit (AU, the AU is a tamper-proof application interface between P and PT) to receive the passenger’s demand to transmit to MoDSS via BS.
(7) Certification Authority (CA) is an entity that issues digital certificates for use by other parties. It is an example of a trusted third party. In our scheme, the CS’s identification and certificate issued to PT by the trustworthy CA.

The flow chart of our scheme is illustrated in Fig. 1.

1. PT owner ↔CA: The PT owner sends vehicle information to the CA for registration via secure channels. After verification, the CA issues the certificate and public key to the PT.
2. P ↔CS: The P wants to enjoy the multimedia service he/she uses the OBU and AU to select the related
multimedia service and sends the request to CS.
3. CS→BS: When the CS delivers multimedia service request tabulation to MoDSS through legal BS, and multimedia service will be sent back through legal BS.
4. BS→MoDSS: The BS delivers the request list of the PT’s multimedia service to the MoDSS, and the multimedia data will be sent back via BS to PT.
5. MoDSS→PT: MoDSS sends the multimedia data to PT via BS.

3.1 Notation

\( ID_X \): the X’s identity
\( seat_n \): the seat number of n
\( mul_m \): the number of multimedia data m
\( \alpha, \beta \): nonces
\( h(\cdot) \): a one-way hash function
\( S_{prk_{X}}(M) \): use X’s private key to make a signature of message
\( V_{puk_{X}}(M) \): use X’s public key to verify a signature of message M
\( Sig_{i} \): the i-th digital signature
\( SK \): the session key shared between PT and BS
\( E_{SK}(M) \): use session key SK to encrypt the message M
\( D_{SK}(M) \): use session key SK to decrypt the message M
\( E_{puk_{X}}(M) \): use public key puk\(_X\) to encrypt the message M
\( D_{prk_{X}}(M) \): use private key prk\(_X\) to decrypt the message M
\( M_i \): the i-th message
\( C_i \): the i-th ciphertext
\( Cert_X \): the X’s certificate
\( g \): a public primitive element
\( P \): a permit message issued by BS
\( \tau \): a permit signature issued by BS, where

\[ \tau = S_{prk_{X}}(P) \]

\( T \): the valid time of session key SK
\( n \): the CA generates two large prime numbers p and q, and computes \( n = p \cdot q \)

\( A \neq B \): compare whether A is equal to B
\( \oplus \): the concatenation operation

3.2 Key generation phase

In this phase, the CA issues certificate Cert\(_X\) and public key puk\(_X\) for each party as follows:

Step 1: First, CA selects four large primes \( p, q, p', q' \) of almost the same size such that \( p = 2p' + 1 \) and \( q = 2q' + 1 \). CA computes \( n = p \cdot q \) and chooses a base element \( g \) of order \( p' \cdot q' \). CA keeps \( p, q, p' \) and \( q' \) secret to all users, where \( h(\cdot) \) accepts a variable-length input string of bits to generate a fixed-length output string of bits and \( h(m) < \min(p', q') \) denotes the minimal value of \( p' \) and \( q' \).

Step 2: When a PT, whose identity is ID\(_{PT}\), wants to join the system, CS randomly chooses a private key prk\(_{PT}\) and computes the PT’s \( y_i \).

\[ y_i = g^{p_{PT}} \mod n. \] (1)

Then, CS sends ID\(_{PT}\) and \( y_i \) to CA.

Step 3: After receiving ID\(_{PT}\) and \( y_i \), CA computes

\( puk_{PT} = (y_i - ID_{PT})^{h(\beta_{PT})} \mod n \) \hspace{1cm} (2)

as PT’s public key and issues Cert\(_{PT}\) to CS.

Step 4: CS verifies PT’s public key puk\(_{PT}\) is valid.
\[ puk_{pt}^{h(ID_{pt})} + ID_{pt} \equiv r^{p_{pt}} \mod n. \] (3)

### 3.3 Registration phase

In the registration phase, the PT wants to offer the MoD service for passengers; the PT proposes Cert_{pt} to MoDSS for requesting the MoD service. After verification, PT provides Cert_{pt} to MoDSS and MoDSS will provide ID_{MoDSS} and puk_{MoDSS} for PT. The scenario is described in Fig. 2.

**Step 1:** PT proposes Cert_{pt} to MoDSS for MoD service.

**Step 2:** MoDSS receives PT’s Cert_{pt} for verifying the identity. If the certificate Cert_{pt} is valid, MoDSS provides one’s own identity ID_{MoDSS} and public key puk_{MoDSS} for the PT to generate the parameters and encrypt messages in the communication phase.

![Figure 2](image-url) The scenario of registration phase

### 3.4 Authentication phase

In this phase, PT verifies the legitimacy of base station, and the BS_{n} generates a session key SK and permit \( \tau \) for authentication. The scenario is shown in Fig. 3.

**Step 1:** First, CS generates a request authentication message \( M_{auth} \) to BS_{n}, and the PT uses private key prk_{pt} to generate signature \( \text{Sig}_{1} \):

\[ \text{Sig}_{1} = S_{puk_{pt}}(\text{Cert}_{pt} \parallel M_{auth}). \] (4)

The CS sends \( (\text{Cert}_{pt}, \text{Sig}_{1}, M_{auth}) \) continuously, to the BS_{n} for verification.

**Step 2:** After receiving \( (\text{Cert}_{pt}, \text{Sig}_{1}, M_{auth}) \), the BS_{n} firstly verifies the correctness of certificate Cert_{pt}.

If the certificate is valid, the BS_{n} verifies the signature \( \text{Sig}_{1} \) with the public key puk_{n}:

\[ V_{puk_{n}}(\text{Sig}_{1}) = (\text{Cert}_{pt} \parallel M_{auth}). \] (5)

After verification, the BS_{n} chooses a valid time \( T \), and generates a permit \( \tau = S_{puk_{n}}(P \parallel T) \). (6)

and Cert_{pt}, then uses the public key puk_{CS} to encrypt \( (\text{Cert}_{pt} \parallel M_{rep} \parallel \tau \parallel T) \) into ciphertext \( C_{1} \):

\[ C_{1} = E_{puk_{CS}}(\text{Cert}_{BS} \parallel M_{rep} \parallel \tau \parallel T). \] (7)

![Figure 3](image-url) The scenario of authentication phase
The BS_{s} uses private key prk_{s} to generate a signature \( \text{Sig}_{2} \):
\[
\text{Sig}_{2} = S_{prk_{BS}}(\text{Cert}_{BS} \,||\, M_{\text{req}} \,||\, \tau \,||\, T). \tag{8}
\]
The BS_{s} then sends (\text{Cert}_{BS}, C_{1}, \text{Sig}_{2}, M_{\text{resp}}) to the CS for verification.

Step 3: Upon receiving (\text{Cert}_{BS}, C_{1}, \text{Sig}_{2}, M_{\text{resp}}), the CS firstly verifies the correctness of certificate \text{Cert}_{BS}. If the certificate is valid, the CS decrypts the ciphertext \( C_{1} \) to obtain (\text{Cert}_{BS} || M_{\text{resp}} || \tau || T) and verifies the signature \text{Sig}_{2}. The related computations are as follows:
\[
D_{prk_{CS}}(C_{1}) = (\text{Cert}_{BS} || M_{\text{resp}} || \tau || T), \tag{9}
\]
\[
V_{prk_{BS}}(\text{Sig}_{2}) = (\text{Cert}_{BS} || M_{\text{resp}} || \tau || T). \tag{10}
\]
The CS continuously stores \( \tau \) and \( T \). Besides, CS uses the \( \tau \) as the session key between PT and BS_{s}. PT also generates acknowledge message \( M_{\text{ack}} \) of the session key \( SK \).

Step 4: When receiving the acknowledge message \( M_{\text{ack}} \), the BS_{s} stores the (ID_{PT}, \tau) into database, and uses the \( \tau \) as the session key between PT and BS.

---

**Figure 4** The scenario of communication phase
3.5 Communication phase

In this phase, the passenger uses the OBU of the front seat to choose the desired multimedia data. The AU utilizes Chang et al.’s scheme to make a signature to send to MoDSS, which sends multimedia data to PT. BS encrypts multimedia data with copyright into a ciphertext for avoiding attacks; the scenario is shown in the Fig. 4.

Step 1: After choosing multimedia data, AU generates a multimedia content message $Content_{mul}$, the $Content_{mul}$ includes seat number $seat_n$, multimedia number $mul_n$ as follows.

\[ Content_{mul} = (seat_n, mul_n). \]  

(11)

CS continuously aggregates the P’s request.

Step 2: The PT integrates the passenger’s request into $M_{req}$, $M_{req} = (Content_{mul1}, Content_{mul2}, \ldots , Content_{muln})$.  

(12)

And chooses a random number $k$, MoDSS’s identity $ID_{MoDSS}$, MoDSS’s public key $puk_{MoDSS}$ and request message $M_{req}$ to generate three provable values: $r_1$, $r_2$, and $s$. The PT performs the following equations:

\[ r_1 = M_{req} \cdot (puk_{MoDSS}^{h(ID_{MoDSS})} + ID_{MoDSS})^{-k} \mod n, \]

(13)

\[ r_2 = M_{req} \cdot (puk_{MoDSS}^{h(ID_{MoDSS})} + ID_{MoDSS})^{-\eta} \mod n, \]

(14)

\[ s = r_1 \cdot k - prk_{PT} \cdot h(r_2). \]

(15)

The PT continuously sends $(r_1, r_2, s)$ to MoDSS via BS_n.

Step 3: As soon as it receives $(r_1, r_2, s)$, the MoDSS first decrypts and checks the validity of $M_{req}$. The MoDSS performs the following computation:

\[ M_{req} = r_2 \cdot g^t \cdot ((puk_{PT}^{h(ID_{MoDSS})} + ID_{PT})^{(\tau(TMEC))^{-k}})^{mod MoDSS} \mod n \]  

(16)

and verifies:

\[ (r_1 \cdot M_{req}^{-1})^\eta \mod n \overset{?}{=} (r_2 \cdot M_{req}^{-1})^{\eta(MoDSS)}. \]

(17)

If the requirement message $M_{req}$ of PT is authorized, the MoDSS searches the multimedia database and BS_n performs compression and division; then serial blocks $(M_1, M_2, \ldots, M_m)$ are generated. The MoDSS continuously chooses random number $k$ and uses the PT’s identity $ID_{PT}$ and $puk_{PT}$ to generate proofs $(t, d_1, d_2, \ldots, d_m, d, \sigma, s)$. The MoDSS performs the following computations:

\[ t = (puk_{PT}^{h(ID_{PT})} + ID_{PT})^{-k} \mod n, \]

(18)

\[ d_j = M_j \cdot (d_{j+1} \oplus t) \mod n \quad \text{for } i = 1, 2, \ldots, m, \]

(19)

\[ d = (d_1 || d_2 || \ldots || d_m), \]

(20)

\[ \sigma = h(d || t), \]

(21)

\[ s = k - prk_{MoDSS} \cdot \sigma \mod n. \]

(22)

Afterward, the MoDSS sends $(t, d_1, d_2, \ldots, d_m, d, \sigma, s)$ to PT via BS.

Step 4: After receiving $(t, d_1, d_2, \ldots, d_m, d, \sigma, s)$, the PT uses $ID_{MoDSS}$, $puk_{MoDSS}$ and $prk_{PT}$ to perform the following computations:

\[ d' = h(d_1 || d_2 || \ldots || d_m), \]

(23)

\[ d = d'. \]

(24)

PT computes $t'$ and checks the validity $\sigma$.

\[ t' = g^k \mod PT. \]

(25)

\[ \sigma = h(d'||t'). \]

(26)

If the PT passes the above verification, the CS computes $(M_1, M_2, \ldots, M_m)$ and $Data_{mul}$ as follows.

\[ M_i = d_i \cdot h(d_{i+1} \oplus t')^{-1} \mod n \quad \text{for } i = 1, 2, \ldots, m, \]

(27)

\[ Data_{mul} = M_1 || M_2 || \ldots || M_m. \]

(28)

CS continuously sends the related multimedia information to all passengers.

3.6 Handoff phase

In case of handoff, when the PT is moving away from its serving base station (BS_n) and the quality of service is worsening, it is necessary to transfer the connection from the original serving BS_n to a neighboring BS_{n+1} or BS_{n-1} to maintain the acceptable QoS and without the loss or interruption of service. We utilize certification and permit $\tau$ to carry on a two-way authentication between PT and BS, as shown in Fig. 5.

Step 1: First, the vehicle PT checks if the permit $\tau$ is valid, and computes a handoff request cipher $C_2$ (Including: a permit $\tau$, handoff request message $M_{hav}$ and valid time $T$) as follows:

\[ C_2 = E_{\tau}(\tau || M_{hav} || T). \]

(29)

Then the PT transmits $(C_2, Cert_{pr})$ to the BS_{n+1} or BS_{n-1}.

Step 2: While the BS_n receives the handoff request cipher, the neighborhood base station BS_{n+1} or BS_{n-1} decrypts the cipher with session key $\tau$. 

\[ D_{pr}(C_2) = (\tau || M_{hav} || T). \]

(30)

BS_{n+1} or BS_{n-1} will continuously verify the correctness of permit $\tau$ with PT’s public key $puk_{PT}$.

\[ V_{puk_{PT}}(\tau) = P || T. \]

(31)
4 Analysis and discussions

In this section, we discuss the security and notable issues. First, we discuss the security issue of our scheme and carry out a performance analysis.

4.1 Security issue

4.1.1 Impersonate PT attack issue

The attacker may try to impersonate PT to forge a valid signature; he/she will encounter the discrete logarithm problems difficulties. In section 3.5, \( r_1, r_2 \) and \( s \) are computed by PT’s random number \( k \) and private key \( prk_{PT} \) respectively, as follows:

\[
\begin{align*}
  r_1 &= M_{req} \cdot (puk_{BS_{n1}}^{ID_{BS_{n1}}} + ID_{BS_{n1}})^{-k} \mod n, \\
  r_2 &= M_{req} \cdot (puk_{BS_{n1}}^{ID_{BS_{n1}}} + ID_{BS_{n1}})^{-\gamma \cdot k} \mod n, \\
  s &= r_1 \cdot k - prk_{PT} \cdot h(r_2). 
\end{align*}
\]

However, if the attacker tries to forge \( r_1, r_2 \) and \( s \), it is impossible since the attacker will confront the difficulty of discrete logarithm problems (the unknown of PT’s private key \( prk_{PT} \) and random number \( k \)).

4.1.2 Replay attack issue

In the real world, an attacker may want to resend a legal signature or cipher as a legal message. To prevent this, the properties of authentication and confidentiality are used in our scheme. In the scenario of section 3.4, the PT or BS will verify the certificate \( Cert_{PT} \) or \( Cert_{BS} \) respectively, before the transaction. Also, the PT or BS examines the
certificate with the other session key r to maintain privacy in the scenario of section 3.6. Once the attacker replays the transmitted data, it is easily detected because of the uniqueness of the certificate. Without any knowledge of any other’s group session key, plain text or random numbers, the attacker cannot achieve a replay attack.

4.1.3 Hijacking attack issue

In our proposed scheme, the hijacking attack may occur if there is an adversary who holds the communication messages \((t, d_1, d_2, \cdots, d_m, d, \sigma, s)\). An adversary can enforce the scenario of impersonating the lawful party to deceive other lawful parties, and this is referred to as the Man-in-the-Middle attack, where the attacker wants to destroy or steal this multimedia data. It must know PT’s private key prkPT to recover multimedia data through the following computations:

\[
d' = h(d_1 || d_2 || \cdots || d_m),
\]

\[
t' = g^{\text{prkPT}},
\]

\[
\sigma = h(d'||t').
\]

After receiving \((t, d_1, d_2, \cdots, d_m, d, \sigma, s)\), the PT checks the integrity of the communication messages as follows:

\[
d'' = h(d_1 || d_2 || \cdots || d_m),
\]

\[
d = d'.
\]

Therefore, if an attacker tries to modify the communication messages \((t, d_1, d_2, \cdots, d_m, d, \sigma, s)\), he/she will not achieve a successful forgery. Therefore, our scheme is effective in preventing the hijacking attack.

4.1.4 DOS attack issue

The PT can offer the MoD service for passengers. However, in the real world, an attacker may want to interrupt the service offered by the PT by resending a legal signature or cipher as a legal message. To prevent this, authentication and confidentiality are used in our scheme. In the authentication and handoff phase, the authentication schemes are involved, in which the PT or BS will verify the certificate CertPT and CertBS before transaction. Once the attacker attempts to blockade the service, it is easily detected because of the unique certificate. Since the attack cannot pass the authentication proof in the authentication and handoff phase, he cannot interrupt the communication phase. Therefore, the attacker cannot achieve a DoS attack in our scheme, we can resist Dos attack successfully.

4.2 Authenticity issue

The authentication service is concerned with ensuring that the communication is authentic. The public transit should only react to disseminated messages or multimedia data generated by a legitimate base station.

Thus, the messages need to be authenticated by using a digital signature. As the receivers have received the messages with a signature in VANET, the public transit can use the originator’s public key to authenticate itself. The verifiable proofs are shown in Table 2.

<table>
<thead>
<tr>
<th>Evidence</th>
<th>Evidence Issuer</th>
<th>Evidence Holder</th>
<th>Evidence Verification</th>
</tr>
</thead>
<tbody>
<tr>
<td>(CertPT, Sig1, Mauth)</td>
<td>PT</td>
<td>BS</td>
<td>Vpubb (Sig1) \equiv (CertPT \parallel Mauth)</td>
</tr>
<tr>
<td>(C1, Sig2)</td>
<td>BS</td>
<td>PT</td>
<td>Vpubb (Sig2) \equiv (CertBS \parallel Mresp)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Encryption</th>
<th>Encryption Issuer</th>
<th>Decryption</th>
<th>Decryption Holder</th>
</tr>
</thead>
<tbody>
<tr>
<td>C1 = Epubb(CertBS \parallel Mresp \parallel t \parallel T)</td>
<td>PT</td>
<td>Dpubb(C1) = (CertBS \parallel Mresp \parallel t \parallel T)</td>
<td></td>
</tr>
<tr>
<td>C2 = E_t(t \parallel Mhand \parallel T)</td>
<td>PT</td>
<td>D_t(C2) = (t \parallel Mhand \parallel T)</td>
<td></td>
</tr>
<tr>
<td>C3 = E_t(t \parallel Tnew)</td>
<td>BS</td>
<td>D_t(C3) = (t \parallel Tnew)</td>
<td></td>
</tr>
</tbody>
</table>
4.3 Confidentiality issue
Confidentiality must be ensured in regard to the network handoff message and multimedia data-related message. Thus, the communication of multimedia data or the handoff request messages in a Vehicular Ad-Hoc Network (VANET) should be carried out under the utilization of PKI. Basically, the system needs a common authority organization trusted by all public transit which we refer to as CA. The CA issues these public/private keys and preloads them into all public transits. We take into account the specific aspects of our network environment and the use of the certificate in designing an appropriate PKI protocol. Our protocol conforms to the confidentiality issue as Table 3 shows.

4.4 Integrity issue
The data integrity issue can be ensured in our scheme since the replay attack or other malicious behaviors will be detected by checking the proof \((t, d_1, d_2, \ldots, d_m, d, \sigma, s)\) which consists of a signature and multimedia data. Upon receiving the multimedia, PT will check the integrity of the multimedia data \((d_1, d_2, \ldots, d_m)\) by the following operations:

\[
d' = h(d_1 || d_2 || \ldots || d_m),
\]
\[
d = d'.
\]

The proposed scheme maintains its integrity.

4.5 Handoff issue
We envision that each public transit will be outfitted with a receiver device and communication server for collecting information or multimedia data. In particular, we assume that public transit communication will become ubiquitous. A fixed infrastructure which comprises a number of base stations positioned in proximity to the highways is necessary.

Due to the fact that public transit travels at high speeds and simultaneously spends little time in communicating or broadcasting with the remote multimedia server, a secure handoff protocol [31-33], which is a notable security feature of vehicular networks, should be utilized. In our handoff phase, as a public transit moves from one region to another, its state is handed over from one base station to the next by carrying a permit \(\tau\).

Thus, cryptographic session key \(\tau\) of the public transit can be renewed by a periodic technical checkup. These features have been available and are of equal importance for receiving a new session key \(\tau_{new}\) from the new base station. Therefore, the handoff issue in our protocol is definitively assured.

4.6 Performance analysis
In this section, we evaluate the performance of our proposed scheme. While the AES-symmetric engages in encryption and decryption, digital signature and hash functions are applied in order to ensure the transmission security. We concentrate on the performance of the authentication, communication and handoff phases at both the PT and MoDSS side; we show the computation cost of our scheme in Table 4. We provide a security scheme to perform the transfer request with the multimedia data scenario; our protocol requires small time complexity of communications. We present the rounds of communication and the communication amounts between PT and BS of the proposed scheme in Table 5.

Finally, we assume the transmission rates of WiMax as 35 Mbps and 10 Mbps within a common realistic WiMax environment, for example: A 2 GB multimedia datum (it can be played approximately 130 min) is translated to conform to ISO/IEC 13818-2 criteria, and is split into 188 bytes for each transmission package [32]. Therefore, 2 GB is divided into \(2*10^6/188=10638298\) packs. The transmitted packages are 10638298 blocks. We use two transmission rates which are 35 Mbps and 10 Mbps to illustrate the communication cost. In the environment of 10 Mbps, the transmission time of the stream information is only 0.1024 ms/packet (Table 5 shows the 10 Mbps bandwidth, the communication cost of the communication phase is \((n+5)T_s + 2T_{ek} = (10638298+5)*10^4+320=1089362592\) bits, 1089362592*10^-6=1089362.2592 ms, 1089362.2592 ms/10638298 packs=0.1024 ms/packs). Therefore, the total communication cost \((n+10)T_s + 11T_{ek} + 2T_{ek} + 2T_{sk} + 4T_{sig}\) is 311264.55 ms for a 2 GB multimedia. The resulting time is good.
Conclusions

A secure public transport MoD system is proposed to allow passengers choose their favorite multimedia services during long hours of travel in public transport. Our scheme combines Wi-Max networks and integrates the cryptology to protect the copyrighted multimedia data. The performance is good. Moreover, the proposed scheme meets the following requirements:

1. Protects against known attacks; these attacks include: prevent an impersonation public transport (PT) attack, prevent a replay attack, prevent a hijacking attack, and prevent a Denial of Service (DoS) attack.
2. Authenticity;
3. Confidentiality;
4. Integrity;
5. Handoff.

In the future, we hope that the proposed scheme can be applied widely to various public transport systems such that public transport companies can provide more value-added services for passengers, and enhance their interest in taking public transportation.

<table>
<thead>
<tr>
<th>Phase</th>
<th>PT</th>
<th>BS(or MoDSS)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication phase</td>
<td>$1T_D + 1T_S + 2T_{verf}$</td>
<td>$1T_E + 2T_S + 2T_{verf}$</td>
</tr>
<tr>
<td>Communication phase</td>
<td>$(n+2)T_{mul} + 2T_{mmul} + 6T_{exp} + 4T_h + 2T_{verf}$</td>
<td>$1T_{mul} + (n+5)T_{mmul} + 10T_{exp} + 5T_h + 1T_{verf}$</td>
</tr>
<tr>
<td>(to MODSS)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Handoff phase</td>
<td>$1T_{SK} + 1T_D$</td>
<td>$1T_{SK} + 1T_D + 1T_S + 2T_{verf}$</td>
</tr>
<tr>
<td>Total</td>
<td>$2T_D + 1T_{SK} + 1T_S + 4T_{verf}$</td>
<td>$1T_D + 1T_{SK} + 1T_S + 5T_{verf}$</td>
</tr>
<tr>
<td></td>
<td>$+(n+2)T_{mul} + 2T_{mmul} + 6T_{exp} + 4T_h$</td>
<td>$+1T_{mul} + (n+5)T_{mmul} + 10T_{exp} + 5T_h$</td>
</tr>
</tbody>
</table>

Notes:

$T_E$: the time for executing an asymmetric encryption operation.
$T_D$: the time for executing an asymmetric decryption operation.
$T_{SK}$: the time for executing a symmetric encryption / decryption operation.
$T_S$: the time for verifying a signature.
$T_{mul}$: the time for multiplication without module $N$.
$T_{mmul}$: the time for multiplication with module $N$.
$T_{exp}$: the time for exponentiation with module $N$.
$T_h$: the time for executing a one-way hash function.
$T_{verf}$: the time for verification.

<table>
<thead>
<tr>
<th>Phase</th>
<th>Cost</th>
<th>Data transmission time (ms/packs)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>35 Mbps</td>
</tr>
<tr>
<td>Authentication</td>
<td>$1T_E^* + 4T_S^* + 3T_{msg}$</td>
<td>0.14697</td>
</tr>
<tr>
<td>Communication</td>
<td>$(n+5)T_S^* + 2T_h^*$</td>
<td>0.02923</td>
</tr>
<tr>
<td>Handoff</td>
<td>$2T_{SK}^* + 1T_T^* + 1T_{msg}$</td>
<td>0.04411</td>
</tr>
</tbody>
</table>

$T_E^*$: the time of transmission a one-way hash function (160 bits).
$T_D^*$: the time of transmission an asymmetric ciphertext (1024 bits).
$T_{SK}^*$: the time for executing a symmetric encryption / decryption operation (256 bits).
$T_S^*$: the time of transmission a signature (1024 bits).
$T_{msg}$: the time of transmission message code (8 bits).
$n$: the divided blocks of the multimedia.

<table>
<thead>
<tr>
<th>Phase</th>
<th>Cost</th>
<th>Data transmission time (ms/packs)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>35 Mbps</td>
</tr>
<tr>
<td>Authentication</td>
<td>$1T_E^* + 4T_S^* + 3T_{msg}$</td>
<td>0.14697</td>
</tr>
<tr>
<td>Communication</td>
<td>$(n+5)T_S^* + 2T_h^*$</td>
<td>0.02923</td>
</tr>
<tr>
<td>Handoff</td>
<td>$2T_{SK}^* + 1T_T^* + 1T_{msg}$</td>
<td>0.04411</td>
</tr>
</tbody>
</table>

$T_E^*$: the time of transmission a one-way hash function (160 bits).
$T_D^*$: the time of transmission an asymmetric ciphertext (1024 bits).
$T_{SK}^*$: the time for executing a symmetric encryption / decryption operation (256 bits).
$T_S^*$: the time of transmission a signature (1024 bits).
$T_{msg}$: the time of transmission message code (8 bits).

5 Conclusions

A secure public transport MoD system is proposed to allow passengers choose their favorite multimedia services during long hours of travel in public transport. Our scheme combines Wi-Max networks and integrates the cryptology to protect the copyrighted multimedia data. The performance is good. Moreover, the proposed scheme meets the following requirements:
This research was supported by the Ministry of Science and Technology, Taiwan, R.O.C., under contract number MOST103-2632-E-324-001-MY3, MOST 103-2221-E-324 -023, MOST 103-2622-E-212-009 -CC2 and MOST 104-2221-E-324-012.

Acknowledgements

References


**Biographies**

**Chin-Ling Chen** received his PhD from National Chung Hsing University, Taiwan in 2005. From 1979 to 2005, He was a senior engineer at Chunghwa Telecom Co., Ltd. He is a professor. His research interests include cryptography, network security and electronic commerce. He has published over 70 articles in SCI/SSCI international journals.

**Ming-shaw Lu** received his M.S. degree at the Institute of Information Management and Computer Science, Chaoyang University of Technology in 2010. His research interests include cryptography, vehicular communication and radio frequency identification system.

**Jian-Wei Li** received Ph.D. in Computer Science and Information Engineering from National Cheng Kung University, Taiwan, in 2008. Currently, he is an assistant professor in the Department of Information and Communication Engineering, Chaoyang University of Technology, Taiwan. His research interests include Wireless and Mobile Communication Protocols, Wireless and Mobile Network Security.

**Changqing Gong** is a professor in Shenyang Aerospace University China. He received his Ph. D. from Northeastern University China in 2006. His research interests include IPv6, VANET, MANET, and cloud computing.

**Liang Zhao** is currently a lecturer in Shenyang Aerospace University China. He worked as associate senior researcher in Hitachi (China) Research and Development Corporation from 2012 to 2014. He received his PhD degree from Edinburgh Napier University in 2011. His research interests include WMNs, VANETs, MANETs, and Intelligent Transport Services.