International Journal of Security and Its Applications
Vol.8, No.1 (2014), pp.33-44
http://dx.doi.org/10.14257/ijsia.2014.8.1.04

Efficient Data Memory Usages of 3GPP Authentication and Key Agreement Protocol

Minha Park[1], Yeog Kim[2] and Okyeon Yi[3]

[1 3] Dept. of Mathematics, Kookmin University, Korea, [2] Cryptography & Information Security Institute, Kookmin University, Korea
mhpark@kookmin.ac.kr, yeogkim@gmail.com, oyyi@kookmin.ac.kr

Abstract

There are various services using mobile devices due to development of communication technology and mobile equipment, regardless of time and place. To secure usage of convenience and smart services, authentication between users' devices and network is necessary. To achieve this, many researches have been studied about 3rd Generation Partnership Project Authentication and Key Agreement (3GPP-AKA). Therefore, during authentication between MS and network in radio environments, it is very important to reduce the amount of processing and stored data in MS as much as possible in order that overload of authentication does not occur. So, in this paper, we propose an advanced authentication protocol to solve the problems of 3GPP-AKA discussed other papers and to minimalize data memory usage, keeping the security. As a result, the proposed protocol decreases data memory usage by maximum 37%.

Keywords: *3GPP, authentication, AKA, efficiency*

1. Introduction

Today, we can use the convenient and smart services using mobile devices, such as smartphones and tablet PCs, regardless of time and place due to development of communication technology and mobile equipment. Mobile devices, with performance of 1.3GHz CPU and 1GB RAM, are commonly used as MS instead of PCs with performance of 3GHz quad-core CPU and 4GB RAM. These MSs are not so much low-performance devices for providing diversity services. However, if it is possible to minimize the amount of process performance and storage data in MS, the services will be more comfortably. These services are usually provided in wireless environments, which are prone to security threats, such as forgery. So, the cryptographic techniques need to deal with these threats between MS and network. Especially, the mutual authentication between them is positively necessary. For example, there is a mutual authentication in 3G Network, AKA [1]. 3G Network consists of MS, Serving Network (SN) that provides a direct communication service with MS and shares of Home Network (HN)'s role for the efficiency of network management, and HN which manages and authenticates MS.

Like this, 3GPP-AKA operates in MS, SN and HN. In related researches, the weaknesses of 3GPP-AKA are brought up [4]-[6]. 1) Increasing of bandwidth consumption between SN and HN and storage overhead of SN [4] because of using a lot of Authentication Vectors (AV) for many authentication, 2) synchronization of Sequence Number (SQN) which used for freshness of authentication and distinguished AVs [4], 3) possibility of attack due to weakness of SN's reliability [5], 4) invasion of MS's privacy [6], *etc*.

ISSN: 1738-9976 IJSIA

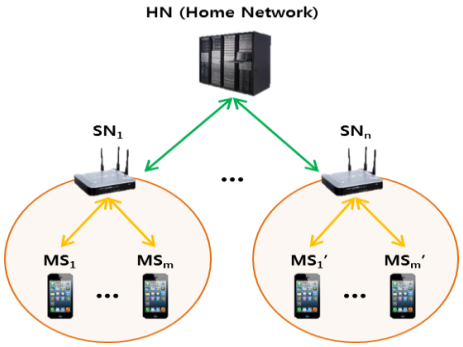

Figure 1. 3G Network Environment

3GPP-AKA and the earlier studies designed mutual authentication protocols focusing on security, but didn't consider overload about authentication. So, it is difficult to expect efficiency. On the contrary, in this paper, we design the advanced protocol that solves all problems of 3GPP-AKA, maintaining security, and minimizes data memory usage for efficiency. This paper is organized as follows. In Section 2, we arrange protocols that improve weakness of 3GPP-AKA. In Section 3, we describe proposed protocol of authentication in detail. In Section 4, we compare existing protocols and proposed protocol by solution of problems and using memory of data. In last Section, we give the conclusion.

2. Related Research

2.1. Problems of 3GPP-AKA Discussed Earlier Studies

1) Bandwidth consumption and storage overhead of SN

Authentication is performed periodically to maintain the reliability between MS and SN and the security of shared key. In 3GPP-AKA, HN generates a lot of AVs and sends them to SN, then SN can use it every authentication without HN's extra permission. It occurs that bandwidth consumption and storage spaces increase.

2) Synchronization of SQN

AVs have distinct SQNs that provide the freshness of each authentication procedure. And considering SQN's gap of MS and HN for movement of MS, MS checks whether difference of MS's and HN's SQN is within the reasonable range during authentication process. If not, SQN and AVs are all updated by process of re-synchronization.

3) Weakness of reliability of SN

SN conducts authentication between MS and HN. So, it needs a reliability of SN. In 3GPP-AKA, since SN just delivers authentication values, it is difficult to trust SN. As a result, redirection attack can occur.

4) Invasion of MS's privacy

To check MS's ID, IMSI (International Mobile Subscriber Identity) of MS is sent to SN in clear. So, an invasion of MS privacy can occur.

2.1. Related Researches

1) UMTS X-AKA [4]

In [4], HN generates only one AV and sends it to SN. Then bandwidth consumption and storage of SN can be reduced. In addition, it can solve the problem of SQN synchronization to use timestamp instead of SQN, providing freshness. But, if HN sends AV to SN continuously because of often movement of MS, then bandwidth consumption will increase.

2) Kim-AKA [5]

[5] uses only one AV and proposed efficient and fast protocol that is used in Handover which operates between MS and SN without HN. And it improves the reliability of SN by using authentication value of SN.

3) PE-AKA [6]

[6] uses SN's information, LAI (Location Area Identity), as to improve reliability of SN. In addition, it provides the privacy of MS by masking IMSI with secret token.

Table 1. The Notations used in this Paper

Problems	Solutions	Related Studies
Bandwidth consumption and storage overhead of SN	**Using only one AV**	**[4], [5], [6]**
Synchronization of SQN	**Using timestamp instead of SQN**	**[4], [5], [6]**
Weakness of reliability of SN	**Using SN's information or random number**	**[5], [6]**
Invasion of MS's privacy	**Masking IMSI with secret token**	**[6]**

2.3. Consideration for Proposed Protocol

1) For Efficiency of Operation

• *Use one Session Key (SK)*: After authentication, SK, generating by authentication, is used to encrypt data for confidentiality and integrity. While 3GPP-AKA and others generate different two keys for confidentiality and integrity, the proposed protocol generates one key for both, reducing data memory usage. So, we consider the safety of SK, updating it periodically in Re-Authentication.

• *Minimum of calculation in SN*: For enhanced of SN's validation, SN generates new random number and computes MAC in [4], [5] and [6]. So, it occurs calculation overhead. But the protocol minimizes the same overhead by using LAI of SN.

2) For Solution of Problems

• *Use Only One AV*: HN generates only one AV and sends it to SN. This reduces bandwidth consumption and SN storage, and also skips SQN comparison.

• *Use Information of SN*: Using LAI, SN's local information, improves reliability of SN.

• *Use Temporary Identity (TID) of MS*: After initial authentication, SN gives MS TID, using for MS's ID instead of PID (Personal Identity). So, it can provide MS privacy.

• *Proposed Fast Authentication Protocol*: In proposed protocol, additional authentication for updating SK or access with new SN as the mobility of MS is proposed with communication between MS and SN without HN.

3. Proposed Protocol

3.1. Full-Authentication and Key Agreement

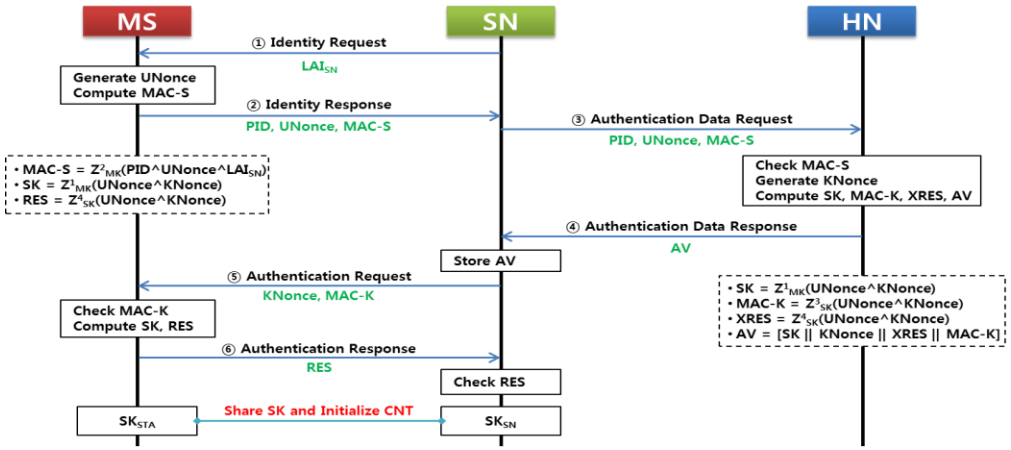

Figure 2. Full Authentication Protocol

When an MS initially accesses an SN or MS requests new authentication as failure of before authentication, Full Authentication is operated according to the process found in Figure 2.

① When MS accesses SN, SN sends its LAI to MS and requests identity of MS.

② MS generates nonce, UNonce, and computes MAC-S, which is Message Authentication Code, with received LAI and PID which is the identity of MS. And then, MS sends PID, UNonce and MAC-S to SN.

$$MAC\text{-}S = Z^{2}_{MK}\,(PID||UNonce||LAI_{SN}) \tag{1}$$

③ SN sends MS's information received from MS to HN. Then, HN identifies MS and SN with PID, LAI_{SN} and MAC-S. If it successes, HN generates nonce, KNonce, and SK and computes XRES and MAC-K which are values for authentication of MS and HN respectively. Using these values, HN generates an AV.

$$SK = Z^{1}_{MK}\,(UNonce\text{^}KNonce) \tag{2}$$

$$MAC\text{-}K = Z^{3}_{SK}\,(UNonce\text{^}KNonce) \tag{3}$$

$$XRES = Z^{4}_{SK}\,(UNonce\text{^}KNonce) \tag{4}$$

$$AV = [SK||KNonce||MAC\text{-}K||XRES] \tag{5}$$

④ HN sends an AV to SN. Then, SN saves it.

⑤ SN sends KNonce and MAC-K, which are in AV, to SN. After MS generates SK, using received KNonce, it computes XMAC-K, which is a value for authentication of HN, using SK. Then, MS validates HN, comparing MAC-K and XMAC-K.

$$XMAC\text{-}K = Z^{3}_{SK}\,(UNonce\text{^}KNonce) \tag{6}$$

If it successes, MS computes RES which is a value for validating MS.

If the comparison of the values of authentication is failed, authentication process terminates by Authentication failure.

⑥ MS sends RES to SN. Then, SN authenticates MS, comparing RES with XRES extracted from AV.

After mutual authentication success, MS and SN save SK and initialize CNT (counter), which is value about usage of SK, to zero. Then, they can communicate securely with encryption data, using SK. And SN generates TID of MS, encrypts it and sends it to MS. So, it can provide privacy of MS that MS use it for identity in after authentication.

3.2. Re-Authentication

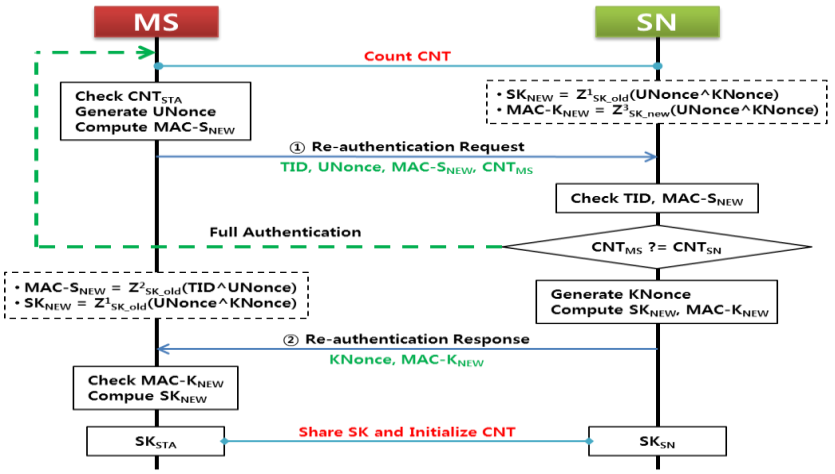

Figure 3. Re-Authentication Protocol

Using same SK continually can cause exposure to attack. So, it needs to update SK periodically. We set maximum value, threshold, of usage count of SK and limit the value for safety of SK. Every time SK is used, MS and SN increase CNT of SK and MS checks whether CNT reaches threshold or not. If it does, MS requests SN for Re-Authentication which progresses between MS and SN only as Figure 3. When SN is requested Re-Authentication, it checks that CNT of MS and of SN are same. If not, Full Authentication is operated instead of Re-Authentication.

① If CNT reaches threshold, MS generates UNonce, computes MAC-S and requests Re-Authentication to SN, sending TID, UNonce, MAC-S and CNT. Then, SN checks TID and MAC-S for confirming MS with old SK, and CNT. If successes, SN generates KNonce and computes new SK and MAC-K.

$$MAC\text{-}S = Z^{2}_{SKold}\ (TID \wedge UNonce) \tag{7}$$

$$SK_{NEW} = Z^{1}_{SKold}\ (UNonce \wedge KNonce) \tag{8}$$

$$MAC\text{-}K = Z^{3}_{SKnew}\ (UNonce \wedge UNonce) \tag{9}$$

② SN sends KNonce and MAC-K to MS. Then, MS checks MAC-K and computes SK.

After Re-Authentication success, MS and SN both save new SK and initialize CNT to zero.

3.3. Authentication for Handover

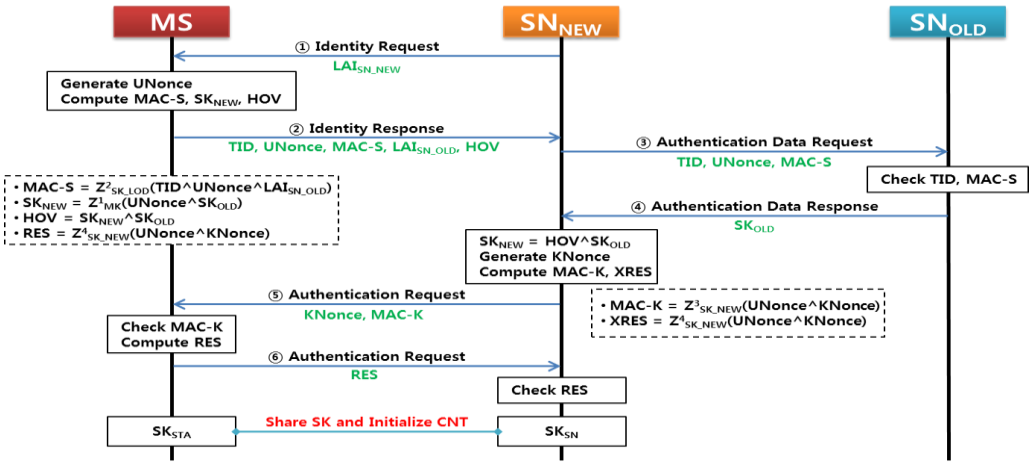

Figure 4. Authentication of Handover Protocol

In radio environment, handover when MS leaves its original SN and then accesses to new SN as MS moves. In that time, it needs that MS confirms validation of new SN and shares the new SK with new SN as Figure 4. In proposed protocol, original SN, which connected MS before, and new SN, which connects MS now, exchanges HOV (Handover Value) that is generated by MS with original SK. As a result, it is not necessary to communicate between SN and HN.

① When MS moves and accesses new SN getting out of the old SN, new SN requests MS for MS's identity, sending LAI of new SN. Then, MS generates UNonce and computes MAC-S, which is a value for validation of MS, new SK and HOV, using old SK.

$$MAC\text{-}S = Z^{2}_{SKold}\,(TID \wedge UNonce \wedge LAI_{SNold}) \tag{10}$$

$$SK_{NEW} = Z^{1}_{MK}\,(UNonce \wedge SK_{OLD}) \tag{11}$$

$$HOV = SK_{NEW} \wedge SK_{OLD} \tag{12}$$

② MS sends TID, UNonce, MAC-S, LAI_{SNold} and HOV to new SN.

③ New SN sends TID, UNonce and MAC-S, received from MS, to old SN. Then, old SN checks TID and MAC-S for confirming MS instead of new SN.

④ If it successes, old SN sends SK_{OLD} to new SN for retrieving new SK. New SN generates KNonce and computes MAC-K and XRES with new SK.

$$SK_{NEW} = HOV \wedge SK_{OLD} \tag{13}$$

$$MAC\text{-}K = Z^{3}_{SKnew}\,(UNonce \wedge KNonce) \tag{14}$$

$$XRES = Z^{4}_{SKnew}\,(UNonce \wedge KNonce) \tag{15}$$

⑤ New SN sends KNonce and MAC-K to MS. Then, MS checks MAC-K for authenticating new SN and computes RES.

$$RES = Z^{4}_{SKnew}\,(UNonce \wedge KNonce) \tag{16}$$

⑥ MS sends RES to new SN. Then new SN checks it for confirming MS.

After authentication success, MS and new SN save new SK and initialize CNT to zero. And new SN sends new TID to MS for privacy and MS saves it, discarding old TID.

4. Analysis of the Proposed Protocol Compared to other Protocols

The proposed protocol is designed for higher efficiency and also solves all problems appeared earlier studies. The efficiency of protocol operation is decided by size of parameters used in calculation of protocol. In this section, we compare the improvements of earlier studies and proposed protocol and explain the efficiency of proposed protocol by analysis of data memory usage from the size of parameters that are used in calculation during authentication. We suppose that the algorithms are same in all protocols.

4.1. Comparison of Improvements

Table 2 lists the improvements offered by several studies through the solving of 3GPP-AKA. Mutual authentication, user traffic confidentiality and signaling data integrity are indispensable function for secure communication. So, 3GPP-AKA and others provide them. And the proposed protocol improves all of these areas, while the earlier studies only improved a few areas.

Table 2. The Lists of Improvements of earlier Studies and Proposed Protocol

List	3GPP-AKA	UMTS X-AKA	Kim-AKA	PE-AKA	Proposed AKA
Mutual authentication	**O**	**O**	**O**	**O**	**O**
User traffic confidentiality	**O**	**O**	**O**	**O**	**O**
Signaling data integrity	**O**	**O**	**O**	**O**	**O**
Reduce bandwidth consumption and storage overhead of SN	**X**	**O**	**O**	**O**	**O**
Skip synchronization of SQN	**X**	**X**	**O**	**O**	**O**
Provide privacy of MS	**O**	**-**	**X**	**O**	**O**
Improve reliability of SN	**X**	**X**	**O**	**O**	**O**
Suggest authentication of handover	**O**	**O**	**O**	**O**	**O**

• *Mutual authentication*: MS, SN and HN authenticate each other with comparison of MAC computed by shared information. In Table 3, 3GPP-AKA operates authentication computing MAC total 4^{th} because it doesn't compute MAC of SN. While others compute total 8^{th} add to computing MAC of SN, the proposed protocol computes total 6^{th}. Consequently, it is more efficient due to less calculation of MAC than others.

• *User traffic confidentiality & signaling data integrity*: During authentication, MS and HN generate new SK with Mater Key (MK) shared secretly. Then they use it for user traffic confidentiality and signaling data integrity by encryption. The proposed protocol generates one SK for reducing data memory usage, while others generate different keys which are Confidentiality Key (CK) and Integrity Key (IK). And considering security of SK's usage, it updates SK periodically by Re-Authentication.

• *Reduce bandwidth consumption and storage overhead of SN*: In initial of 3GPP-AKA, HN and SN exchange a lot of AVs, so it needs many bandwidth consumption and storage of SN.

The proposed protocol decreases them using only one AV, reduced 240bits than 3GPP-AKA's AV. As a result, the proposed protocol is considered more efficiency.

• *Skip synchronization of SQN*: SQN is used for distinguishing many AVs in 3GPP-AKA. So, it needs to check SQNs of MS and SN. If it is not satisfied with condition, authentication is begun newly with re-synchronization. On the contrary, proposed protocol uses one AV so, comparing of SNQ is not necessary.

• *Provide privacy of MS*: SN sends TID to MS after initial authentication, which is used in next authentication.

• *Improve reliability of SN*: In 3GPP-AKA, SN just delivers authentication values, received from HN. Therefore, it is ambiguous to trust SN. On the other hand, the proposed protocol computes MAC with SN's LAI and sends it to HN, then we can trust SN as HN checking it.

• *Suggest authentication of handover*: When MS accesses a new SN, they need confirm for each with authentication. We propose authentication of handover for that time, considering efficiency by communication between original SN and new SN without HN. Others studies also proposed similar protocol, but the proposed protocol is more efficiency with reducing memory size.

Table 3. The Information of Parameters and Calculations in Protocol

List		3GPP-AKA	UMTS X-AKA	Kim-AKA	PE-AKA	Proposed AKA
MAC generation function		f^1, f^{1*}, f^2	f^1, f^2	f^1, f^2	f^1, f^2, H	Z^2, Z^3, Z^4
Key generation function		f^3, f^4, f^5, f^{5*}	f^3, f^4, f^x	f^3, f^4, f^5	f^3, f^4, f^5	Z^1
Size of data		LAI : 16bit, IMSI/TMSI/P_i/w_i : 32bit PID/TID/SQN/AMF : 48bit T_i/t : 148bit MAC : 64bit K/MK/CK/IK/SK/TK/RAND/RES : 128bit				
Parameters	MS	RAND, CK, IK, SQN, AK, AMF, XMAC, RES	RAND, $RAND_S$, MAC_H, MAC_S, AMF, TK, CK, IK, RES	SK, T_i, LAI_{SN}, MAC_{MS}, $RAND_H$, $RAND_{Si}$, $RAND_S$, CK, IK, MAC_S, MAC_H, RES	Ti, LAI_{SN}, SK, P_i, w_i, MAC_{MS}, RAND, $RAND_{SN}$, MAC_H, MAC_{SN}, r_i, RES, CK, IK	UNonce, MAC-S, LAI_{SN}, KNonce, MAC-K, SK, RES
	SN	RAND, CK, IK, SQN, AK, AMF, MAC, XRES	RAND, $RAND_S$, MAC_H, MAC_S, AMF, TK, CK, IK, RES	RAND, $RAND_S$, $RAND_{Si}$, T_i, T_0, SK, CK, IK, MAC_H, MAC_{Si}, XRES, LAI_{SN}	RAND, $RAND_{SN}$, SK, AMF, T_i, MAC_H, MAC_{SN}, XRES, CK, IK	SK, KNonce, UNonce, MAC-K, XRES
	HN	RAND, CK, IK, SQN, AK, AMF, MAC, XRES	t, MAC_U, RAND, TK, AMF, MAC_H	RAND, MAC_{MS}, MAC_H, T_i, SK, LAI_{SN}	Pi, SK, MAC_{MS}, Ti, LAI_{SN}, RAND, r_i, w_i, MAC_H, AMF	UNonce, LAI_{SN}, MAC-S, KNonce, SK, MAC-K, XRES
Data memory usage	MS	688bit	912bit	1252bit	1316bit	656bit
	SN	688bit	912bit	1336bit	1060bit	576bit
	HN	688bit	548bit	548bit	756bit	656bit
Size of one AV		688bit	208bit	484bit	484bit	448bit
Number of message transmission		5	5	5	5	5
Number of MAC calculation		4	8	8	8	6
Number of Key calculation		6	6	6	6	2

4.2. Analysis of Data Memory Usage

In this section, since we have shown the efficiency of the proposed protocol, we will now analyze its data memory usage and data, which are used to calculate MS, SN, and HN authentication. For comparing the proposed protocol and earlier studies, we analyze them in full authentication and authentication of handover process.

First, we compare earlier protocols and the proposed protocol with data memory usage when full authentication is operated. Table 4 gives each entity and section's data memory usage (left side), as well as their ratio of consumption (right side), which shows data memory usage changes compared to proposed protocol. As a result, the proposed protocol decreases data memory usage in MS and SN, but not in HN. However, show the total of the usage, it uses the lowest data memory than others, decreasing maximum 37% beside them. Consequently, the proposed protocol is more efficient than those of earlier studies.

Table 4 The Data Memory Usage and Ratio for Full Authentication

Entities and sections of authentication	3GPP-AKA		UMTS X-AKA		Kim-AKA		PE-AKA		Proposed AKA
MS	688	5% ↓	912	28% ↓	1252	48% ↓	1316	50% ↓	656
MS ↔ SN	464	21% ↑	708	21% ↓	656	15% ↓	964	42% ↓	560
SN	688	16% ↓	912	37% ↓	1336	57% ↓	1060	46% ↓	576
SN ↔ HN	720	4% ↓	580	19% ↑	576	19% ↑	872	21% ↓	688
HN	688	5% ↓	548	20% ↑	548	20% ↑	756	13% ↓	656
Total	3248	3% ↓	3660	14% ↓	4368	28% ↓	4968	37% ↓	3136

In addition, we compare Kim-AKA [5], PE-AKA [6] and the proposed protocol with data memory usage when authentication of handover is operated, because [5] and [6] similarly proposed authentication of handover with the proposed protocol that operates between original SN and new SN. Table 5 represents the data memory usage (left side) and the ratio of consumption (right side) on the same Table 4. In consequence, while the proposed protocol more uses 5% data memory than [5] in original SN, it decreases data memory usage noticeably in the other entities and sections. So, it reduces maximum 51% data memory beside others.

Table 5. The Data Memory Usage and Ratio for Authentication of Handover

Entities and sections of authentication	Kim-AKA		PE-AKA		Proposed AKA
MS	1252	39% ↓	1060	28% ↓	768
MS ↔ SN_{NEW}	888	21% ↓	788	11% ↓	704
SN_{NEW}	2408	76% ↓	1508	62% ↓	576
SN_{NEW} ↔ SN_{OLD}	644	43% ↓	660	44% ↓	368
SN_{OLD}	228	5% ↑	308	22% ↓	240
Total	5420	51% ↓	4324	39% ↓	2656

Therefore, according to above analysis, the proposed protocol not only solves all problems, but also takes account of data memory usage efficiency.

5. Conclusion

Today, the various services in radio environments are more convenience and smarter. For these services, smart devices are the focus of attention instead of PC. But the performance of MS, such as process ability and memory usage, is more limited than PC. These MSs are not so much low-performance devices for providing diversity services. Thus, if it is possible to minimize the amount of process performance and storage data in MS, the services will be more comfortably. In wireless environments, there exist many security threats, such as forgery, wiretapping, and so on. So, the authentication of communication entities must be necessary for security communication service.

In this paper, we proposed the advanced protocol that increased efficiency, minimized data memory usage, and solved all 3GPP-AKA problems discussed earlier studies, maintaining the established security. For efficiency, the proposed protocol uses minimal authentication values and only one AV for decreasing of bandwidth consumption and storage overhead, so synchronization of SQN is not needed. It also uses LAI of SN and TID of MS for reliability of SN and privacy of MS respectively. As a result, the proposed protocol solves all problems that were brought up in earlier studies. In addition, the proposed protocol can be expected to more efficient than other protocols, reducing data memory usage by maximum 37% when full authentication is operated and maximum 51% when authentication of handover is operated. As a result, the proposed protocol increases efficiency, solving many problems. So, it can be used in not only 3G Network, also various environments, especially limited performance.

The communication service can thus provide better service, as mutual authentication provides a lot of functions and efficient data memory usage.

Acknowledgements

This work was supported by the IT R&D program of MKE/KEIT [10041864, Development on spectrum efficient multiband WPAN system for smart home networks].

References

[1] 3rd Generation Partnership Project, “Technical Specification Group Services and System Aspects; 3G Security; Security architecture (Release 5)”, 3GPP TS 33.102 v5.7.0 (2005-12).
[2] 3rd Generation Partnership Project, “Technical Specification Group Services and System Aspects; 3G Security; Security threats and requirements (Release 5)”, 3GPP TS 21.133 v4.1.0 (2001-12).
[3] 3rd Generation Partnership Project, “Technical Specification Group Services and System Aspects; UMTS; Numbering, addressing and identification (Release 5)”, 3GPP TS 23.003 v5.11.0 (2006-06).
[4] C. Huang and J. Li, “Authentication and Key Agreement protocol for UMTS with low bandwidth consumption”, Proceedings of the 19th International Conference on Advanced Information Networking and Application, **(2005)** March, pp. 392-937.
[5] D. Kim and S. Jung, “Improved AKA Protocol for Efficient Management of Authentication Data in 3GPP Network”, Korea Institute of Information Security & Cryptology, vol. 19, no. 2, **(2009)** April.
[6] S. Jeon and S. Oh. “An Efficient Authentication Mechanism Strengthen the Privacy Protection in 3G Network”, Korea Academia Industrial Cooperation Society, vol. 11, no. 12, **(2010)**, pp. 5049-5057.
[7] Y. Kim and M. Park, “Secure AKA (Authentication and Key Agreement) Protocol for Binary CDMA Network”, Korea Institute of Information Security & Cryptology, vol. 20, no. 1, **(2010)** February.
[8] J. Jeon, “A Wireless Network Structure and AKA (Authentication and Key Agreement) Protocol of Advanced Metering Infrastructure on the Smart Grid based on Binary CDMA”, Korea Institute of Information Security & Cryptology, vol. 20, no. 5, **(2010)**, September.
[9] L. Harn and H. Lin, “Modifications to enhance the security of GSM”, Proceedings of the 5th National Conference on Information Security, Taipei, Taiwan, R.O.C, **(1995)** May.
[10] H. Lin and L. Harn, “Authentication protocols for personal communication System”, ACM SIGCOMM Computer Communication Review, vol. 25, no. 4, **(1995)** October, pp. 256-261.
[11] M. Zhang and Y. Fang, “Security Analysis and Enhancements of 3GPP Authentication and Key Agreement Protocol”, IEEE Transactions on Wireless Communication, vol. 4, no. 2, **(2005)** March, pp. 734-742.

[12] W. Juang and J. Wu, "Efficient 3GPP authentication and key agreement with robust user privacy protection", Proceedings of the 2007 IEEE on Wireless communications and Networking Conference, **(2007)** March, pp. 2720-2725.

Authors

Minha Park graduated in Mathematics from Kookmin University in 2013. She is currently studying for a master's degree at the Kookmin University, Seoul, South Korea. Her research interests include the mobile security, TVWS security, network security.

Yeog Kim received her Ph.D. in Information Security from the Korea University in 2010. She is currently a researcher and lecture in C Programming at the Cryptography & Information Institute in the Kookmin University, Seoul, South Korea. Her research interests include the mobile security, certification of cryptography module, forensic accounting,

Okyeon Yi received his Ph.D. in Mathematics from the University of Kentucky in 1996. From July 1999 to1 August 2001, he was at the Electronics and Telecommunications Research Institute, Taejeon, Korea as a team leader for Mobile Information Security. He is currently a Professor at the Kookmin University, Seoul, South Korea. His research interests include the mobile security, smartgrid security, white-box cryptography, Binary CDMA security.