

A study on secure protocol using the Public Key Infrastructure approach in an e-passport

Yong-Sik Choi*, Young-Jun Jeon*, Sang-Hyun Park*

* Dept. of Computer Science & Engineering, University of Incheon,
12-1 SongDo-Dong, Yeons-Gu, Incheon, South Korea

mars@incheon.ac.kr, 0961144@incheon.ac.kr, tank1862@nate.com

Abstract— An e-passport is a passport that includes biometrics information and ID by an RFID chip inserted internally. An e-passport not only prevents forging of ID but also makes rapid progress at immigration. The number of forged passports is increasing worldwide; therefore, to strengthen national security against international terrorism or crime, nations all over the world are now driving to bring in electronic passports. The e-passport can prevent passport forgery and increase stability by intensifying the personal verification procedure. The fundamental weakness of a wireless channel, which is the instability of the link, limitation of physical protection of each node, there involves a high risk in the reality of the connection between nodes. In addition, there is no guarantee of security because of the fundamental weakness of the sensor node itself in hardware restriction. This paper designates the deduced security weakness and demands that could occur in an electronic passport, and suggests a direction for security service based on safe key distribution and an authorization technique. The proposed public key method to hash lock on reverse functional difficulty of a one-direction hash function to detect and verify a damaged electronic passport increases stability and creates resistance on capture. And to block illegal information on an authentication server, the kill Tag method is executed. The proposed method provides the high efficiency of a multi-leader management method through a mutual authentication mechanism and a multi-leader management method between the passport and the Reader. Therefore, the method can increase security by protecting from reprinting, wiretapping and meson efficiently.

Keywords— e-passport, RFID, Hash Lock

I. INTRODUCTION

Due to the terrorist attack on September 11, 2001, and as some countries in Europe, e-passport immigration management has become an essential characteristic of national security. Therefore, the biometrics technique has stood out in bold relief as the most accurate measure for verifying identity. What biometrics does is compare and judge from each person's differences in physical, behavior

feature extraction. For those examples, there are facial appearance, iris, retina, fingerprint and DNA.

An electronic passport (e-passport) is a passport that saves biometrics information and ID by an RFID chip inserted internally. It is not only prevents forging ID but also makes rapid progress at immigration. The number of forged passports is increasing worldwide; therefore, to strengthen national security against international terrorism or crime, nations all over the world are now driving to bring in electronic passports. The e-passport can prevent from forging passport and increase stability by intensifying the personal verification procedure. [1].

However, in addition to the threat to privacy, diverse security problems are occurring when e-passports are brought in to be used. The major problem is the leaking of private information. In some circumstances when Readers had been obtained by others, private information can easily be leaked and is untouchable, which will make it almost impossible to find whether it has been leaked or not. And the information that leaked will become a huge social problem.

The composition of this paper is as follows: in the second section, e-passport security, e-passport copy protection, biometrics, and RFID Authentication Protocol will be discussed as related research. In the third section, the designs of e-passport secure protocol and antenna module will be discussed. The conclusion is in the final section.

II. RELATED WORK

The components of the e-passport can be divided into two techniques that are hardware or software. The hardware technique is the print technique that forms part of a paper passport and includes a contactless IC chip, which is the untouchable IC chip technique that is adhered to the front cover. The software technique includes the information security-related technique and biometrics related technique. [2].

The technique related to protecting information is mostly formed by authentication and access control techniques that are for the protection of the information and security between the IC chip and the unit. There is a basic access control (BAC) technique and an extended access control (EAC) technique in

the access control technique, for the authentication technique can be divided into the active authentication technique (AA) and the passive authentication (PA). Last, as for technique related to biometrics authentication, there is a personal authentication technique using save or trade information of biometrics and saved biometrics information; therefore, it is advised to apply the international ISO/IEC JTC1 SC37 in ICAO standard. [3].

A. e-passport Security

An e-passport collects the same information to scan as an existing passport in the machine, and by using the BAC method to include personal information related to the passport without biometrics information, security can be retained.

For information access to and control of the inside of the untouchable IC chip, an electronic passport uses various encryption and decryption algorithms and digital signatures. Often, the techniques used include the coding public key method, hash or digital signature in ISO/IEC JTC1 SC27 to form a secure channel between the electric IC chip of the electronic passport and the reading unit. [1], [2].

The BAC method allows to access to the inside of the chip only for the person who knows the MRZ information in 88 positions that is physically indicated inside the electronic passport. This method disables reading of the information when the passport have not been received physically. In addition, when the person had been verified, this method disables wiretapping by creating a coded channel using the DES algorithm between the passport and the Reader.

The EAC method controls additional access to biometrics information such as personal fingerprint or iris scan that is inserted in the electronic passport; therefore, each nation has to designate the process. However, the BAC and EAC are all optional; thus, it is dependent on the user nation to decide and use.

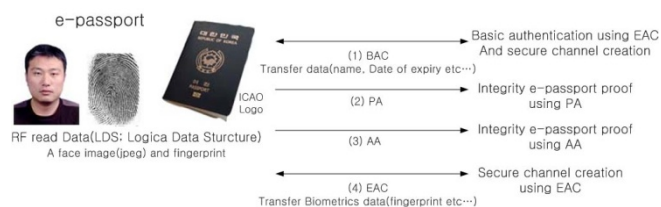


Figure 1. e-passport verification architecture

Figure 1 shows the e-passport verification architecture. The basic authentication uses EAC and secure channel creation. Then the e-passport integrity proof using PA and AA. A secure channel is created using EAC.

B. e-passport copy protection

There is passive authentication (PA) and active authentication (AA) in preventing forging of electronic passports ordained by ICAO; there is a chip authentication function in the EAC function to confirm a forgery.

The PA function saves any hash and digital signature that includes a document security object on the personal information inserted in electronic passport within the

passport by the authenticity verification on the saved data in electronic passport; it downloads the authentication registered in the ICAO PKD and distinguishes itself when it is read.

The AA function uses the method by guaranteeing the chip has not been altered in an electronic passport. The produced pair-key using either the RSA or ECDSA algorithm for active authentication saved in the electronic passport guarantees the chip has not been copied by confirming the personal information that has been saved in the security domain of the chip in the Reader.

In the CA function, the method for proving the chip has not been copied is quite similar to the AA function; however, this method differs from utilizing the security channel that is used in EAC.

C. Biometrics

Facial, fingerprint and iris scans in the biometrics information are saved in an electronic passport. According to the ICAO regulation, the facial image is essentially designated to be in the biometrics information when electronic passport is being used, and either a fingerprint or iris image is advised to be saved as optional information. The biometric data interchange format for the biometrics image and biometrics authenticity is produced by the biometrics information and authenticity algorithm, which also known as the image and original signal. It is said to be the standard format to save biometrics authenticity information that is in use. The biometrics information data trade format that is required for an electronic passport is designated to be the IS international standard.

D. RFID authentication protocol

The key control protocol plays a role in constructing a safe communication networks and create a secret key, which are necessary for various security protocols by establishing the reliance relationship between sensor nodes, which are installed at its discretion under the condition without a reliable sensor or infra. As key control mechanisms, there are pairwise key, random key pre-distribution, public key infrastructure and hierarchical key management. As a shared key in network, the pairwise key is used in encoding and authentication and provides effectiveness and simplification. However, the damage caused by node capture may affect the entire network, and an additional key renewal protocol is required. Before installation, random key pre-distributions receive a random number of keys from the previously created key pool. The protocol uses the key if the neighbor key and common key exist but establishes a link key through the connected neighbor node if they do not exist. In this method, depending on the density of the sensor network, the entire network may not be entirely connected. [4], [5], [6].

Furthermore, because it is a pre-distribution method, it is impossible to provide the newness of key. The public key infrastructure provides a hardware-based public key through the selection of the proper algorithm and parameter and optimal embodiment. Although it suggests the application of public key technology in order to distribute low-frequency key, the public key-based structure should be established in advance.

Hierarchical key management includes a hop-by-hop message encoding/decoding process by the key, which is distributed between nodes in advance according to the characteristic of the hierarchical communication structured, suggesting the processing process of sensor addition/deletion. An intermediate node saves the key in proportion to the number of child nodes; however, the node requires the capacity to create a key. The node cannot provide the resilience for sensor capture.

The hash lock method, based on the difficulty of calculating the reverse function of a one-way hash function, can prevent Tag reading by an unauthorized Reader. Although spoofing cannot be prevented, detection is possible. Although this method can be realized with low cost since the method requires only the hash function, there lies a possibility of the corresponding Tag's location tracking by the attacker using the MetaID, since the MetaID is fixed. To lock the Tag, the Reader sends a hash of a random key, as the MetaID, to the Tag, i.e., $\text{MetaID} \leftarrow \text{hash}(\text{key})$. The Reader then stores the MetaID and key in the back-end database. While locked, the Tag responds only with the MetaID when queried. As shown in Figure. 5, to unlock the Tag, the Reader queries the Tag for the MetaID. The Reader then uses the MetaID to look up a key and ID for the Tag in the database. If the MetaID is found, then the Reader sends the key to the Tag in an attempt to unlock the Tag. The Tag hashes the key and compares the results against the MetaID stored in the Tag. If this compares successfully, the Tag will unlock itself and allow access by the Reader. [7].

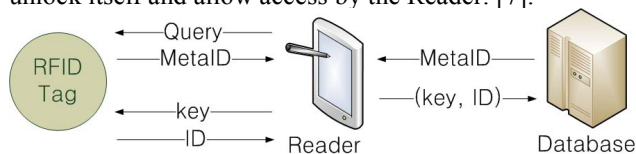


Figure 2. Unlocking Hash Lock Protocol

Randomizing the Tag response during the query process prevents tracking of individuals based on MetaIDs. The randomized hash lock approach requires the Tags to compute a one-way hash function and include an onboard, random number generator. As shown in Figure. 6, a Tag responds to a query with a random number r , and a hash of the ID concatenated with random number r . The Reader queries the database for all IDs and hashes each ID concatenated with the returned random number r from the Tag. If a match is found, the Reader sends the ID to the Tag for authentication.

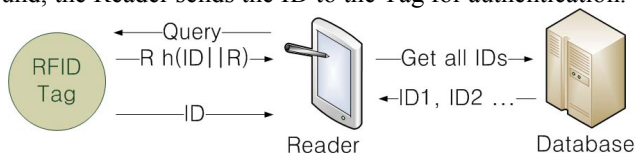


Figure 3. Unlocking Randomized Hash Lock Protocol

III. PROPOSED E-PASSPORT AUTHENTICATION PROTOCOL

Utilizing the public key method of hash lock for key management, which could be used to code either authentication of an electronic passport or sensed

information, provides the key managing method and the security protocol to protect information in the passport.

A. E-passport authentication protocol

Using the meta ID as a secret key utilizes the public key method on hash lock that is based on the reverse functional calculation difficulty of one-direction hash function. Hash lock can prevent other unauthorized machinery accessing the sensor node and possibly embody less cost by requesting only the hash function. The sensor node verifies the electronic passport with a previously registered public key (produced by using MetaID) and produces only the key (k) of each sensor node, and has $\text{MetaID} = H(k)$ that corresponds to. At this point, $H(\)$ is the function.

The electronic passport should obtain an authorized key by executing transmission with the key of the corresponding electronic passport to the authentication server. The executing procedure is as follows.

[Step 1]

The authentication server produces a public key and a secret key for the electronic passport and registers it. The server requests the meta ID.

$$P(Kdb\{H(\text{MetaID})\}||Kmd1\})$$

Figure 4. Secure Protocol

However, Kdb is the public key for the authentication server, and $Kmd1$ is the public key for the sensor node. At this point, $P(k\{\})$ is the public key method, and it is coded with the public key k . $H()$ is the hash function. The public key method is used to provide the code and service on an unspecific sensor node. Even though the exposed MetaID of the unauthorized passport has been obtained, authentication authority cannot be earned on the sensor node if the corresponding value of $H(\text{MetaID})$ is not registered in the database. For this reason, the authority of $H(\text{MetaID})$ should be registered in the database and the corresponding passport in advance.

[Step 2]

e-passport that receipt of message is response e-passport-response message.

[Step 3]

The Reader or the e-passport generates the authentication key by $P(\text{MetaID})$ and sends the value.

$$P(Kmd1\{H(\text{DBid})\}||Ksv\})$$

Ksv is the server secret key, and DBid is the nonce ID of DB.

[Step 4]

The electronic passport executes $H(K\{\})$ by the hash function with the server key received from the database and sees the quality of the code on the value of the hash function and server with the printed ID of the database. And the sensor node sends the message 'sensor-node-response.'

$H(K_{sv}\{H(DBid)||query||authcode||Kmd2\})$

authcode is the authentication code, and Kmd2 is the e-passport secret key.

[Step 5]

The authentication server verifies the authenticode of the electronic passport. The passport compares the value from the database of the authentication server, distinguishes if the passport is valid, and sends a data message. In other words, the corresponding passport has access authority and indicates it made the transference legally.

$H(Kmd2\{H(SVid)||cmd1..cmd2..cmdn\})$

SVid is the nonce ID of the server, and cmd is the command set.

The command circuit is made through a fixed server when willing to deliver any command to the corresponding electronic passport in the authenticating process is as follows. First, it can complement efficiency of the electronic passport, which has limited calculation ability and is able to reject the command that has not been authorized. In other words, it can reduce equipment requirements and provide security at an adequate level for electronic passport security.

B. Antenna Module

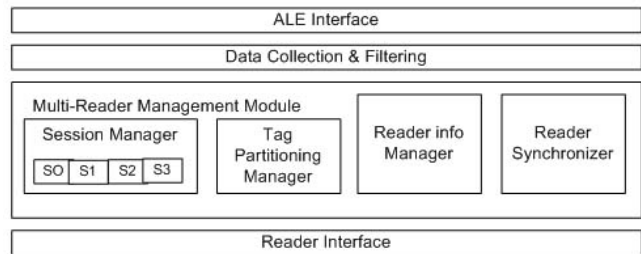
The Proposed Multiple Reader Management Module is placed next to the step of the Reader Management Interface in the Middleware Reader Management that uses the Gen2 protocol. In the previous process to data collection, exactly how data is collected through which Reader antenna by communicating with which Tag can be known.

Figure 5 shows the overall design of the proposed Multiple Reader Management Module. In the Multiple Reader Management Module of the RFID middleware, the Reader synchronizer monitors the condition of the Reader as it maintains synchronization between the Reader and the antenna. Moreover, the connection status of the Reader and antenna is monitored, and antenna connection information is collected and sent to the Reader information manager. The Reader information manager administers the antenna connection and Reader information. The session manager is able to know the number of connected antennas through the Reader information manager, and the antenna session is given based on the number of antennas. According to the Gen2 protocol, each antenna is able to approach as a Source Object, and a Session can be given to each antenna through this. The divided Tag data entered in each Session are sent to the Data Collection & Filter Module together with the antenna information and Tag data.

The movement diagram of the proposed module is same as the picture. The administrator who takes care of the Reader's information should transfer and receive all of the Reader's information with each administrator. The Reader binder should receive the event for antenna addition or Reader addition and synchronize the Reader and middleware. At the completion of synchronization, Reader should request a grant of session's value from the session administrator to each of the Source Object. In addition, Middleware should

request to wait for the session to be granted to the Reader interface. The session administrator should report the granted session value to the Reader interface. The Tag data should be obtained from the Reader interface through the set session, and the Tag dividing administrator should combine the data divided by the Source Object with other various data. These data should be transferred to Data Collection & Filter Module to finish the movement.

Middleware



Reader

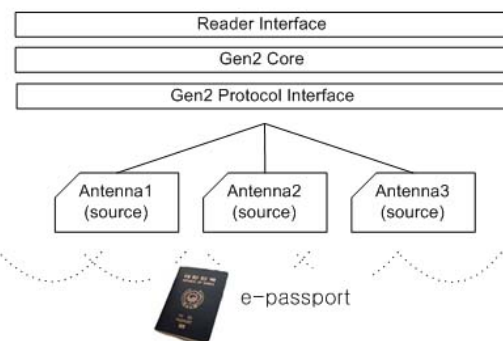


Figure 5. Antenna Reader Architecture

If you look carefully at the algorithm side, creation of a Source Object limited by the information related to Reader and maximum number of the Reader's possible requests is possible. This contains the name of each Source Object, the Instance of Read Point, the Trigger instance, the Read timeout for accurateness for recognizing the Tag, the first Tags defined session value, etc.

The session administrator divides the value of session according to the Source Object's number. Basically, the session value in the form of an Integer is previously set as static, by the arrangement of the session administrator. The session of the Tags in the Gen2 protocol is set to be 4; therefore, if it is in the form of static, faster accomplishment is possible.

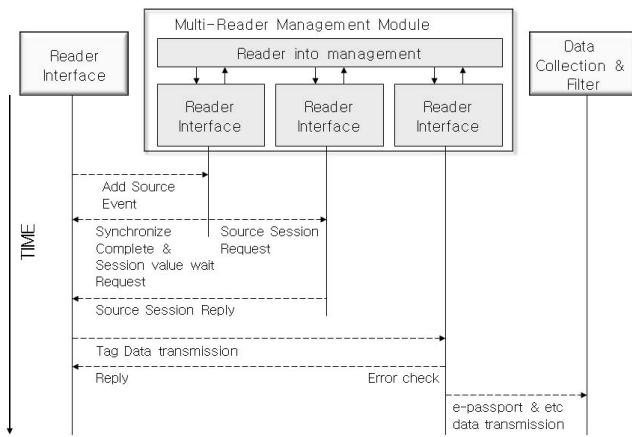


Figure 6. Proposed Module Active Diagram

Table 1. Source Object Generation and Information Gathering

```

if CurrentSourceNum !=
    Source.getMaxNumberSupported()
{
    sr1 = Source.create("mysource1")
    ... // Information gathering of Reader
    session1 = Source.getSession()
}

```

Table 2. Structure Definition of the Session Value

```

static struct session_arr {
    integer session_value // session value
    boolean flag          // session uses friend-or-foe
}

```

It is a structure that sets the sessions value in the Table 2, but in the case of a flag, it acts as a variable to figure whether the session is in use or not. The number of variables of the flag has a false value in the process of initializing. With the set structure as the base, it grants a session to each Source Object. The algorithm of the granting session value uses the selected lined algorithm to compare each Source Object. If there is a difference in the session values after comparing, the algorithm grants the needed session value.

Table 3. Session Value Naming Algorithm

```

for i=0 to i < CurrentSourceNum-1
{
    for j=i+1 to j < CurrentSourceNum
    {
        if Source[i].getSession()==Source[j].getSession()
        {
            for k=0 to k=3

```

```

{
    if session[k].flag == false
    {
        Source[i].setSession
            (session_arr[k].session_value)

        break
    }
}
}
j = j + 1
}
i = i + 1
}

```

Table 3 is the algorithm that grants the session value, and contains the time complexity metric in $O(n^2)$.

The Source Object that obtained the granted session starts transmitting with the Tag. The Reader in the Gen2 protocol starts the transmission by changing the beginning of the new round and session through demands by the Tag query. When each Tag finishes the transaction transmission with the Reader, the data are inputted to the Tag dividing administrator. The inputted data, including the EPC (Electronic Product Code) and other information, are sent to the data structure through higher module Data Collection & Filter.

Basically, Data about EPC, the Source Object Name, which is an information regarding the source, and the Reader Device name are recorded. The ERR Code, which shows the error during the transmission with the Tag, the Query Rep, which shows emergency signals regarding the commands from the Reader, the Tag Logging info, which records the access information after the movement for security, etc. are sent to Data Collection & Filter in one bulk amount of information.

IV. CONCLUSIONS

An e-passport is the passport that saves biometrics information and ID by inserting an RFID chip internally. This is not only to prevent forging of ID but also to make rapid progress at immigration. Forged passports is increasing worldwide; therefore, to protect national security against international terrorism or crime, nations all over the world are now striving to use electronic passports. An e-passport can prevent forging of passports and increase stability by intensifying the personal verification procedure.

The fundamental weakness of the wireless channel, which is the instability of the link, limitation of physical protection of each node, involves high risk on reality of connection between nodes. Also there is no guarantee of security because of the fundamental weakness of the sensor node itself in hardware restriction.

This paper designated deduced the security weakness and demands that could occur in an electronic passport, and

suggested a direction for security service based on safe key distribution and the authorizing technique.

The meta ID is used as a secret key by utilizing the PKI method on hash lock based on the reverse functional calculation difficulty of one-direction hash function. The Reader authenticates the electronic passport with the previously registered key, and produces only the key (k) of each sensor node, and has MetaID = H(k) that corresponds. At this point, H() is the function. Using the personal secret key, the passport sends produced the MetaID to the Reader, and the Reader produces the corresponding key (k) to send it to the Tag. At this point, the electronic passport should compare the key that was sent from the Reader as the hash value and the personal MetaID, and send the personal ID if those values correspond to each other. In addition, to prevent wiretapping, super encryption of the electronic passport ID should be periodically executed.

Proposing a public key method for the hash lock on reverse functional difficulty of one direction hash function to detect and verify a damaged electronic passport increases stability and creates resistance on capture. And to block illegal information in the authentication server, the kill Tag method should be executed. Therefore, it can possibly increase security by protecting passports from reprinting, wiretapping and meson efficiently.

ACKNOWLEDGMENT

This work was supported by Brain Korea 21 project in 2009.

REFERENCES

- [1] B. Schouten, B. Jacobs, "Biometrics and Their Use in e-Passports", *Image and Vision Computing*, pp 205-312, 2009.
- [2] G.M. Ezovski, S.E. Watkins, "The Electronic Passport and the Future of Government-Issued RFID-Based Identification", *RFID*, 2007. *IEEE International Conference*, pp 15-22, 2007.
- [3] M. Meingast, J. King, and D.K. Mulligan, "Embedded RFID and Everyday Things: A Case Study of the Security and Privacy Risks of the U.S. e-Passport", pp 7-14, *RFID*, 2007. *IEEE International Conference*, 2007.
- [4] I.F.Akyiliz, W. Su, Y.Sankarasubramaniam, and E. Cayirci, "A Survey on Sensor Network", *IEEE Communication Magazine*, pp 102-114, 2002.
- [5] A. Perrig, R. Szewczyk, V. Wen, D. Culler and J. D. Tygar, "SPINS: Security Protocols for Sensor Network", *Wireless Network Journal(WINE)*, 2002.
- [6] W. Du, J. Deng, Y. S. Han, and P. Varshney, "A Pairwise Key Pre-distribution Scheme for Wireless Sensor Network", *10th ACM Conference on Computer and Communications Security (CCS)*, October 2003.
- [7] J. Staddon, S. Miner, and M. Franklin, "Self-Healing Key Distribution with Revocation", *Proceedings of 2002 IEEE Symposium on Security and Privacy (S&P2002)*, 2002.