Verification of Authentication Protocol for CDMA Mobile Communication Network

Ki-Yoong Hong, Seok-Woo Kim, and Dong-Kyoo Kim

Abstract

In this paper, we present an analysis of the IS-95 authentication protocol for the Code Division Multiple Access (CDMA) mobile communication network. We propose a mutual authentication protocol, AP-6, to improve the security and correctness. Formal description and verification of the proposed AP-6 are also presented on the basis of the formal logic. It is shown that the proposed AP-6 is more secure and correct than the IS-95 authentication protocol.

I. Introduction

Throughout the rapid advance of computer and communication technologies, the information and communication services tend to move toward the mobile communication and personal communication services (PCS) [1]-[3]-[6]-[8]. Nowadays, security and privacy problems of computer, communication systems and digital mobile communication systems are getting important. Many kinds of mobile communication systems have authentication, signaling encryption and voice privacy mechanisms to support security services, and also the standards are being developed for the mobile communication systems [2][7].

In this paper, we review the recently proposed scheme that is IS-95 authentication protocol for Code Division Multiple Access (CDMA) mobile communication [2]. For CDMA mobile communication network, five kinds of authentication protocols have been proposed such as authentication protocol of mobile station (MS) registration, authentication protocol of MS origination, authentication protocol of MS termination, authentication protocol of unique challenge-response, and authentication protocol of updating shared secret data (SSD) [1]-[3]. In [4][5], Hong and Kim presented an analysis of these authentication protocols and also described a counter example to show that the IS-95 authentication protocol was not correct. They also proposed a mutual authentication protocol, called AP-6 in this paper, to solve the identified problem [4][5]. In this paper, we will present a formal logic to evaluate the proposed authentication protocol AP-6. On the basis of this formal logic, a formal description of the AP-6 will be presented and the correctness of the AP-6 will be also formally verified.

Manuscript received August 10, 1995;accepted November 3, 1995.
K.Y.Hang is with the senior Researcher National Computerization Agency.
S.W.Kim is with Electronics and Telecommunications Research Institute.
D.K.Kim is with Department of Computer Engineering, Ajou University.

II. A Formalism

1. Formal Notations and Predicates

A formal notation is presented to be used for evaluation of the cryptographic protocols such as the authentication and key distribution protocols especially from the view point of the correctness. Our formal logic, as presented in this section, will give a conciseness for the description and analysis of the cryptographic protocols. For the formal description, the following notations are used :

- Ω : Let this symbol denote a termination of the cryptographic protocols.
- E : Let E denote an encryption function of a cryptographic algorithm.
- D : Let D denote a decryption function of a cryptographic algorithm.
- $\wedge$: Let this symbol denote the logical AND.
- $\vee$: Let this symbol denote the logical OR.
- $\sim$: It means the logical negation.
- $\leftarrow$: Let this symbol denote the mathematical assignment. The value of right hand side is assigned to the variable of the left hand side.
- = : Let this symbol denote the equivalent relation.
- ? : This symbol means the verification of both sides. If both sides are equivalent, then it is TRUE. Otherwise,

it is FALSE.

- $\oplus$: Let this symbol denote a bit-wise exclusive-OR.
- $\circ$: Let this symbol denote the concatenation.
- m_A : It denotes the information m for A side.
- m_A^B : It denotes the information m for A side, but calculated or stored on B side. This implies that B calculates or stores the information m_A. Therefore, m_A^A means A calculates or stores its own information m_A.
- Φ : Let this symbol denote a function to return a random number.
- $\delta(T)$: Let this symbol denote a function to return a boolean TRUE or FALSE regarding to input timestamp T. If T is valid, then it returns TRUE.
- $\diamond$: Let this symbol denote the call to the right hand side.
- $\overline{m}$: Let this symbol denote an update or change of information m.
- $A \perp m$: This symbol means that A knows information m or m is known to A. It also implies that A is able to recover m as same as an original one.
- $a \Rightarrow b$: Let this symbol denote the implication so that if left hand side of the symbol, e.g., a, truly realizes then right hand side of the symbol, e.g., b, would realize.
- $<W_1|W_2>$: It denotes a choice of two tasks W_1 *and* W_2.
- $W_0 \Rightarrow <W_1|W_2>$: It denotes that if the task W_0 is truly realized then the task W_1 would be realized. Otherwise, W_2 would be realized.
- $\langle \omega_1 | \omega_2 \rangle \Rightarrow <W_1|W_2>$: It denotes that if $\omega_1 (or\ \omega_2)$ is realized then $W_1 (or\ W_2)$ would be realized.
- ! : This symbol denotes the wait function on the input communication channel.
- *In* : It means a function that returns a received message on the input communication channel.
- [ ] : The symbol "[ ]" denotes to keep the conditions inside this symbol.

Now the following formal predicates are defined for the analysis of the cryptographic protocols.

- $A||\{W\}$: It denotes an action that means "A performs the task W". The symbol "$\{W\}$" implies a stream of the symbols, for example $\{W_1 \wedge W_2 \vee W_3 \ldots\}$.
- $A||\{W\}$ *SetName* : [*Cond*] : It denotes an action that means "A performs task W and results in the condition *Cond*". The symbol "$\{W\}$" implies a stream of the symbols, for example $\{W_1 \wedge W_2 \vee W_3 \ldots\}$. The symbol *SetName* denotes the tag name of the set of *Cond*.
- $A||W \xrightarrow{\{I\}} B$: It denotes an action that means "A sends the information I to B after performing the task W". The symbol "$\{I\}$" implies a stream of the symbols, for example $\{I_1 \circ I_2 \circ \ldots \circ I_n\}$.
- $A||\{W\} \xrightarrow{\{I\}} B$ *SetName* : [*Cond*] : It denotes an action that means "A sends the information I to B after performing the task W and also results in the condition *Cond*".
- $A||\{\} \xrightarrow{\{I\}} B$: It denotes an action that means "A sends the information I to B without performing any task". The symbol of empty "{}" implies that A does not perform ant kind of task.
- $A||\{\} \xrightarrow{\{I\}} B$ *SetName* : [*Cond*] : It denotes an action that means "A sends the information I to B without performing any task and also results in the condition *Cond*".
- P_Γ: [$Cond_p$] : It denotes a set of preconditions $Cond_p$ that should be defined before starting the cryptographic protocol Γ.
- I_Γ: [$Cond_I$] : It denotes a set of invariant conditions $Cond_I$ that should be kept through the whole execution of the cryptographic protocol Γ.
- Ω_Γ: [$Cond_\Omega$] : It denotes a set of post conditions $Cond_\Omega$ that should be satisfied after termination of the cryptographic protocol Γ.
- F_Γ: [$Cond_F$] : It denotes a set of final conditions $Cond_F$ that can be obtained from the calculus of the whole cryptographic protocol Γ.

2. *Logical Reasoning*

For logical reasoning about the cryptographic protocols, the following procedures are given as a formal approach :

Phase 1 : Define the sets of conditions for a cryptographic protocol before describing it as a formal one. Three sets, e.g., P_Γ: [$Cond_p$], I_Γ: [$Cond_I$], and Ω_Γ: [$Cond_\Omega$], should be clearly and unambiguously set out in this phase.

Phase 2 : Describe a formal form of the cryptographic protocol using the formal notations. The formal steps should be consistent with the informal steps of the cryptographic protocol.

Phase 3 : Make a logical calculus on all steps of the cryptographic protocol based on its formal description. This step will continue when the cryptographic protocol terminates. This step will also produce a set of final conditions, called F_Γ: [$Cond_F$], that may present the status or health of this protocol.

Phase 4 : Evaluate the cryptographic protocol. The cryptographic protocol is correct as an intended pursuit, if the following holds :

$$(I_\Gamma: [Cond_I] \Rightarrow F_\Gamma: [Cond_F]) \wedge (\Omega_\Gamma: [Cond_\Omega] \Rightarrow F_\Gamma: [Cond_F]).$$

III. An Authentication Protocol for CDMA Mobile Communication System

In this section, the five kinds of protocols are discussed for evaluating the IS-95 CDMA authentication protocol [2]. An attack is also presented to show the system could not provide the correctness with respect to these conditions. The security and Correctness of the protocol transaction are analyzed. An optimized and efficient authentication protocol is proposed for the CDMA mobile communication system in order to keep the system from falling into the incorrect state in the section TV. A proof of correctness and an analysis of the proposed scheme are also given in the next section.

1. Network Overview of CDMA Mobile Communication System

The CDMA mobile communication system consists of mobile station (MS), base station (BS), mobile switching center (MSC), visitor location register (VLR), home location register (HLR) and authentication center (AC) [2]. Both private and system wide security information are stored only on AC and MS for authentication, signaling encryption, and voice privacy. The AC is assumed to be the trusted center to enforce the security service, and could be coupled with HLR. There would also be multiple ACs on the mobile communication network. Figure 1 represents a schematic network overview of the CDMA mobile communication system.

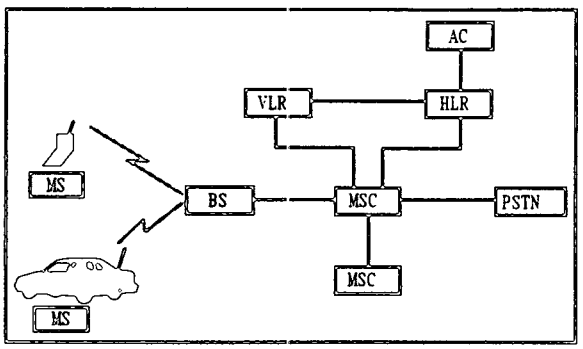


Fig. 1. Network overview of CDMA mobile communication system.

2. Authentication Protocol of CDMA Mobile Communication System

1) System Information and Algorithms

Proposed IS-95 CDMA mobile communication system potentially provides the several security services such as authentication, signaling message encryption and voice privacy [2]. These security services can be implemented by the security mechanisms of authentication signature algorithm (CAVE), shared secret data generation algorithm (SSDGEN), signaling message encryption algorithm (CMEA) and voice privacy algorithm. System information used for authentication procedure consists of two-bit AUTH field, four kinds of random variables such as 32-bit RAND, 24-bit RANDU, 56-bit RANDSSD, 32-bit RANDBS, 32-bit Electronic Serial Number (ESN), 34-bit Mobile Identification Number (MIN), 24-bit DIGITS, 64-bit A-key, 6-bit COUNT, 128-bit Shared Secret Data (SSD) composed of 64-bit SSD_A and 64-bit SSD_B.

2) Review of IS-95 Authentication Protocols

The CDMA mobile communication system supports five fundamental authentication procedures between the MS and the BS according to the proposal of Telecommunications Industry Association/Electronics Industry Association (TIA/EIA) IS-95 [2]. These authentication procedures should be incorporated to the inter-systems including MSC, VLR, HLR and AC as a description of TIA/EIA IS-41 [1]. The five authentication protocols (AP) are described as follows :

o AP-1 : Authentication Protocol of MS Registration

1) BS ---> MS : RAND
2) MS : AUTHR = CAVE(RAND, ESN, MIN1, SSD_A)
3) MS ---> BS : AUTHR, RAND, COUNT
4) BS : Verify ESN, MIN, and RAND;
   AUTHR = CAVE(RAND, ESN, MIN1, SSD_A);
   Compare received AUTHR with calculated AUTHR;
   Verify COUNT; (Optionally)
   If comparison is not successful, the MS shall perform Authentication Protocol of Unique Challenge-Response or perform Authentication Protocol of the Updating the Shared Secret Data;

o AP-2 : Authentication Protocol of MS Origination

1) BS ---> MS : RAND
2) MS : AUTHR = CAVE(RAND, ESN, DIGITS, SSD_A)
3) MS ---> BS : AUTHR, RAND, COUNT
4) BS : Verify ESN, MIN, RAND;
   AUTHR = CAVE(RAND, ESN, DIGITS, SSD_A);
   Compare received AUTHR with calculated AUTHR;
   Verify COUNT;
   If comparison is successful, the channel is allocated;
   If comparison is not successful, the MS shall perform Authentication Protocol of Unique Challenge-Response, or perform Authentication Protocol of the Updating the Shared Secret Data;

o AP-3 : Authentication Protocol of MS Termination

1) BS ---> MS : RAND
2) MS : AUTHR = CAVE(RAND, ESN, MIN1, SSD_A);
3) MS ---> BS : AUTHR, RAND, COUNT
4) BS : Verify ESN, MIN, and RAND;

AUTHR = CAVE(RAND, ESN, MIN1, SSD_A);
Compare received AUTHR with calculated AUTHR;
Verify COUNT;
If comparison is successful, the channel is allocated;
If comparison is not successful, the MS shall perform Authentication Protocol of Unique Challenge-Response or perform Authentication Protocol of the Updating the Shared Secret Data;

o AP-4 : Authentication Protocol of Unique Challenge-Response

1) BS ---> MS : RANDU
2) MS : AUTHU = CAVE({RANDU,MIN2}, ESN, MIN1, SSD_A);
3) MS ---> BS : AUTHU
4) BS : Verify ESN and MIN;
AUTHU = CAVE({RANDU, MIN2}, ESN, MIN1, SSD_A);
Compare received AUTHU with calculated AUTHU;
If comparison is not successful, the MS shall perform Authentication Protocol of Updating the Shared Secret Data;

o AP-5 : Authentication Protocol of Updating SSD

1) BS : Generate RANDSSD;
{SSD_A_NEW,SSD_B_NEW}=SSDGEN(RANDSSD, ESN, A-key);
2) BS ---> MS : RANDSSD
3) MS : {SSD_A_NEW, SSD_B_NEW}=SSDGEN (RANDSSD, ESN, A-key);
Generate RANDBS;
AUTHBS=CAVE(RANDBS, ESN, MIN1, SSD_A_NEW);
4) MS ---> BS : RANDBS
5) BS : AUTHBS = CAVE(RANDBS, ESN, MIN1, SSD_A_NEW);
6) BS ---> MS : AUTHBS
7) MS : Compare AUTHBS with calculated AUTHBS;
8) MS ---> BS : If the comparison is successful, the MS shall send an SSD Update Confirmation order to the BS; If the comparison is not successful, the MS shall discard SSD_A_NEW and SSD_B_NEW, and shall send an SSD Update Rejection Order to the BS;

3. Analysis of Authentication Protocol

This section describes an analysis to verify whether the system is correct or not. To do this, an attack is presented in order to show that the system may fall into the incorrect state. It is assumed that an impersonated MS' could handle the protocol transaction regardless of the processing state. We suppose that the MS' does not know A-key and SSD_A of the MS.

<Attack 1 on AP-5>

In 7) and 8) steps of the authentication protocol AP-5, if the comparison is not successful, the MS shall discard SSD_A_NEW and SSD_B_NEW, and also MS shall send an SSD Update Rejection Order to the BS for the purpose of cancellation of the SSD Update procedure with consistency. If the impersonated MS' can send an SSD Update Confirmation Order to the BS regardless of the comparison status in the step 7) and 8) of AP-5, the BS, strictly speaking AC/HLR, should set SSD_A and SSD_B to SSD_A_NEW and SSD_B_NEW, respectively. This attack demonstrates that the system is not correct any more.

IV. Proposed Authentication Protocol

1. Informal Description

We propose a mutual authentication scheme, called AP-6, to enhance the AP-5 [4][5]. It is considerably important to decide whether SSD_A and SSD_B should be updated or not on both of the MS and the BS sides. Additionally, the signal authentication scheme is also recommended to prevent the impersonated terminal from sending the security related signals such as SSD Update Confirmation Order.

o AP-6 : Proposed Authentication Protocol for Updating SSD

1) BS : Generate RANDSSD;
{SSD_A_NEW, SSD_B_NEW} = SSDGEN (RANDSSD, ESN, A-key);
2) BS ---> MS : RANDSSD
3) MS : {SSD_A_NEW, SSD_B_NEW} = SSDGEN (RANDSSD, ESN, A-key);
Generate RANDBS;
AUTHBS = CAVE(RANDBS, ESN, MIN1, SSD_A_NEW);
4) MS ---> BS : RANDBS
5) BS : AUTHBS = CAVE(RANDBS, ESN, MIN1, SSD_A_NEW);
6) BS ---> MS : AUTHBS
7) MS : Compare AUTHBS with calculated AUTHBS;
8) MS ---> BS : If the comparison is not successful, the MS shall discard SSD_A_NEW and SSD_B_NEW, send an SSD Update Rejection Order to the BS, and drop it; If the comparison is successful, the MS shall send an SSD Update Confirmation Order to the BS;
9) If the BS receives an SSD Update Rejection Order from the MS, then the BS discards SSD_A_NEW and

SSD_B_NEW, and drops it; If the BS receives an SSD Update Confirmation Order from the MS, then the BS performs the following steps;

9.1) BS ---> MS : RANDU

9.2) MS : AUTHU = CAVE({RANDU, MIN2}, ESN, MIN1, SSD_A_NEW);

9.3) MS ---> BS : AUTHU

9.4) BS : Verify ESN and MIN;
AUTHU = CAVE({RANDU, MIN2}, ESN, MIN1, SSD_A_NEW);
Compare received AUTHU with calculated AUTHU;

9.5) BS ---> MS : If comparison is not successful, the BS shall discard SSD_A_NEW and SSD_B_NEW, send an SSD Update Rejection Order to the MS, and drop it; If the comparison is successful, the BS shall send an SSD Update Confirmation Order to the MS and update the SSD values;

9.6) MS : If the previous kept as the success in step 8) and the SSD Update Confirmation Order is now received, the MS shall update the SSD values.

2. Formal Description

A formal description of AP-6 is as follows : Let $SSD\_A_A^B$ denote A's SSD_A calculated by B. Let $AUTHBS_A^B$ and $AUTHU_A^B$ denote A's AUTHBS and A's AUTHU calculated by B, respectively. Let $A-key_A^B$ denote the A's secret A-key stored on B side.

Formal Description of AP-6

1. $BS \| \{RANDSSD \leftarrow \Phi \wedge$
$\{\overline{SSD\_A_{MS}^{BS}}, \overline{SSD\_B_{MS}^{BS}}\} \leftarrow SSDGEN(RANDSSD, ESN, A-key_{MS}^{BS})\}$
$\xrightarrow{\{RANDSSD\}} MS.$

2. $MS \| \{\{\overline{SSD\_A_{MS}^{MS}}, \overline{SSD\_B_{MS}^{MS}}\} \leftarrow SSDGEN(RANDSSD, ESN, A-key_{MS}^{MS}) \wedge$
$RANDBS \leftarrow \Phi \wedge$
$AUTHBS_{BS}^{MS} \leftarrow CAVE(RANDBS, ESN, MIN1, \overline{SSD\_A_{MS}^{MS}})\}$
$\xrightarrow{\{RANDBS\}} BS.$

3. $BS \| \{AUTHBS_{BS}^{BS} \leftarrow CAVE(RANDBS, ESN, MIN1, \overline{SSD\_A_{MS}^{BS}})\}$
$\xrightarrow{\{AUTHBS_{BS}^{BS}\}} MS.$

4. $MS \| \{AUTHBS_{BS}^{MS} \,?\, AUTHBS_{BS}^{BS} \Rightarrow \langle \omega_1 | \omega_2 \rangle\}$
4.1 $\omega_1 : MS \| \{\} \xrightarrow{\{SSD\_Update\_Confirmation\_Order\}} BS.$
4.2 $\omega_2 : MS \| \{\Omega\} \xrightarrow{\{SSD\_Update\_Rejection\_Order\}} BS.$

5. $BS \| \{\langle Case_1 | Case_2 \rangle \Rightarrow \langle \Omega | RANDU \leftarrow \Phi \rangle\} \xrightarrow{\{RANDU\}} MS.$
where $Case_1 : In = SSD\_Update\_Rejection\_Order$ and
$Case_2 : In = SSD\_Update\_Confirmation\_Order.$

6. $MS \| \{AUTHU_{MS}^{MS} \leftarrow CAVE(\{RANDU, MIN2\}, ESN, MIN1, \overline{SSD\_A_{MS}^{MS}})\}$
$\xrightarrow{\{AUTHU_{MS}^{MS}\}} BS.$

7. $BS \| \{AUTHU_{MS}^{BS} \leftarrow CAVE(\{RANDU, MIN2\}, ESN, MIN1, \overline{SSD\_A_{MS}^{BS}}) \wedge$
$AUTHU_{MS}^{MS} \,?\, AUTHU_{MS}^{BS} \Rightarrow \langle \omega_3 | \omega_4 \rangle\}$
7.1 $\omega_3 : BS \| \{\{SSD\_A_{MS}^{BS}, SSD\_B_{MS}^{BS}\} \leftarrow \{\overline{SSD\_A_{MS}^{BS}}, \overline{SSD\_B_{MS}^{BS}}\}\}$
$\xrightarrow{\{SSD\_Update\_Confirmation\_Order\}} MS.$
7.2 $\omega_4 : BS \| \{\Omega\} \xrightarrow{\{SSD\_Update\_Rejection\_Order\}} MS.$

8. $MS \| \{In = SSD\_Update\_Confirmation\_Order \Rightarrow \langle \{SSD\_A_{MS}^{MS}, SSD\_B_{MS}^{MS}\} \leftarrow \{\overline{SSD\_A_{MS}^{MS}}, \overline{SSD\_B_{MS}^{MS}}\} | \Omega \rangle\}.$

3. Formal Verification

We analyze two attacks to verify whether AP-6 can be correct against these attacks or not. Firstly, it is assumed that there is an impersonated MS, called MS' as the previous section, for the proposed AP-6. In the step 8) of the AP-6, the MS' may send an SSD Update Confirmation Order to the BS regardless of the comparison status in the step 7). Then, the BS may receive the SSD Update Confirmation Order sent from the MS' in the step 9). Therefore, the BS shall send a RANDU in the step 9.1) and wait to receive a AUTHU sent from the MS'. Since the MS' can not generate the original SSD_A_NEW due to the unknown A-key, the generated AUTHU of the step 9.2) is not equivalent to the original one. The BS also can know that the received AUTHU is not equivalent to the calculated AUTHU in the step 9.4). Then, the BS shall discard SSD_A_NEW and SSD_B_NEW, send an SSD Update Rejection Order to the MS', and drop it. Therefore, the BS can keep these SSD_A and SSD_B from being violated.

Secondly, it is also assumed that there is an impersonated BS, called BS', for the proposed AP-6. In the step 5) of the AP-6, the BS' may send an AUTHBS to the MS. Then, the MS may receive the AUTHBS sent from the BS' in the step 6). Since the BS' can not generate the original AUTHBS, in the step 5), due to the unknown A-key and SSD_A_NEW, the generated AUTHBS is not equivalent to the original one. The MS also can know that the received AUTHBS is not equivalent to the calculated AUTHBS in the step 7). Then, the MS shall discard SSD_A_NEW and SSD_B_NEW, send an SSD Update Rejection Order to the BS', and drop it. Therefore, the MS can keep these SSD_A and SSD_B from being violated.

The above two cases can be analyzed formally through a formal description and verification for the proposed scheme AP-6. For a formal verification, three sets of conditions are derived such as a set of preconditions, a set of invariant conditions and a set of post conditions from the formal description of AP-6.

- A set of preconditions

$$P_{AP-6}:[(BS \wedge MS)\perp(CAVE \wedge SSDGEN) \wedge (BS \wedge MS)\perp\Phi \wedge BS\perp\{SSD\_A_{MS}^{BS}, SSD\_B_{MS}^{BS}\} \wedge MS\perp\{SSD\_A_{MS}^{MS}, SSD\_B_{MS}^{MS}\} \wedge \{SSD\_A_{MS}^{BS}, SSD\_B_{MS}^{BS}\} = \{SSD\_A_{MS}^{MS}, SSD\_B_{MS}^{MS}\} \wedge BS\perp A-key_{MS}^{BS} \wedge MS\perp A-key_{MS}^{MS} \wedge A-key_{MS}^{BS} = A-key_{MS}^{MS} \wedge \sim(X\perp A-key_{MS})].$$

Suppose X means an opponent. This set of preconditions means i) BS and MS know CAVE and SSDGEN functions and a random number generator Φ, ii) only BS and MS know MS's SSD_A and SSD_B as the secret information, and iii) only BS and MS also know MS's secret A-key. It is assumed that $A-key_{MS} = A-key_{MS}^{MS} = A-key_{MS}^{BS}$. Both of legal BS and MS have same values of SSD_A, SSD_B, and A-key.

○ A set of invariant conditions

$$I_{AP-6}:[\sim(X\perp SSD\_A_{MS}) \wedge \sim(X\perp SSD\_B_{MS}) \wedge \sim(X\perp A-key_{MS})]$$

This set of invariant conditions also can be derived from the review of AP-6 protocol. It means that each SSD_A_{MS}, SSD_B_{MS}, and $A-key_{MS}$ should not be revealed to an opponent X.

○ A set of post conditions

$$\Omega_{AP}:[\{SSD\_A_{MS}^{BS}, SSD\_B_{MS}^{BS}\} = \{SSD\_A_{MS}^{MS}, SSD\_B_{MS}^{MS}\}]$$

This set of post conditions means that SSD_A_{MS} and SSD_B_{MS} should be consistent on both of BS and MS sides when the protocol terminates.

<Attack 1 on AP-6> As same as attack 1 on AP-5, suppose that an opponent X may impersonate MS and send the SSD Update Confirmation Order message to BS in the step 4 of the formal description of AP-6. This attack may cause that BS updates the SSD_A and SSD_B values regardless of the invalid AUTH13S in the step 4 of the formal description of AP-6. This would yield that SSD values on BS side may not be consistent with those of MS side. Therefore, AP-6 shall fail in the next call attempt.

Formal Description of Attack 1 on AP-6

1. $BS\|\{RANDSSD \leftarrow \Phi \wedge \{\overline{SSD\_A_{MS}^{BS}}, \overline{SSD\_B_{MS}^{BS}}\} \leftarrow SSDGEN(RANDSSD, ESN, A-key_{MS}^{BS})\} \xrightarrow{\{RANDSSD\}} MS.$
2. $X\|\{\{\overline{SSD\_A_{MS}^{X}}, \overline{SSD\_B_{MS}^{X}}\} \leftarrow SSDGEN(RANDSSD, ESN, A-key_{MS}^{X}) \wedge RANDBS \leftarrow \Phi \wedge AUTHBS_{BS}^{X} \leftarrow CAVE(RANDBS, ESN, MIN1, \overline{SSD\_A_{MS}^{X}})\} \xrightarrow{\{RANDBS\}} BS.$
3. $BS\|\{AUTHBS_{BS}^{BS} \leftarrow CAVE(RANDBS, ESN, MIN1, \overline{SSD\_A_{MS}^{BS}})\} \xrightarrow{\{AUTHBS_{BS}^{BS}\}} X.$
4. $X\|\{!\} \xrightarrow{\{SSD\_Update\_Confirmation\_Order\}} BS.$
5. $BS\|\{\langle Case_1 | Case_2\rangle \Rightarrow \langle\Omega | RANDU \leftarrow \Phi\rangle\} \xrightarrow{\{RANDU\}} X,$
   where $Case_1$: $In = SSD\_Update\_Rejection\_Order$ and
   $Case_2$: $In = SSD\_Update\_Confirmation\_Order$.
6. $X\|\{AUTHU_{MS}^{X} \leftarrow CAVE(\{RANDU, MIN2\}, ESN, MIN1, \overline{SSD\_A_{MS}^{X}})\} \xrightarrow{\{AUTHU_{MS}^{X}\}} BS.$
7. $BS\|\{AUTHU_{MS}^{BS} \leftarrow CAVE(\{RANDU, MIN2\}, ESN, MIN1, \overline{SSD\_A_{MS}^{BS}}) \wedge AUTHU_{MS}^{X} ? AUTHU_{MS}^{BS} \Rightarrow \langle\omega_3 | \omega_4\rangle\}.$
   7.1 ω_3 : $BS\|\{\{SSD\_A_{MS}^{BS}, SSD\_B_{MS}^{BS}\} \leftarrow \{\overline{SSD\_A_{MS}^{BS}}, \overline{SSD\_B_{MS}^{BS}}\}\} \xrightarrow{\{SSD\_Update\_Confirmation\_Order\}} X.$
   7.2 ω_4 : $BS\|\{\Omega\} \xrightarrow{\{SSD\_Update\_Rejection\_Order\}} X.$

In the step 7 of the above formal description for Attack 1, AP-6 shall terminate because the validation of $AUTH_{MS}^{X}$? $AUTHU_{MS}^{BS}$ yields FALSE. A formal verification for the case of Attack 1 is as follows :

Definition 1 Let AP-6 be correct against Attack 1 if SSD_A and SSD_B can be maintained consistently on both of BS and MS sides. This implies that AP-6 is correct against Attack 1 if $(\Omega_{AP-6} \Rightarrow F_{AP-6})$ and $(I_{AP-6} \Rightarrow F_{AP-6})$ hold.

Proposition 1 AP-6 is correct against Attack 1.

<Proof> On the basis of the initial set of preconditions P_{AP-6} and the formal description of Attack 1 on AP-6, the following logical calculus is given in order to show that proposition 1 holds.

1. $BS\|\{RANDSSD \leftarrow \Phi \wedge \{\overline{SSD\_A_{MS}^{BS}}, \overline{SSD\_B_{MS}^{BS}}\} \leftarrow SSDGEN(RANDSSD, ESN, A-key_{MS}^{BS})\} \xrightarrow{\{RANDSSD\}} MS$
   $F_{AP-6}:[(BS \wedge MS)\perp(CAVE \wedge SSDGEN) \wedge (BS \wedge MS)\perp\Phi \wedge BS\perp\{SSD\_A_{MS}^{BS}, SSD\_B_{MS}^{BS}\} \wedge MS\perp\{SSD\_A_{MS}^{MS}, SSD\_B_{MS}^{MS}\} \wedge \{SSD\_A_{MS}^{BS}, SSD\_B_{MS}^{BS}\} = \{SSD\_A_{MS}^{MS}, SSD\_B_{MS}^{MS}\} \wedge BS\perp A-key_{MS}^{BS} \wedge MS\perp A-key_{MS}^{MS} \wedge A-key_{MS}^{BS} = A-key_{MS}^{MS} \wedge \sim(X\perp A-key_{MS}) \wedge \{SSD\_A_{MS}^{BS}, SSD\_B_{MS}^{BS}\} \neq \{\overline{SSD\_A_{MS}^{BS}}, \overline{SSD\_B_{MS}^{BS}}\}].$
2. $X\|\{\{\overline{SSD\_A_{MS}^{X}}, \overline{SSD\_B_{MS}^{X}}\} \leftarrow SSDGEN(RANDSSD, ESN, A-key_{MS}^{X}) \wedge RANDBS \leftarrow \Phi \wedge AUTHBS_{BS}^{X} \leftarrow CAVE(RANDBS, ESN, MIN1, \overline{SSD\_A_{MS}^{X}})\} \xrightarrow{\{RANDBS\}} BS$
   $F_{AP-6}:[(BS \wedge MS \wedge X)\perp(CAVE \wedge SSDGEN) \wedge (BS \wedge MS \wedge X)\perp\Phi \wedge BS\perp\{SSD\_A_{MS}^{BS}, SSD\_B_{MS}^{BS}\} \wedge MS\perp\{SSD\_A_{MS}^{MS}, SSD\_B_{MS}^{MS}\} \wedge \{SSD\_A_{MS}^{BS}, SSD\_B_{MS}^{BS}\} = \{SSD\_A_{MS}^{MS}, SSD\_B_{MS}^{MS}\} \wedge BS\perp A-key_{MS}^{BS} \wedge MS\perp A-key_{MS}^{MS} \wedge A-key_{MS}^{DS} = A-key_{MS}^{MS} \wedge \sim(X\perp A-key_{MS}) \wedge \{SSD\_A_{MS}^{BS}, SSD\_B_{MS}^{DS}\} \neq \{\overline{SSD\_A_{MS}^{BS}}, \overline{SSD\_B_{MS}^{DS}}\} \wedge X\perp(ESN \wedge MIN1 \wedge AUTHBS_{BS}^{X} \wedge A-key_{MS}^{X}) \wedge A-key_{MS}^{X} \neq A-key_{MS}^{DS} \wedge \{\overline{SSD\_A_{MS}^{X}}, \overline{SSD\_B_{MS}^{X}}\} \neq \{\overline{SSD\_A_{MS}^{BS}}, \overline{SSD\_B_{MS}^{DS}}\}].$

3. $BS \| \{AUTHBS_{BS}^{BS} \leftarrow CAVE(RANDBS, ESN, MIN1, \overline{SSD\_A_{MS}^{BS}})\}$

$\xrightarrow{\{AUTHBS_{BS}^{BS}\}} X$

F_{AP-6}:$[(BS \wedge MS \wedge X) \perp (CAVE \wedge SSDGEN) \wedge (BS \wedge MS \wedge X) \perp \Phi \wedge$
$BS \perp \{SSD\_A_{MS}^{BS}, SSD\_B_{MS}^{BS}\} \wedge MS \perp \{SSD\_A_{MS}^{MS}, SSD\_B_{MS}^{MS}\} \wedge$
$\{SSD\_A_{MS}^{BS}, SSD\_B_{MS}^{BS}\} = \{SSD\_A_{MS}^{MS}, SSD\_B_{MS}^{MS}\} \wedge$
$BS \perp A - key_{MS}^{BS} \wedge MS \perp A - key_{MS}^{MS} \wedge A - key_{MS}^{BS} = A - key_{MS}^{MS} \wedge$
$\sim (X \perp A - key_{MS}) \wedge \{SSD\_A_{MS}^{BS}, SSD\_B_{MS}^{BS}\} \neq \{\overline{SSD\_A_{MS}^{BS}}, \overline{SSD\_B_{MS}^{BS}}\} \wedge$
$X \perp (ESN \wedge MIN1 \wedge AUTHBS_{BS}^{X} \wedge A - key_{MS}^{X}) \wedge A - key_{MS}^{X} \neq A - key_{MS}^{BS} \wedge$
$\{\overline{SSD\_A_{MS}^{X}}, \overline{SSD\_B_{MS}^{X}}\} \neq \{\overline{SSD\_A_{MS}^{BS}}, \overline{SSD\_B_{MS}^{BS}}\} \wedge$
$AUTHBS_{BS}^{X} \neq AUTHBS_{BS}^{BS}]$.

4. $X \| \{!\} \xrightarrow{\{SSD\_Update\_Confirmation\_Order\}} BS$

F_{AP-6} has the same conditions of the above step 3.

5. $BS \| \{\langle Case_1 | Case_2 \rangle \Rightarrow \langle \Omega | RANDU \leftarrow \Phi \rangle\} \xrightarrow{\{RANDU\}} X$,

where $Case_1$: $In = SSD\_Update\_Rejection\_Order$ and

$Case_2$: $In = SSD\_Update\_Confirmation\_Order$

F_{AP-6} has the same conditions of the above step 4.

6. $X \| \{AUTHU_{MS}^{X} \leftarrow CAVE(\{R6ANDU, MIN2\}, ESN, MIN1, \overline{SSD\_A_{MS}^{X}})\}$

$\xrightarrow{\{AUTHU_{MS}^{X}\}} BS$.

F_{AP-6}:$[(BS \wedge MS \wedge X) \perp (CAVE \wedge SSDGEN) \wedge (BS \wedge MS \wedge X) \perp \Phi \wedge$
$BS \perp \{SSD\_A_{MS}^{BS}, SSD\_B_{MS}^{BS}\} \wedge MS \perp \{SSD\_A_{MS}^{MS}, SSD\_B_{MS}^{MS}\} \wedge$
$\{SSD\_A_{MS}^{BS}, SSD\_B_{MS}^{BS}\} = \{SSD\_A_{MS}^{MS}, SSD\_B_{MS}^{MS}\} \wedge$
$BS \perp A - key_{MS}^{BS} \wedge MS \perp A - key_{MS}^{MS} \wedge A - key_{MS}^{BS} = A - key_{MS}^{MS} \wedge$
$\sim (X \perp A - key_{MS}) \wedge \{SSD\_A_{MS}^{BS}, SSD\_B_{MS}^{BS}\} \neq \{\overline{SSD\_A_{MS}^{BS}}, \overline{SSD\_B_{MS}^{BS}}\} \wedge$
$X \perp (ESN \wedge MIN1 \wedge AUTHBS_{BS}^{X} \wedge A - key_{MS}^{X}) \wedge A - key_{MS}^{X} \neq A - key_{MS}^{BS} \wedge$
$\{\overline{SSD\_A_{MS}^{X}}, \overline{SSD\_B_{MS}^{X}}\} \neq \{\overline{SSD\_A_{MS}^{BS}}, \overline{SSD\_B_{MS}^{BS}}\} \wedge$
$AUTHBS_{BS}^{X} \neq AUTHBS_{BS}^{BS} \wedge X \perp AUTHU_{MS}^{X}]$.

7. $BS \| \{AUTHU_{MS}^{BS} \leftarrow CAVE(\{RANDU, MIN2\}, ESN, MIN1, \overline{SSD\_A_{MS}^{BS}}) \wedge$
$AUTHU_{MS}^{X} \neq AUTHU_{MS}^{BS} \wedge \omega_4\}$

F_{AP-6}:$[(BS \wedge MS \wedge X) \perp (CAVE \wedge SSDGEN) \wedge (BS \wedge MS \wedge X) \perp \Phi \wedge$
$BS \perp \{SSD\_A_{MS}^{BS}, SSD\_B_{MS}^{BS}\} \wedge MS \perp \{SSD\_A_{MS}^{MS}, SSD\_B_{MS}^{MS}\} \wedge$
$\{SSD\_A_{MS}^{BS}, SSD\_B_{MS}^{BS}\} = \{SSD\_A_{MS}^{MS}, SSD\_B_{MS}^{MS}\} \wedge$
$BS \perp A - key_{MS}^{BS} \wedge MS \perp A - key_{MS}^{MS} \wedge A - key_{MS}^{BS} = A - key_{MS}^{MS} \wedge$
$\sim (X \perp A - key_{MS}) \wedge \{SSD\_A_{MS}^{BS}, SSD\_B_{MS}^{BS}\} \neq \{\overline{SSD\_A_{MS}^{BS}}, \overline{SSD\_B_{MS}^{BS}}\} \wedge$
$X \perp (ESN \wedge MIN1 \wedge AUTHBS_{BS}^{X} \wedge A - key_{MS}^{X}) \wedge A - key_{MS}^{X} \neq A - key_{MS}^{BS} \wedge$
$\{\overline{SSD\_A_{MS}^{X}}, \overline{SSD\_B_{MS}^{X}}\} \neq \{\overline{SSD\_A_{MS}^{BS}}, \overline{SSD\_B_{MS}^{BS}}\} \wedge$
$AUTHBS_{BS}^{X} \neq AUTHBS_{BS}^{BS} \wedge X \perp AUTHU_{MS}^{X} \wedge$
$AUTHU_{MS}^{X} \neq AUTHU_{MS}^{BS}]$,

where ω_4 : $BS \| \{\Omega\} \xrightarrow{\{SSD\_Update\_Rejection\_Order\}} X$.

Since $(\Omega_{AP-6} \Rightarrow F_{AP-6})$ and $(I_{AP-6} \Rightarrow F_{AP-6})$ hold, AP-6 is correct against attack 1. □

<Attack 2 on AP-6> Suppose that an opponent X may impersonate BS and send the AUTHBS to MS in the step 3 of the formal description of AP-6. This attack may cause that MS updates the SSD_A and SSD_B. Therefore, SSD values on MS side may not be inconsistent with BS side.

Formal Description of Attack 2 on AP-6

1. $X \| \{RANDSSD \leftarrow \Phi \wedge$
$\{\overline{SSD\_A_{MS}^{X}}, \overline{SSD\_B_{MS}^{X}}\} \leftarrow SSDGEN(RANDSSD, ESN, A - key_{MS}^{X})\}$
$\xrightarrow{\{RANDSSD\}} MS$.
2. $MS \| \{\{\overline{SSD\_A_{MS}^{MS}}, \overline{SSD\_B_{MS}^{MS}}\} \leftarrow SSDGEN(RANDSSD, ESN, A - key_{MS}^{MS}) \wedge$
$RANDBS \leftarrow \Phi \wedge$
$AUTHBS_{BS}^{MS} \leftarrow CAVE(RANDBS, ESN, MIN1, \overline{SSD\_A_{MS}^{MS}})\}$
$\xrightarrow{\{RANDBS\}} X$.
3. $X \| \{AUTHBS_{BS}^{X} \leftarrow CAVE(RANDBS, ESN, MIN1, \overline{SSD\_A_{MS}^{X}})\}$
$\xrightarrow{\{AUTHBS_{BS}^{X}\}} MS$.
4. $MS \| \{AUTHBS_{BS}^{MS} ? AUTHBS_{BS}^{X} \Rightarrow \langle \omega_1 | \omega_2 \rangle\}$.
4.1 ω_1 : $MS \| \{!\} \xrightarrow{\{SSD\_Update\_Confirmation\_Order\}} BS$.
4.2 ω_2 : $MS \| \{\Omega\} \xrightarrow{\{SSD\_Update\_Rejection\_Order\}} BS$.

In the step 4 of the above formal description for Attack 2, AP-6 shall terminate because the validation of $AUTHBS_{HS}^{MS}$? $AUTHBS_{BS}^{X}$ yields FALSE. A formal verification for the case of Attack 2 is as follows :

Definition 2 Let AP-6 be correct against Attack 2 if SSD_A and SSD_B can be maintained consistently on both of BS and MS sides. This implies that AP-6 is correct against Attack 2 if $(\Omega_{AP-6} \Rightarrow F_{AP-6})$ and $(I_{AP-6} \Rightarrow F_{AP-6})$ hold.

Proposition 2 AP-6 is correct against Attack 2.

<Proof> On the basis of the initial set of preconditions and the formal description of Attack 2 on AP-6, the following logical calculus is given to show that proposition 2 holds.

1. $X \| \{RANDSSD \leftarrow \Phi \wedge$
$\{\overline{SSD\_A_{MS}^{X}}, \overline{SSD\_B_{MS}^{X}}\} \leftarrow SSDGEN(RANDSSD, ESN, A - key_{MS}^{X})\}$
$\xrightarrow{\{RANDSSD\}} MS$
F_{AP-6}:$[(BS \wedge MS \wedge X) \perp (CAVE \wedge SSDGEN) \wedge (BS \wedge MS \wedge X) \perp \Phi \wedge$
$BS \perp \{SSD\_A_{MS}^{BS}, SSD\_B_{MS}^{BS}\} \wedge MS \perp \{SSD\_A_{MS}^{MS}, SSD\_B_{MS}^{MS}\} \wedge$
$\{SSD\_A_{MS}^{BS}, SSD\_B_{MS}^{BS}\} = \{SSD\_A_{MS}^{MS}, SSD\_B_{MS}^{MS}\} \wedge$
$BS \perp A - key_{MS}^{BS} \wedge MS \perp A - key_{MS}^{MS} \wedge A - key_{MS}^{BS} = A - key_{MS}^{MS} \wedge$
$\sim (X \perp A - key_{MS}) \wedge A - key_{MS}^{X} \neq A - key_{MS}^{BS} \wedge$
$\{SSD\_A_{MS}^{BS}, SSD\_B_{MS}^{BS}\} \neq \{SSD\_A_{MS}^{X}, SSD\_B_{MS}^{X}\} \wedge$
$\{SSD\_A_{MS}^{BS}, SSD\_B_{MS}^{BS}\} \neq \{\overline{SSD\_A_{MS}^{X}}, \overline{SSD\_B_{MS}^{X}}\}]$.
2. $MS \| \{\{\overline{SSD\_A_{MS}^{MS}}, \overline{SSD\_B_{MS}^{MS}}\} \leftarrow SSDGEN(RANDSSD, ESN, A - key_{MS}^{MS}) \wedge$
$RANDBS \leftarrow \Phi \wedge$
$AUTHBS_{BS}^{MS} \leftarrow CAVE(RANDBS, ESN, MIN1, \overline{SSD\_A_{MS}^{MS}})\}$
$\xrightarrow{\{RANDBS\}} X$
F_{AP-6}:$[(BS \wedge MS \wedge X) \perp (CAVE \wedge SSDGEN) \wedge (BS \wedge MS \wedge X) \perp \Phi \wedge$
$BS \perp \{SSD\_A_{MS}^{BS}, SSD\_B_{MS}^{BS}\} \wedge MS \perp \{SSD\_A_{MS}^{MS}, SSD\_B_{MS}^{MS}\} \wedge$
$\{SSD\_A_{MS}^{BS}, SSD\_B_{MS}^{BS}\} = \{SSD\_A_{MS}^{MS}, SSD\_B_{MS}^{MS}\} \wedge$

$BS \perp A-key_{MS}^{BS} \wedge MS \perp A-key_{MS}^{MS} \wedge A-key_{MS}^{BS} = A-key_{MS}^{MS} \wedge$

$\sim(X \perp A-key_{MS}) \wedge A-key_{MS}^{X} \neq A-key_{MS}^{BS} \wedge A-key_{MS}^{X} \neq A-key_{MS}^{MS} \wedge$

$\{SSD\_A_{MS}^{BS}, SSD\_B_{MS}^{BS}\} \neq \{SSD\_A_{MS}^{X}, SSD\_B_{MS}^{X}\} \wedge$

$\{SSD\_A_{MS}^{BS}, SSD\_B_{MS}^{BS}\} \neq \{\overline{SSD\_A_{MS}^{X}}, \overline{SSD\_B_{MS}^{X}}\} \wedge MS \perp AUTHBS_{BS}^{MS} \wedge$

$\{\overline{SSD\_A_{MS}^{MS}}, \overline{SSD\_B_{MS}^{MS}}\} \neq \{\overline{SSD\_A_{MS}^{X}}, \overline{SSD\_B_{MS}^{X}}\}]$.

3. $X \| \{AUTHBS_{BS}^{X} \leftarrow CAVE(RANDBS, ESN, MIN1, \overline{SSD\_A_{MS}^{X}})\}$

$\xrightarrow{\{AUTHBS_{MS}^{X}\}} MS$.

F_{AP-6}:[$(BS \wedge MS \wedge X) \perp (CAVE \wedge SSDGEN) \wedge (BS \wedge MS \wedge X) \perp \Phi \wedge$

$BS \perp \{SSD\_A_{MS}^{BS}, SSD\_B_{MS}^{BS}\} \wedge MS \perp \{SSD\_A_{MS}^{MS}, SSD\_B_{MS}^{MS}\} \wedge$

$\{SSD\_A_{MS}^{BS}, SSD\_B_{MS}^{BS}\} = \{SSD\_A_{MS}^{MS}, SSD\_B_{MS}^{MS}\} \wedge$

$BS \perp A-key_{MS}^{BS} \wedge MS \perp A-key_{MS}^{MS} \wedge A-key_{MS}^{BS} = A-key_{MS}^{MS} \wedge$

$\sim(X \perp A-key_{MS}) \wedge A-key_{MS}^{X} \neq A-key_{MS}^{BS} \wedge A-key_{MS}^{X} \neq A-key_{MS}^{MS} \wedge$

$\{SSD\_A_{MS}^{BS}, SSD\_B_{MS}^{BS}\} \neq \{SSD\_A_{MS}^{X}, SSD\_B_{MS}^{X}\} \wedge$

$\{SSD\_A_{MS}^{BS}, SSD\_B_{MS}^{BS}\} \neq \{\overline{SSD\_A_{MS}^{X}}, \overline{SSD\_B_{MS}^{X}}\} \wedge MS \perp AUTHBS_{BS}^{MS} \wedge$

$\{\overline{SSD\_A_{MS}^{MS}}, \overline{SSD\_B_{MS}^{MS}}\} \neq \{\overline{SSD\_A_{MS}^{X}}, \overline{SSD\_B_{MS}^{X}}\} \wedge X \perp AUTHBS_{BS}^{X} \wedge$

$AUTHBS_{BS}^{MS} \neq AUTHBS_{BS}^{X}$].

4. $MS \| \{AUTHBS_{BS}^{MS} \neq AUTHBS_{BS}^{X} \wedge \omega_2\}$

F_{AP-6}:[$(BS \wedge MS \wedge X) \perp (CAVE \wedge SSDGEN) \wedge (BS \wedge MS \wedge X) \perp \Phi \wedge$

$BS \perp \{SSD\_A_{MS}^{BS}, SSD\_B_{MS}^{BS}\} \wedge MS \perp \{SSD\_A_{MS}^{MS}, SSD\_B_{MS}^{MS}\} \wedge$

$\{SSD\_A_{MS}^{BS}, SSD\_B_{MS}^{BS}\} = \{SSD\_A_{MS}^{MS}, SSD\_B_{MS}^{MS}\} \wedge$

$BS \perp A-key_{MS}^{BS} \wedge MS \perp A-key_{MS}^{MS} \wedge A-key_{MS}^{BS} = A-key_{MS}^{MS} \wedge$

$\sim(X \perp A-key_{MS}) \wedge A-key_{MS}^{X} \neq A-key_{MS}^{BS} \wedge A-key_{MS}^{X} \neq A-key_{MS}^{MS} \wedge$

$\{SSD\_A_{MS}^{BS}, SSD\_B_{MS}^{BS}\} \neq \{SSD\_A_{MS}^{X}, SSD\_B_{MS}^{X}\} \wedge$

$\{SSD\_A_{MS}^{BS}, SSD\_B_{MS}^{BS}\} \neq \{\overline{SSD\_A_{MS}^{X}}, \overline{SSD\_B_{MS}^{X}}\} \wedge MS \perp AUTHBS_{BS}^{MS} \wedge$

$\{\overline{SSD\_A_{MS}^{MS}}, \overline{SSD\_B_{MS}^{MS}}\} \neq \{\overline{SSD\_A_{MS}^{X}}, \overline{SSD\_B_{MS}^{X}}\} \wedge X \perp AUTHBS_{BS}^{X} \wedge$

$AUTHBS_{BS}^{MS} \neq AUTHBS_{BS}^{X}$],

where $\omega_2 : MS \| \{\Omega\} \xrightarrow{\{SSD\_Update\_Rejection\_Order\}} BS$.

Since $(\Omega_{AP-6} \Rightarrow F_{AP-6})$ and $(I_{AP-6} \Rightarrow F_{AP-6})$ hold, AP-6 is correct against attack 2.

As a result, it has been shown that the proposed scheme has the enhanced correctness. Hence it is more secure than the IS-95 authentication protocol for CDMA mobile communication network.

V. Conclusion

In this paper, we reviewed the TIA/EIA IS-95 CDMA authentication protocol mainly between the MS and the BS as a wireless communication link from the view points of security and correctness. It has been shown that the IS-95 CDMA authentication protocol might fall into the incorrect state. To enhance the correctness and security for the CDMA mobile communication network, we proposed a mutual authentication protocol, called AP-6. A formal logic has been presented in order to describe and verify the proposed authentication protocol AP-6 that is an improved version of AP-5 : IS-95 based authentication protocol of updating SSD. It has been shown that AP-6 could have more enhanced correctness and security than the IS-95 authentication protocol for CDMA mobile communication network.

References

[1] Telecommunications Industry Association/Electronics Industry Association (TIA/EIA), "Cellular Radio telecommunications Intersystem Operations : Automatic Roaming," Interim Standard 41.3 (Rev. B), Jul. 1991.

[2] Telecommunications Industry Association/Electronics Industry Association (TIA/EIA), "Interim Standard Mobile Station-Base Station Compatibility Standard for Dual-Mode Wide band Spread Spectrum Cellular System," Interim Standard 95, Jul. 1993.

[3] Ken Thompson and Dave Whipple Spokane Divn, "The essential concepts of CDMA," Asian Electronics Engineer, Vol. 7, No. 1, pp. 86 - 91 Apr. 1994,.

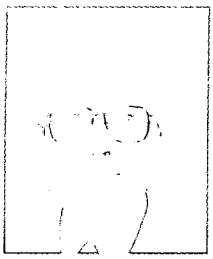
[4] Ki-Yoong Hong and Dong-Kyoo Kim, "Correctness of Authentication Protocol for IS-95 Based CDMA Mobile Communication Network," Journal of The Korean Institute of Information Security and Cryptology, Vol. 5, No. 2, pp. 23 - 36 Jun. 1995,.

[5] Ki-Yoong Hong, "Cryptographic Protocols and Secure Information Flow Control for Network Security," Ph.D. Dissertation, Department of Computer Engineering, AJOU University, 1996.

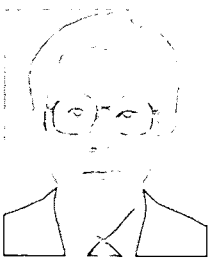
[6] Mello and P. Wayner, "Wireless Mobile Communications," Byte, Vol. 18, No. 2, pp. 147 - 154, Feb. 1993.

[7] Seshadri Mohan and Ravi Jain, "Two User Location Strategies for Personal Communications Services," IEEE Personal Communications, Vol. 1, No. 1, pp. 42 - 50, First Quarter 1994.

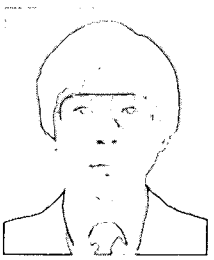
[8] Randy H. Katz, "Adaptation and Mobility in Wireless Information Systems," IEEE Personal Communications, Vol. 1, No. 1, pp. 6 - 17, First Quarter 1994.



Ki-Yoong Hong 1985. Cheon Nam National University (B.S.) 1990. Chung Ang University, Department of Computer Science (M.S.) 1994. 8. 8. P.E., MOST(Minister Of Science and Technology) 1996. AJOU University, Department of Computer Engineering (Ph.D.) 1985~1995. Researcher, Senior Researcher, ETRI 1992~1993. Senior Researcher, Alenia Spazio S.p.A., Italy 1995. Senior Researcher, NCA(National Computerization Agency) Jar.. 1995. Best Paper Award, '95 Joint Workshop on Information Security and Cryptology (JW-ISC'95), Inuyama, Japan Fields of Research Interest Information Communications and Networks; Computer and Network Security; Security Protocol; Cryptographic Protocol, etc.



Dong-Kyoo Kim Seoul National University, College of Engineering (B.E.). Kansas State University, Computer Science Department, Graduate School (Ph.D.). 1972~1976. Researcher, KIST. 1977~1979. Senior Researcher, ETRI 1984~1985. Professor, Kansas State University. 1993. Vice President, Korea Institute of Information Security and Cryptology. 1979. Professor, Department of Computer Engineering, AJOU University Fields of Research Interest Information Communications and Networks; Computer and Network Security; Protocol Engineering; Security Protocol; Security System, etc.



Seok-Woo Kim 1979. Civil Aviation of College (B.S.) 1984. YONSEI University (M.S.) 1989. New Jersey Institute of Technology (M.S.). 1995. AJOU University, Department of Computer Engineering (Ph.D.). 1987~1988. Visiting Researcher, AT&T BELL Lab. 1980. Principal Member of Research Staff, ETRI. Fields of Research Interest Information Communications and Networks; Computer and Network Security; Security Protocol, etc.