BAN Logic Analysis of SEHAP

I. Introduction

In this document, we prove the security of the SEHAP protocol using BAN logic. We outline the analysis goals, initial assumptions, standardized protocol results, and the proof process.

BAN logic is a deductive tool for proving security properties. First, goals are set and an idealized model is created for reasoning. Protocol steps are then converted into BAN logic formulas. Assumptions based on the protocol's characteristics establish the initial state. If a goal is derived, the corresponding property is confirmed. The following logical rules existed in BAN logic are used in the proof:

Message-Meaning rule:

$$\frac{P| \equiv Q \overset{K}{\longleftrightarrow} P, P\{X\}_K}{P| \equiv Q| \sim X}$$

Nonce Verification rule:

$$\frac{P| \equiv \sharp(X), P| \equiv Q \mid\sim X}{P| \equiv Q| \equiv X}$$

Jurisdiction rule:

$$\frac{P| \equiv Q| \Rightarrow X, P| \equiv Q| \equiv X}{P| \equiv X}$$

See Conduction rule:

$$\frac{\frac{P(X,Y)}{PX} P| \equiv Q \overset{K}{\longleftrightarrow} P, \{X\}_K}{PX}$$

Freshness Conduction rule:

$$\frac{P| \equiv \sharp(X)}{P| \equiv \sharp(X, Y)}$$

Belief Operator rule:

$$\frac{P| \equiv X, P| \equiv Y}{P| \equiv (X, Y)}, \frac{P| \equiv (X, Y)}{P| \equiv X}, \frac{P| \equiv Q| \equiv (X, Y)}{P| \equiv Q| \equiv X}$$

II. Proof process and result

Formal Proof Goal. This formal analysis aims to demonstrate the security and effectiveness of SEHAP, showing it achieves both the switching function and privacy protection during handover. To this end, we design four proof goals, presented as BAN logic definitions.

Goal1: $UE \mid\equiv UE \overset{K_{gNBt}}{\longleftrightarrow} Sat_{TRAN}$

Goal2: $Sat_{TRAN} \mid\equiv UE \overset{K_{gNBt}}{\longleftrightarrow} Sat_{TRAN}$

Goal3: $UE \mid\equiv Sat_{TRAN} \mid\equiv UE \overset{K_{gNBt}}{\longleftrightarrow} Sat_{TRAN}$

Goal4: $Sat_{TRAN} \mid\equiv UE \mid\equiv UE \overset{K_{gNBt}}{\longleftrightarrow} Sat_{TRAN}$

Idealization Model. An essential step in the formal analysis is the idealization of the protocol. This standardized description allows BAN logic to recognize the protocol, forming the basis for goal derivation. BAN logic simplifies the process by focusing on variable transmission between entities and ignoring internal parameter conversion. The modeling results of SEHAP are as follows:

Message 1. $Sat_{SRAN} \rightarrow AMF$: m_1 is formalized as

$$AMF \lhd \{GUTIs, \textit{HandoverRequest}\}_{K_S}$$

Message 2. $AMF \rightarrow Sat_{TRAN}$: m_2 is formalized as

$$Sat_{TRAN} \lhd \{Sat_{TRAN}, NCC, K_{gNB}\}_{K_T}$$

Message 3. $Sat_{TRAN} \rightarrow UE_i$: m_3 is formalized as

$$UE_i \lhd \{GUTI_i, R_T\}_{K_{gNB}}$$

Message 4. $UE_i \rightarrow Sat_{TRAN}$: m_4 is formalized as

$$Sat_{TRAN} \lhd \{R_T\}_{K_{gNB}}$$

Message 5. $Sat_{TRAN} \rightarrow AMF$: m_5 is formalized as

$$AMF \lhd \{K_{gNBt}, result\}_{K_T}$$

Formal Assumption. According to the protocol description, the following security assumptions are made for our proposed scheme before the execution of the protocol.

A1: $UE_i \mid\equiv K_{gNB}$
A2: $UE_i \mid\equiv GUTI$
A3: $UE_i \mid\equiv NCC$
A4: $Sat_{TRAN} \mid\equiv Sat_{TRAN} \overset{K_T}{\longleftrightarrow} AMF$
A5: $Sat_{TRAN} \mid\equiv \sharp(GUTIs, NCC, K_{gNB})$
A6: $Sat_{TRAN} \mid\equiv R_T$
A7: $AMF \mid\equiv Sat_{TRAN} \overset{K_T}{\longleftrightarrow} AMF$
A10: $AMF \mid\equiv NCC$
A11: $AMF \mid\equiv K_{gNB}$
A12: $AMF \mid\equiv Sat_{TRAN}| \implies GUTIs$

Derivation Proof. After completing the steps of goal formulation, idealized modeling, and state assumption, we proceed with the formal proof of the protocol. This involves the comprehensive use of BAN logic, and the specific derivation process is detailed below.

First, from the Message 2 via the message-meaning rule and the assumption A4, we obtain:

$$Sat_{TRAN}| \equiv AMF| \sim (GUTIs, NCC, K_{gNB}).$$

According to A5, the nonce-verication rule is applied to get:

$$Sat_{TRAN}| \equiv AMF| \equiv (GUTIs, NCC, K_{gNB}). \quad (1)$$

Combine Message1 and the assumption A7-A9, apply the see conduction rule, the message-meaning rule and the nonce-verication rule to obtain:

$$AMF| \equiv UE| \equiv GUTI.$$

Given the assumption A10-A12, we use the jurisdiction rule and the belief operator rule to get the equation:

$$AMF| \equiv (GUTIs, NCC, K_{gNB}).$$

According to the fact that $(GUTIs, NCC, K_{gNB})$ is generated in AMF and sent to Sat_{TRAN}. Using the above formula, we can get :

$$Sat_{TRAN} \mid\equiv AMF| \implies (GUTIs, NCC, K_{gNB}).$$

Due to Equation (1), we can apply the jurisdiction rule to the above equation to obtain:

$$Sat_{TRAN} \mid\equiv (GUTIs, NCC, K_{gNB}). \tag{2}$$

Next, since K_{gNBt} is derived from K_{gNB}, combine the belief operator rule twice to get:

$$Sat_{TRAN} \mid\equiv K_{gNBt}.$$

Therefore, we have proved Goal1

$$UE_i \mid\equiv UE_i \overset{K_{gNBt}}{\longleftrightarrow} Sat_{TRAN}.$$

Second, according to the assumption A1-A2, we directly apply the belief operator rule to have

$$UE_i \mid\equiv K_{gNBt}.$$

Then, we get the Goal2

$$Sat_{TRAN} \mid\equiv UE_i \overset{K_{gNBt}}{\longleftrightarrow} Sat_{TRAN}$$

Third, combining the assumption A11 and Equation

$$Sat_{TRAN} \mid\equiv K_{gNB},$$

we can obtain

$$UE_i \overset{K_{gNB}}{\longleftrightarrow} Sat_{TRAN}.$$

Further, there is

$$UE_i \mid\equiv UE_i \overset{K_{gNB}}{\longleftrightarrow} Sat_{TRAN}.$$

From the Message3 via the message-meaning rule, we obtain

$$UE_i| \equiv Sat_{TRAN}| \sim (R_T, GUTI_i).$$

Sat_{TRAN} have sent the random number R_T for the first time, then

$$UE_i \mid\equiv \sharp(R_T).$$

Using the freshness conduction rule, we get

$$UE \mid\equiv \sharp(R_T, GUTI_i).$$

Combing above Equation, we have

$$UE| \equiv Sat_{TRAN}| \equiv (R_T, GUTI_i).$$

From the Equation(2), we apply the belief operator rule and the assumption A6,A13 to get

$$Sat_{TRAN} \mid\equiv (R_T, GUTI_i).$$

$(R_T, GUTI_i)$ is generated by Sat_{TRAN} and sent to the UE_i , we have

$$UE_i \mid\equiv Sat_{TRAN}| \implies (R_T, GUTI_i).$$

Applying the jurisdiction rule to obtain

$$UE_i \mid\equiv (R_T, GUTI_i).$$

According to the belief operator rule, from A2-A3, we can get

$$UE_i \mid\equiv R_T$$

and

$$UE \mid\equiv R_T + NCC.$$

We can conclude that the verification on the UE side is successful. Thus there is

$$UE \mid\equiv Sat_{TRAN}| \equiv K_{gNBt}.$$

Finally, the Goal3

$$UE_i \mid\equiv Sat_{TRAN} \mid\equiv UE_i \overset{K_{gNBt}}{\longleftrightarrow} Sat_{TRAN}$$

is verified.

Then, we present the proof for the last Goal4. According to the see conduction rule, we get the following formula from Message4:

$$UE_i \lhd R_T + NCC.$$

Since R_T is a random number and is sent from Sat_{TRAN} to UE_i for the first time and according to the freshness conduction rule that has

$$UE_i \mid\equiv \sharp(R_T + NCC),$$

that is

$$UE_i \mid\equiv \sharp(R_T + NCC).$$

Combined with Message5, we apply the See conduction rule to obtain

$$Sat_{TRAN}| \equiv UE_i| \sim R_T.$$

Since R_T is processed in UE_i and sent to Sat_{TRAN}. We can infer

$$Sat_{TRAN} \mid\equiv UE_i| \implies R_T.$$

Then, using the jurisdiction rule to obtain

$$Sat_{TRAN} \mid\equiv R_T.$$

Finally, we can determine that the check on the Sat_{TRAN} side is successful. Therefore, there is

$$Sat_{TRAN} \mid\equiv UE_i \mid\equiv R_T.$$

Goal4 is proven to hold

$$Sat_{TRAN} \mid\equiv UE_i \mid\equiv UE_i \overset{K_{gNBt}}{\longleftrightarrow} Sat_{TRAN}.$$

So far, we have completed the formal analysis of SEHAP, and all the goals have been proved. We can conclude that the SEHAP protocol not only enables the next-hop session key K_{gNBt} to be shared between the UE and Sat_{TRAN} but also keeps related variables synchronized, which provides a handover function and ensures security.