STATE OF THE ART ON SECURE AND LOW COST RFID AUTHENTICATION PROTOCOLS FOR RFID BASED VEHICLE LICENSE PLATE

Irfan Syamsuddin
CAIR - Center for Applied ICT Research
Department of Computer and Networking Engineering
State Polytechnic of Ujung Pandang, Makassar, Indonesia
Emails: irfans@poliupg.ac.id

Submitted: July 15, 2013 ***Accepted: Oct. 30, 2013*** ***Published: Dec. 16, 2013***

Abstract- RFID technology has many potential applications that would ease object identification seamlessly. One of its potential benefits to government is the adoption of RFID tag as embedded smart material within vehicle license plate. However, adoption of RFID in vehicle license plate is fragile from various RFID attacks while efforts to improve its security will lead to additional cost. Enhancing RFID security without extra cost poses new challenges to researchers in the area. This study aims to provide a state of the art on RFID authentication protocols under low cost restriction as a foundation for decision maker for further development stage of RFID based vehicle license plate. In depth analysis is performed by assessing the protocols according to three features namely data protection, tracking prevention, and forward security. Finally, it is concluded that the protocols are vary in satisfying three aspects of security features.

Index terms*:* RFID, vehicle plate license, smart identification, security and privacy, low cost, data protection, tracking prevention, and forward security.

I. INTRODUCTION

Radio Frequency Identification (RFID) is a technology to simplify automatic identification of objects with electromagnetic fields. In general, RFID tags can be divided into two categories, active and passive. Active tags require a power source, while passive ones do not rely on power source. This paper interests on passive tags because the tags do not require batteries and low production and maintenance cost. In addition, they also have an indefinite operational life and are small enough to fit into a practical adhesive label.

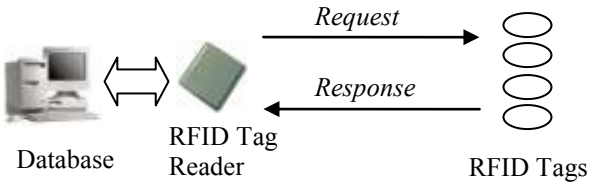

Figure 1. RFID communication model

Generally, RFID systems consist of Radio Frequency Identification (RFID) tags and RFID readers. While RF tags operate as transponders, RF readers act as transceivers. In case of a more complex application, a database server is required to store information comes from both transponders and receivers sides [1].

The bandwidth for RFID communication systems is relatively low in several kBit per second. Although this is very small compared to other wireless technologies, recent modes offer higher data rates due to only small data is exchanged with a single tag. The bandwidth is more appropriate to perform scanning to all tags in the operation range of a reader within a short time [5].

Low cost RFID is attractive for wider implementation (replacing magnetic stripe cards and classical contact smartcards) in logistics, point-of-sale checkouts, animal identification, item management in libraries, and waste management [2]. In addition, more sophisticated RFID tags are used for higher value items in more complex applications such as ticketing, electronic purse, key, access control for various facilities, and even for human body [2,34].

In this paper, author look at its potential application in vehicle management in developing

countries by embedding RFID tag within vehicle license plate. Hwang, et.al [33] describes various techniques used to design a prototype of RFID based vehicle license plate in 900 MHz band. Through such innovation it is believed that government will have a better automatic public vehicles management while simplify road toll and it also may be used as anti-theft device for vehicles [31,32].

The issue is low cost RFID tag difficult to provide strong security and privacy mechanism, while improving high level of security will lead to increasing of RFID cost. Leaving government in developing country to adopt low cost and unsecure RFID tag to deal will public vehicle management will eventually result in security and privacy issues in the future.

Therefore, it is important to look at state of art on RFID authentication protocols that compromise security mechanisms in one hand and keeping low cost of RFID tag production on the other hand. This review provides foundation for academia, professionals and government policy makers to decide which protocol to be adopted in the future.

In the second section, several RFID attacks and its characteristics are described. Section 3 serves as literature review for several RFID authentication protocols under low cost boundaries. In addition, in depth evaluation of the protocols based on three security and privacy perspectives namely data protection, tracking prevention, and forward security are given in section 4. Eventually, conclusions and future research direction are drawn in the last section.

II. RFID ATTACKS

Attacks on RFID technology has been a hot area of research. Inherently, RFID was designed with lack of security and privacy mechanism which eventually leads to different types of attack. This paper classifies these attacks according to the location where the attacks occur. In this regard, attacks location are categorized into air interface, reader, and systems.

A. Attacks on the Interface

RFID suffers from this kind of attack which occurs on the interface. Examples of this type are eavesdropping, jamming, relay and replay attacks. Eavesdropping is considered as basic threats to RFID systems. In this case, eavesdroppers could impersonate a target tag without knowing the tag's internal secrets. The eavesdropped information could for example be used to collect privacy sensitive information about a person [12][13].

Jamming attack means a deliberate attempt to disturb the air interface between RFID reader and tag and thereby attacking the integrity or the availability of the communication. This could be achieved by powerful transmitters at a large distance, but also through more passive means such as shielding. As the air interface is not very robust, even simple passive measures can be very effective [14].

A relay attack [15] for contactless cards is similar to the well known man-in-the-middle attack. In this type of attack, attacker sits in the middle of two ways communications and receives data from with both the reader and the victim's card. It is proven that this kind of attack also able to collect sensitive information of the RFID users.

In contrast to relay attack, in replay attack an attacker reuses communications from previous sessions to perform a successful authentication between a tag and a server. If a valid RFID signal can be intercepted and the data is recorded, this data can later be retransmitted to the reader. Because the data appears valid, the system accepts it and therefore users' information can be gained inappropriately. [16]

B. Attacks on the Readers

In contrast to previous type of attack, the main target of this kind of attack is the reader. It attempts to falsify reading processes. Physical attack is an example of this type. It is the most common and considered as the most traditional attack which may lead to denial of service attack if the RFID tags are removed or broken. Unauthorized person could remove tags or put in foil-lined booster bag that will block RFID reader's request and temporarily deactivate the tag.

Another example of attack is falsifying reader ID. In a secure RFID system the reader must authenticate to the tag. Illegal reader may falsify reader ID by faking the "identity" of an authorized reader. In this case, an attacker able to read the data with his own reader, although such an attack can be "very easy" to "practically impossible" to carry out which is depending on the security measures in place.

C. Attacks on the Systems

In this category, attacks fall into three types, flooding attack, RFID exploit and RFID worm and virus. Flooding attack is performed against the database systems of RFID. If it is flooded with useless data then it will lead to denial of service attack. An attacker could attach RFID on other items causing RFID system to record useless data which will flood an RFID system with more

data it can handle.

RFID exploits are attack on RFID which is similar to software in general such as buffer overflows, code insertion and SQL injection. RFID worms and Viruses on the other hand is malicious code which is basically an RFID exploit that downloads and executes remote malwares. A worm could propagate through the network or through tags. Similarly, an RFID virus starts with malicious content of a tag. When the tag is read out, this initiates a malicious SQL query which may disturb the database in the back office. This type of attack already has been demonstrated.

In order to deal with the attacks, researchers have put their best efforts to design and test RFID authentication protocols in various ways. In the case of developing country, since decision to embed RFID tag within vehicle license plate is significantly depend upon minimum cost of implementation, finding appropriate security solution under low cost circumstances is essential for decision makers.

III. LOW COST RFID AUTHENTICATION PROTOCOLS

Increasing RFID security and privacy threats in the past decade have resulted in tremendous number of authentication protocols. However, increasing security and privacy mechanisms usually leads to increase of RFID tag cost. This is considered as a very challenging task where the protocol should provides strong RFID authentication mechanism within the low cost limitation. Low cost RFID tags are very limited devices with very constrained (less than 1K logic gates to security related tasks) computationally.

In current literature [35], there are nine protocols that strictly consider low cost boundaries while offering robust security and privacy mechanism in various ways. They are One Time Password introduced by Juels, et.al [2] with a simple XOR operation. External Re-Encryption as proposed in [4] which utilize simple public key cryptosystem, Hash-based Authentication developed by Ohkubo et al. [7], Blocker Tag as a simple RFID tag blocking mechanism offered in [3], Extended Hash-lock by Weis et al. [8], Hash-based Varying Identifier as another protocol with hash function proposed in [5], Improved Hash-based Varying Identifier as proposed in [9] which focus on preventing “man in the middle” attack under low cost RFID circumstances, Mutual Authentication protocols as presented in [10,11,28], Ultra Lightweight method which was

introduced by Peris-Lopez . [24,26,27].

In depth discussion and analysis the protocols mentioned above are provided in the following sections.

IV. ANALYSIS AND DISCUSSION

In this section, assessment of the low cost authentication protocols will be based on three main security and privacy features namely data protection, tracking prevention, and forward security.

The term of data protection refer to ability to maintain data confidentiality and privacy of tag bearers. While tracking prevention refers to protection capability of location privacy of tag bearers, and forward security means ability to preserve history even after the secrets or keys have been exposed.

A. One-time Pad based on XOR

This method was proposed by Juels [2]. It requires a very simple XOR operation, therefore low computational cost for RFID is satisfied. A reader (or a back-end server) has the common list of randomly generated key for each tag. The reader and the tag find that both of them have the same key of the key list with several message exchanges between them. Then, the tag transmits its ID to the reader. However, this method needs several message exchanges for authentication between the tag and the reader. Besides, the common key list must be refreshed to guarantee the security. Although it seems provide appropriate tracking protection, it could not satisfy data privacy protection. Another limitation is that the protocol does not provide forward security. These are problems for implementation and system efficiency.

Illustration of passive attacks on XOR based RFID protocol is presented in [36].

If $n1, n2 \bmod 96 = 0$

Then

$MixBits(0 \bmod 96, 0 \bmod 96) = 0 \bmod 96$

$C = ROT((ROT(n3 + K1^* + \pi + n1', n3) + K2^* \oplus n1', n2) \oplus n1'$

In case that $n1, n2, n3, n1' \bmod 96$ all become ZEROs

Hence

$C = K1^* + \pi + K2^*$

$K1^*+K2^*=C-\pi$

Similarly

$D = ROT((ROT(n2+K2^*+ ID+n1', n2) +K1^* +n1', n3) +n1'$

$= K1^*+ID+K2^*$

Then $K1^* + K2^* = D - ID$

$IDS^{next} =ROT ((ROT (n1'+K1^*+IDS+n2',n1')+K2^* \oplus n2', n3) \oplus n2'$

$= K1^* + IDS + K2^*$

$K1^* + K2^* = IDS^{next} - IDS$

As a result $ID = D – C + \pi$

Also $ID = D - IDS^{next} + IDS$

And $C-\pi = IDS^{next} - IDS$

While observing the external exchanged public messages, if two successive authentication sessions satisfy final equation, then the secret value of ID is compromised and will be easily obtained by attacker [36].

B. External Re-Encryption Scheme

External Re-Encryption Scheme was proposed in [14]. This method is aimed at protecting RFID security by using public key cryptosystem. This scheme is considered as a low cost protocol since it only utilizes two main mechanisms to authenticate RFID communications.

First, tag data is re-encrypted when a user requires using the data transferred from an external unit. As public key encryption needs high computation cost, a tag cannot process for itself. Thus, this job is generally processed by a reader.

Second, each tag data is randomly shown until next session, the attacker eavesdrop the tag data cannot trace the tag for long-term period therefore, data privacy protection is guaranteed. B

However, this method has limitations to frequently refresh each tag's data since the encrypted ID stored on tag is constant so that user location privacy is compromised. Therefore, it does not fully protect users' privacy. In addition, forward security is not covered by this protocol.

C. Hash Chain-based Scheme

Ohkubo et al. [7] proposed a hash-based authentication protocol. The aim of the protocol is to provide better protection of user privacy with the basic concept of refreshing the identifier of the

tag each time it is queried by a reader. The protocol changes RFID identities on each read based on hash chains. Hash chain method is used in this two ways communication of RFID tag. This work was adopted in [30] by enhancing unilateral randomly authentication protocol using one-way hash function. Even though the protocol does not require a random number generator, it seems satisfy data protection of RFID tags as well as provides adequate tracking prevention. However, this protocol is flawed to certain replay attacks which makes it difficult to guarantee forward security.

D. Blocker Tag

This protocol was introduced by Juels, et.al. [3]. The approach uses an individual tag, namely blocker tag for each tag and according to its purpose. To protect a tag's data, the blocker tag responses for attacker's request to get the tag's data. The response from the blocker tag is not for the tag but all tags. Thus, the attacker cannot distinguish the tag's data. This method basically uses binary tree walking protocol as a collision-avoidance mechanism as can be seen in figure 1.

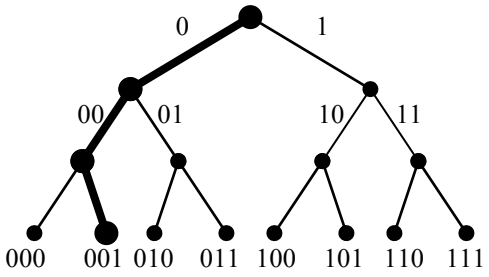

Figure 2. Concept of binary tree walking

Using the binary tree-based protocol, this method has advantages that the range of protecting tags can be efficiently specified into specific area of the binary tree [3]. Doing so, the area of protecting tags is divided into multiple privacy zones and the performance of tree walking can be efficient. This method also provides zone policy to apply protection policy according to various purposes. This method is currently considered as a practical solution for the existing RFID privacy and security protection by adequately maintain tracking prevention and forward security. Problem is that additional blocker tag is needed for every tag and it is susceptible whether tag

bearers strictly follow to attach the additional tag which could pose user privacy.

E. Extended Hash-lock Scheme

The next RFID protocol with low cost constraint is called Extended Hash-lock. It is an authentication scheme introduced by Weis [8] in 2003. It was actually developed in two types, namely hash-lock and extended hash-lock schemes. However, the last name is widely used to identify this unique protocol. Both protocols employed different ways of hash functions.

As can be seen in figure 3, hash-lock scheme uses a back-end server to store keys k in its database for all tags. Each tag unique key with metaID = h(k) as its key. The tag transmits metaID as a response to a reader's query to the tag. Unfortunately, this protocol fails to overcome eavesdrop attacks since metaID is always constant which opens tracing problem. Therefore, location privacy of tag bearers is compromised.

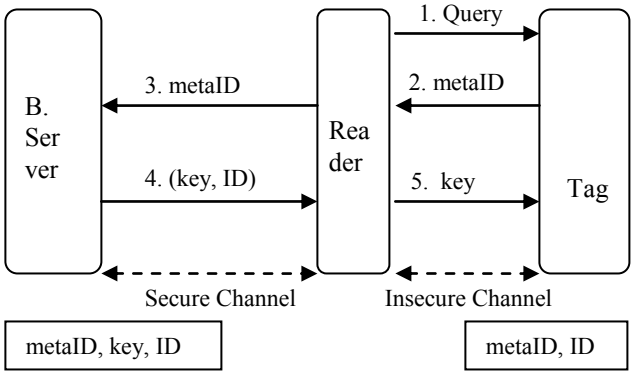

Figure 3: Hash-lock Scheme

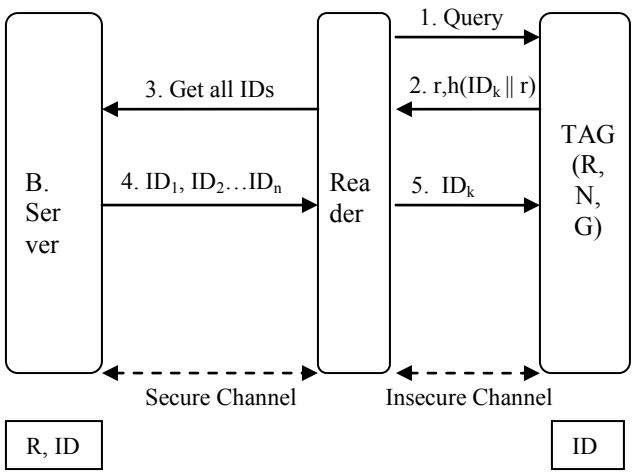

Figure 4. Extended Hash-lock Scheme

On the other hand, extended hash lock protocol [8] provides a unique method to overcome the tracing problem. Figure 4 shows what they called as extended hash-lock scheme. In this scheme, they introduced a tag with random number generator to randomize metaID value. The tag picks pseudo random number r uniformly and calculates *c=hash(IDjjr)* as the tag's unique identification for every session. The tag transmits its c and r to a back-end server by way of the reader. The server sends the unique identifier of the tag comparing c with the construction of r and all IDs that is stored in database of the server, then the server authenticates itself by sending the unique identifier, ID back to the tag.

Although this scheme provides strong authentication and prevents from the replay attacks, the tag can be traced if the tag's ID is exposed. In addition, an adversary can query a tag to get a tag's valid message pair (c; r). Later on, the attacker can impersonate that tag to a legitimate reader. As a result, the protocol could not fully satisfy data protection and forward security issues.

F. Hash-based Varying Identifier

Another hash-based approach is hash-based varying identifier proposed by Henrici and Muller [5]. Their scheme also adopts a hash function and a random number generator, but a pseudo random number is generated by a back-end server and transmitted to the tag for every interrogation to make the tag's queried identifier random and preserve location privacy.

They assume that the communication channel between tags and readers is insecure, while the

communication channel between readers and back-end databases is secure. A tag has only a unique identifier and remaining original data used for applications stored and controlled in a back-end database.

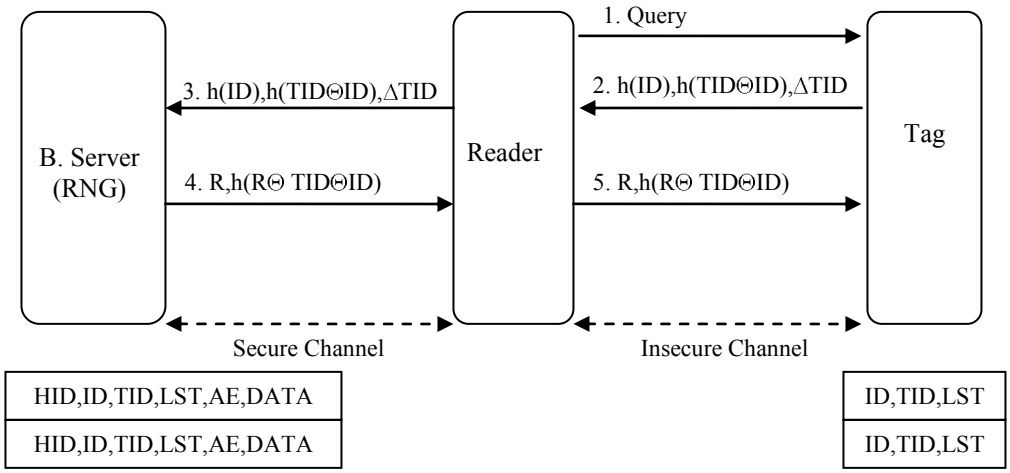

Figure 5: Hash-based Varying Identifier

Figure 5 shows the overall system architecture of this protocol is quite similar to that of other previous works. In server side, DataBase-ID is exist and is set according to the database which will be in charge of the tag and ID, TID and LST of a tag. These are set to a random value initially. A corresponding row in the database ID, TID and LST is similar to the tag. Then HID is set to h(ID) and is used as a primary index. The database manages a pair of record to guarantee message recovery for any data loss using AE fields which pointing each other.

This protocol basically focuses on securing location privacy problems by making a tag's ID randomized in every interrogation. However, location privacy of tag bearers is compromised since the response of tag is constant until the next authentication session. Therefore, attackers able to track tag bearers whose tags are long-distance from readers and scarcely have chance to be queried.

Yet, by employing TIDs, the replay attacks cannot compromise the scheme since tags and back-end servers are mutually authenticated in every single interrogation. Errors in message transfer can be detected and the scheme is reliable for data loss since it can provide the data from the previous record. In short, forward security is not well provided.

G. Improved Hash-based Varying Identifier

Hwang et al. [9] proposed an improved authentication protocol of hash-based varying identifier. The main difference between this protocol and the previous ones is that a reader utilizes what is called a random number generator (RNG) to protect the man-in-the-middle attack.

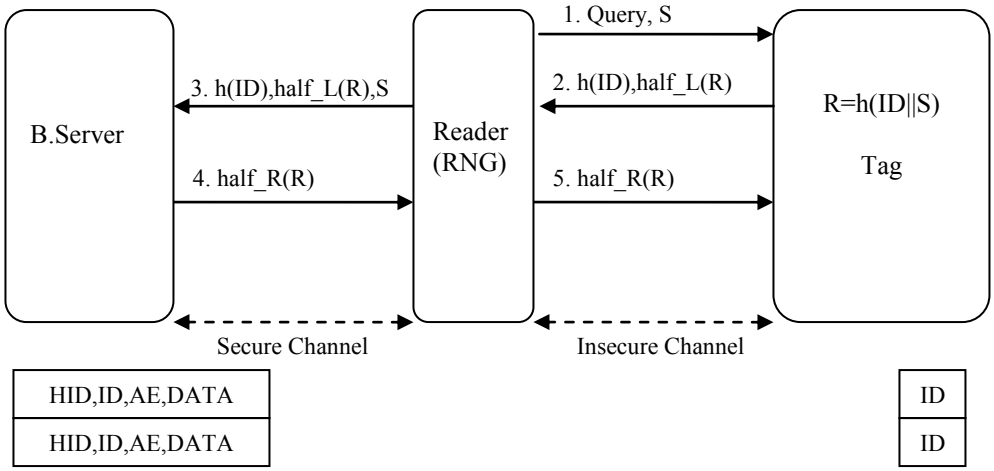

Figure 6: Improved Hash-based Varying Identifier

The above graph shows the overall protocol of Improved Hash-based Varying Identifier. In every query, the reader sends a pseudo-random number, S, to the tag. Then the tag replies h(ID) for finding the record of a back-end server and half of a new identifier, $hal_{fL}(R)$ (R = h(ID||S). Then, the reader forwards h(ID), $hal_{fL}(R)$, and S. At the back-end server, h(ID) is used to find the corresponding record and ID is obtained for authentication process. With stored ID and S received from the reader, the back-end server can calculate R' = ID||S and also the tag can be authenticated by comparing $hal_{fL}(R')$ with the value of $hal_{fL}(R)$ from the tag. If the authentication is successful, then the remaining job is updating ID of the record to a new ID = R' and h(ID) to h(R0), and then updating AE fields of the pair of record to reference each other. Then, the back-end server replies $hal_{fL}(R)$ with tag

data to the tag by way of the reader. With halfR(R), the tag can check whether the reply message is valid or not. If the process is successful, the tag and the back-end database updates its ID ← ID ⊕ (R||R) since they assume the hash function of this protocol is h : {0; 1}* → $\{0; 1\}^{0.5L}$ and R generated by this hash function is 0.5L bits.

Unlike previous protocols, this one changes the location of a R.N.G. from a back-end server to a

reader as a new model. As a result, this scheme needs only 1*l*-field for a unique ID and its challenge and response phase uses a half length of R (R = h(ID||S)) so that its communication performance is more efficient than [7]. The scheme protects the location privacy as a tag's unique identifier is changed in every read attempts. The replay attacks cannot compromise the scheme since tags and back-end servers are mutually authenticated.

However, this scheme is still vulnerable to the man-in-the-middle attack particularly if there is no guarantee that the reader is a trusted party. In short, although the protocol is claimed appropriate to protect traceability of user privacy, the protocol is still suffered from such attacks due to the ID of the tag remains constant until the next authentication session. During this limited period, adversaries can track tag bearers whose tags are long-distance from readers and scarcely have chance to be queried.

H. Mutual Authentication

In [10] Han et al. proposed a new mutual authentication protocol for RFID tags. The RFID reader and tag carry out the authentication based on their synchronized secret information. The synchronized secret information is monitored by a component of the database server. Although, this protocol is claimed satisfies the low-cost requirement of RFID tags, it's highly dependable on back-end database is confirmed as a serious limitation [11].

Highly dependent on database server is criticized in [28]. In reality, connection between the RFID reader and the central database do not always available thus fully relying on a central database means creating a single point of failure, opening up the entire RFID system to denial of service attacks [28].

In addition, two types RFID mutual authentication protocols both without database server was proposed. The first protocol performs challenge and response before sending the tag secret to the reader, whilst in the second version the tag secret is sent in such a way that only an authenticated reader can decrypt it.

This work was then improved in [11] which enable the removal of reliable consistent connections between RFID readers with their database server without the timestamps as can be seen from figure 7.

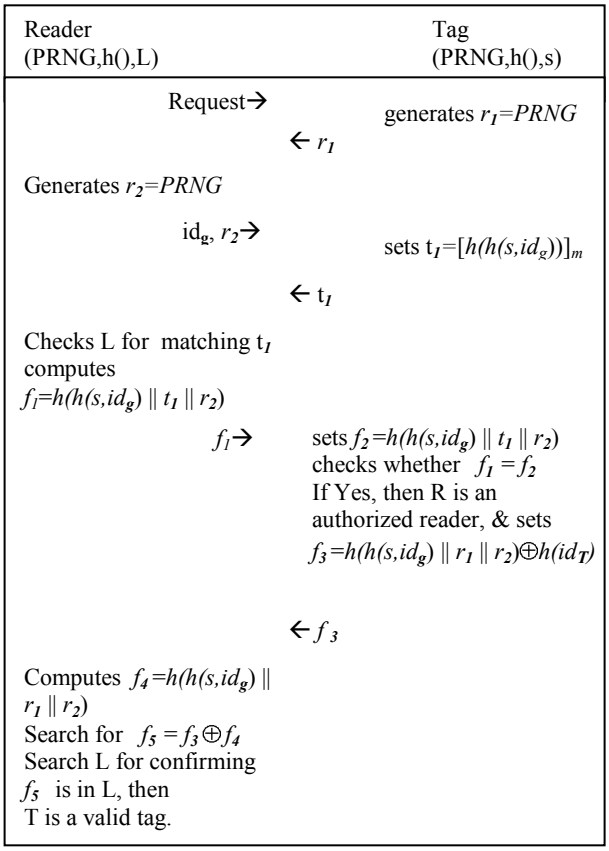

Figure 7. Mutual authentication without database

The protocol enables not only RFID tag to authenticate RFID reader but also the latter to authenticate RFID tag. It is confirmed that the protocol satisfy the requirement of both data protection and tracking prevention [11]. However, we found that it does not fully guarantee forward security.

I. Ultra Lightweight

While various hash formulas are usually applied to increase RFID security, ultra-lightweight security proposed by Lopez et.al [24],[26],[27] maintain security and privacy of RFID using simple operation. They introduced three protocols namely, Lightweight Mutual Authentication Protocol (LMAP) [24] and Minimalist Mutual-Authentication Protocol (M2AP) [26] and Efficient Mutual Authentication Protocol (EMAP) [27]. Instead of using advanced hash formula, they use XOR, OR, AND, mod 2m.. In general, the protocols use a 480 EEPROM and a 96-bit

key divided into 4 parts updates after each message cycle. Preventing users from privacy location tracking and re-transmission attacks is the key feature of the protocols [24],[26],[27].

- Message generation process

$A=IDS_{tag(i)} \oplus K1_{tag(i)} \oplus n1$ $B=(IDS_{tag(i)} \vee K2_{tag(i)})+n1$

$C=IDS_{tag(i)}+K3_{tag(i)}+n2$ $D=(IDS_{tag(i)}+ID_{tag(i)})) \oplus n1 \oplus n2$

- Key renewal process

$IDS_{tag(i+1)}=(IDS_{tag(i)}+(n2 \oplus K4_{tag(i)})) \oplus ID_{tag(i)}$

$K1_{tag(i+1)}=K1_{tag(i)} \oplus n2 \oplus (K3_{tag(i)}+ID_{tag(i)})$

$K2_{tag(i+1)}=K2_{tag(i)} \oplus n2 \oplus (K4_{tag(i)}+ID_{tag(i)})$

$K3_{tag(i+1)}=(K3_{tag(i)} \oplus n1)+(K1_{tag(i)} \oplus ID_{tag(i)})$

$K4_{tag(i+1)}=(K4_{tag(i)} \oplus n1)+(K2_{tag(i)} \oplus ID_{tag(i)})$

Figure 8. LMAP Scheme

LMAP protocol uses only 300 gates to provide security (see figure 8), the 96 bit key is divided into 4, which produce 4 messages, by which the reader sends A, B, C messages to the tag. To provide authentication, the tag replies with a D message, in accordance with messages A, B, and C [24]. However, there are risks of data forgery and fabrication during transfer [28]. If the final session is concluded irregularly, then the IDS and key values are not refreshed. This will expose identical values by which location tracking is possibly occurs.

- Message generation process

$A=IDS_{tag(i)} \oplus K1_{tag(i)} \oplus n1$ $B=(IDS_{tag(i)} \wedge K2_{tag(i)}) \vee n1$

$C=IDS_{tag(i)}+K3_{tag(i)}+n2$ $D=(IDS_{tag(i)} \vee K4_{tag(i)})) \wedge n2$

$E=(IDS_{tag(i)}+ID_{tag(i)})) \oplus n1$

- Key renewal process

$IDS_{tag(i+1)}=(IDS_{tag(i)}+(n2 \oplus n1)) \oplus ID_{tag(i)}$

$K1_{tag(i+1)}=K1_{tag(i)} \oplus n2 \oplus (K3_{tag(i)}+ID_{tag(i)})$

$K2_{tag(i+1)}=K2_{tag(i)} \oplus n2 \oplus (K4_{tag(i)}+ID_{tag(i)})$

$K3_{tag(i+1)}=(K3_{tag(i)} \oplus n1)+(K1_{tag(i)} \oplus ID_{tag(i)})$

$K4_{tag(i+1)}=(K4_{tag(i)} \oplus n1)+(K2_{tag(i)} \oplus ID_{tag(i)})$

Figure 9. M2AP Scheme

Similar to LMAP, M2AP protocol also employs 300 gates. As shown in figure 9, the only difference is that in this protocol there is an additional E value to add more security in database authentication compare to LMAP method [26]. Though it is efficient in that it uses some calculations for authentication, [28] confirm that it fails to provide strong integrity since it does not use hash formulas or encryption algorithms. Therefore, there is a possibility to track user location when the final session is concluded irregularly and also the IDS and key values are not refreshed.

The last protocol is called Efficient Mutual Authentication Protocol or EMAP. This method is considered as the most efficient method among ultra-lightweight protocols, since it only uses 150 gates to provide security of RFID [27]. In his method, the 4 keys, which have been divided from message E, produce the XOR algorithm sigma value (K1K2K3K4) by which provide a more accurate way of authentication. The 96 bit ID can be divided into two, resulting in the use of a 1~48 bit ID and a 49~96 bit ID, which results in the use of 2 identification values. By inputting the key value into the formula, the safety of the system is enhanced. This method is more effective than the two previously mentioned systems, and can provide security within close ranges. However, it can be exposed to 3rd party tapping, message fabrication, or forgery over long ranges [28].

- Message generation process

$A=IDS_{tag(i)} \oplus K1_{tag(i)} \oplus n1 \qquad B=(IDS_{tag(i)} \wedge K2_{tag(i)}) \vee n1$

$C=IDS_{tag(i)}+K3_{tag(i)}+n2 \qquad D=(IDS_{tag(i)} \vee K4_{tag(i)})) \wedge n2$

$E=(IDS_{tag(i)} \wedge n1 \vee n2) \oplus ID_{tag(i)} \oplus_{i=1}^{4} Ki_{tag(i)}$

- Key renewal process

$IDS_{tag(i+1)}=(IDS_{tag(i)}+(n2 \oplus n1)) \oplus ID_{tag(i)}$

$K1_{tag(i+1)}=K1_{tag(i)} \oplus n2 \oplus (K3_{tag(i)}+ID_{tag(i)})$

$K2_{tag(i+1)}=K2_{tag(i)} \oplus n2 \oplus (K4_{tag(i)}+ID_{tag(i)})$

$K3_{tag(i+1)}=(K3_{tag(i)} \oplus n1)+(K1_{tag(i)} \oplus ID_{tag(i)})$

$K4_{tag(i+1)}=(K4_{tag(i)} \oplus n1)+(K2_{tag(i)} \oplus ID_{tag(i)})$

Figure 10. EMAP Scheme

Although the method is quite unique and fit to low cost limitation, the three protocols also

criticized in terms of several weaknesses. As confirmed by Li et.al [29] who reveal these weaknesses by arguing that the protocols are not robust since there is no guarantee that the tag really recognize whether the replying messages are indeed received and verified by a legitimate reader or not.

As illustrated in [29], bit de-synchronization attack is a kind of a man-in-the-middle (MITM) applied to change message C in EMAP. The attack firstly performs eavesdrop on the protocol message exchange to obtain A||B||C. It then changes A||B||C to become A||B||C' , where C'0= $C \oplus I_0$ and $I_0 = (000 \ldots 001)^3$. Similarly, the attacker changes the reply D and E from the tag to D' and E', respectively.

Attack on EMAP mutual authentication:

Reader $\longrightarrow$ MITM: $A||B||C$
MITM $\longrightarrow$ Tag: $A||B||C'$
Tag $\longrightarrow$ MITM: $D||E$
MITM $\longrightarrow$ Reader: $D'||E'$

where:

$n2' = n2 \oplus I_0$
$C' = C \oplus I_0 \qquad D = (IDS^{(n)}_{tag(i)} \wedge K4^{(n)}_{tag(i)}) \oplus n2'$
$D' = D \oplus I_0$
$E = (IDS^{(n)}_{tag(i)} \wedge n1 \vee n2') \oplus ID_{tag(i)} \bigoplus_{I=1}^{4} KI^{(n)}_{tag(i)}$
$E' = E \oplus I_0$

Figure 11. Attack on EMAP

By applying it on EMAP, the attack has an average 75% success rate for E' being accepted, no matter what the values of $IDS^{(n)}_{tag(i)}$, n1 and n2 are. However, since $IDS^{(n)}_{tag(i)}$ is known, if $[IDS^{(n)}_{tag(i)}]_0 = 0$, the attack succeeds with 100% rate and if if $[IDS^{(n)}_{tag(i)}]_0 = 1$, the success rate is only 50%. The following table depicts the final results.

Table 1: Results of bit de-synchronization attack

$[IDS]_0$	$[n1]_0$	$[n2]_0$	$[n2']_0$	$[result_1]_0$	$[result_2]_0$
0	0	0	1	0	0
0	0	1	0	1	1
0	1	0	1	0	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	0	1	1
1	1	0	1	1	0
1	1	1	0	1	0

As can be seen above, the tag might still accept compute the reply message based on the modified values in the received message. If this message is accepted by the reader, then the mutual authentication exist which mean both the reader and the tag will update their secrets to the attacker.

Likewise, they also proof how vulnerable these protocols from full Disclosure attacks. The attack is done by repeatedly running the incomplete protocol many times at the tag side. This action will make the tag expecting that a completion message from the reader to update its secret. If the attacker can discharge the tag in a brute force way immediately after it sends out the reply message, all the secret information in the tag can be extracted [29]. As a result, ultra lightweight protocols also do not provide full protection for forward security and location tracking.

After presenting advantages and disadvantages of all low cost RFID authentication protocols above, the author conclude the analysis in the following table [35].

Table 2: Summary of the analysis

Protocols	Tracking Protection	Data Privacy	Forward Security
A	O	Δ	◊
B	Δ	O	*
C	O	O	◊
D	O	Δ	O
E	O	Δ	Δ
F	Δ	O	◊
G	O	O	◊
H	O	O	Δ
I	Δ	O	Δ

Notation :

O : Satisfied
Δ : Partially Satisfied
* :Not Satisfied
◊ : Not Available

VI. CONCLUSIONS

This work is a preliminary study attempts to provide adequate survey on low cost RFID authentication protocols that would be useful for government decision makers particularly in developing country (in this case Indonesia) with respect to planning of adopting secure and low cost RFID based vehicle license plate.

Nine types of RFID authentication protocols satisfy low cost requirement as mentioned in literature. Then each of them assessed according to tracking prevention, data protection, and forward security as main security and privacy issues for RFID.

From tracking prevention perspective, it is concluded that some of protocols (A,C,D, E, G, H) offer solution for tag anonymity using different kind of cryptographic approaches such as hash, hash-chain, or random number generator, and *ultra-lightweight,* while the rest (B, F, I) apply simple techniques based on some characteristics of RFID interfaces such as RFID tag's command or tag singularization that only partially satisfy tracking prevention requirements. In terms of data protection, only three protocols (A, D, E) could not fully satisfy this aspect, while the rest (B, C, F, G, H, I) provide better data privacy protection. From the view point of the last feature of forward security, only single protocol (D) seems to satisfy this aspect, three other protocols (E, H, I) could not fully satisfy it while the rest protocols (A, B, C, F, G) are fail.

In short, it is clearly seen that each low cost protocol has different security characteristics and no single protocol offers full security features. In the future, findings derived from this study will serve as the basis for government policy maker to select the right low cost RFID authentication protocols for RFID license plate under multi criteria decision analysis (MCDA) environment.

REFERENCES

[1] A. Juels, "Minimalist Cryptography for RFID Tags," in Blundo, C., Cimato, S. (eds.) SCN 2004. LNCS, vol. 3352, Springer, Heidelberg, 2005.

[2] F.Karray, M.Alemzadeh, J. Abou Saleh and M.N.Arab, "Human-Computer Interaction: Overview on State of the Art", International Journal On Smart Sensing And Intelligent Systems,2008, Vol. 1, No. 1, pp.137-159.

[3] D. Henrici, and P. Muller, "Hash-based Enhancement of Location Privacy for Radio-Frequency Identification Devices using Varying Identifiers, "

in *Proceedings of Workshop on Pervasive Computing and Communications Security,* 2004.

[4] D. Molnar and D. Wagner, "Privacy and Security in Library RFID Issues, Practices, and Architectures," in *ACM Conference on Computer and Communication Security*, 2004.

[5] G. Avoine, P. Oechslin, "RFID Traceability: A Multilayer Problem," Financial Cryptography, 2005.

[6] K. Rhee, J. Kwak, S. Kim, D. Won, "Challenge-response based RFID authentication protocol for distributed database environment" *International Conference on Security in Pervasive Computing* SPC 2005, pp. 70-84, 2005.

[7] Lamport, "Password Authentication with Insecure Communication", Communications of the ACM vol. 24, no.11, pp 770-772, 1981.

[8] M. Ohkubo, K. Suzuki, and S. Kinoshita, "Cryptographic approach to privacy-friendly tags", *RFID Privacy Workshop*, 2003.

[9] M.Langheinrich and R.Marti, "Practical Minimalist Cryptography for RFID Privacy," *IEEE Systems Journal*, vol. 1, no. 2, Dec 2007.

[10] P.P.Lopez, J.C.H. Castro, J.M.E. Tapiador, and A.Ribagorda, "RFID Systems: A Survey on Security Threats and Proposed Solutions," IFIP 2006, PWC 2006, LNCS 4217, pp. 159–170, 2006.

[11] R. Want, *Enabling Ubiquitous sensing with RFID*, Computer 37 (4), 2004, pp. 84-86.

[12] S. Han, T.S. Dhillon, and E. Chang, "Anonymous Mutual Authentication Protocol for RFID Tag Without Back-End Database," MSN 2007, LNCS 4864, pp. 623-632.

[13] S. Han, V. Potdar, and E. Chang, "Mutual Authentication Protocol for RFID Tags Based on Synchronized Secret Information with Monitor", ICCSA 2007, LNCS 4707, pp. 227 – 238, 2007.

[14] S. Lee, H. Lee, T. Asano, and K. Kim, "Enhanced RFID Mutual Authentication Scheme based on Synchronized Secret Information", *AUTO-ID Labs White Paper, WPHARDWARE* 032, 2006.

[15] S.A. Weis, S.E. Sarma, R.L. Rivest, D.W. Engels, "Security & Privacy Aspects of Low-Cost Radio Frequency Identification Systems, "*Security in Pervasive Computing*, LNCS no. 2802, pp. 201-212, 2004.

[16] S.E.Sarma, S.A.Weis, and D.W.Engels, "RFID systems, security and privacy implications," in *Technical Report MIT-AUTOID-WH-014*, AutoID center, MIT, Cambridge, 2002.

[17] S.L. Garfinkel, A.Juels and R. Pappu, "RFID Privacy: An Overview of Problems and Proposed Solutions," *IEEE Security and Privacy* May 2005, pp. 34-43.

[18] S.M.Lee, Y.J.Hwang, D.H.Lee, and J.I.Lim, "Efficient Authentication for Low-Cost RFID Systems, " in *International Conference on Computational Science and Its Applications*, pp. 619–627, May 2005

[19] T. Dimitriou, "A Lightweight RFID Protocol to Protect against Traceability and Cloning Attacks," in International Conference on Security and Privacy for Emerging Areas in Communication Networks, September 2005.H. Poor, An Introduction to Signal Detection and Estimation. New York: Springer-Verlag, 1985, ch. 4.

[20] J. Curtin, R. Kauffman, and F. Riggins, "Making the 'MOST' out of RFID technology: A research agenda for the study of the adoption, usage and impact of RFID," *Information Technology and Management,* vol. 8, no. 2, 87–110. 2007

[21] R. Das, "RFID Tag Sales in 2005—How Many and Where," DTechEx Ltd., 2005.

[22] C. Heinrich, *RFID and Beyond,* Wiley, Indianapolis, 2005.
[23] H. Knospe and H. Pohl, "RFID Security," *Information Security Technical Report*, vol. 9, issue 4, pp 39-50, Dec 2004.
[24] P. Peris-Lopez, J.C.Hernandez-Castro, E.T.Juan, and R. Arturo, "LMAP: A Real Lightweight Mutual Authentication Protocol for Low-cost RFID tags*" Workshop on RFID Security -- RFIDSec 06*, July 2006
[25] CC.Tan,, B.Sheng, and Q. Li, "Serverless Search and Authentication protocols for RFID". In: Proceedings of Pervasive Computing Conference (2006)).
[26] P. Peris-Lopez, J.C.Hernandez-Castro, E.T.Juan, and R. Arturo,"M2AP: A Minimalist Mutual-Authentication Protocol for Low-cost RFID Tags", *Lecture Notes inComputer Science, 912--923, Springer-Verlag,* Sep-2006.
[27] P. Peris-Lopez, J.C.Hernandez-Castro, E.T.Juan, and R. Arturo, "EMAP: An Efficient Mutual Authentication Protocol for Low-cost RFID Tags", *OTM Federated Conferences and Workshop: IS Workshop -- IS'06, 2006, 4277 Lecture Notes in Computer Science*, P-352--361, November Springer-Verlag.
[28] S.Y.Kang and I.M.Lee, "A Study on Low-Cost RFID System Management with Mutual Authentication Scheme", *Ubiquitous, 2008 International Conference on Multimedia and Ubiquitous Engineering*
[29] T.Li, G.Wang and R.H.Deng, "Security Analysis on a Family of Ultra-lightweight RFID Authentication Protocols", *Journal of Software*, vol. 3, no. 3, March 2008.
[30] X.Tao, H.Yang, R.Chen, and J.Du, "An Improvement on Randomly Changed Identification Protocol for Low-Cost Tags", *Advanced Materials Research* 1583, 2012, pp. 562-564
[31] J.Segura, J.G.Jordán, M.A.Jaen, F.R.Soriano, and A.Soriano, "Low Cost Identification Applications in Traffic Vehicular Environments", in *Sustainable Radio Frequency Identification Solutions*, 2010.
[32] M.G.Gnoni, V.Elia, and A.Rollo, "RFID technology for an intelligent public transport network management", *International Journal of RF Technologies: Research and Applications*, 2010,Vol. 3, No. 1 , pp.1-13
[33] G.H Hwang, K.H.Cha, S.Bhardwaj and D.S.Lee, "UHF RFID Metal Tag Applying to License Plate Using Metal Shielding and Watertight Methods", International Journal on Smart Sensing And Intelligent Systems, Vol. 2, No. 4, pp. 549 – 563
[34] S. Merilampi, T. Björninen, L. Sydänheimo, and L. Ukkonen, "Passive UHF RFID Strain Sensor Tag For Detecting Limb Movement", *International Journal On Smart Sensing And Intelligent Systems* Vol. 5, No. 2, pp. 315 – 328
[35] I.Syamsuddin, S.Han, T.Dillon, "A survey on low-cost RFID authentication protocols", *ICACSIS 2012 International Conference on Advanced Computer Science and Information Systems*, 2012, pp. 77 – 82
[36] E.G.Ahmed, E.Shaaban, M.Hashem, "Lightweight Mutual Authentication Protocol for Low Cost RFID Tags", *International Journal of Network Security & Its Applications (IJNSA)*, 2010, vol. 2, no. 2 , pp.27-37