# Attachment: Security Analysis using AVISPA and BAN-logic Tool

Xiongpeng Ren

In this attachment, we adopt the AVISPA tool and Burrows-Abadi-Needham (BAN)-logic to evaluate all proposed schemes in the UAV-aided satellite-terrestrial Integration Network (including **Phase1_UAV**, **Phase2_Ter** and **Phase3_HO**) and present the security analysis and results of these protocols. The results show that our schemes are secure.

## I. Security Analysis using AVISPA

In order to facilitate the understanding, we take the protocol **Phase1_UAV** as an example. At first, we specify the scheme in High Level Protocols Specification Language (HLPSL). As the satellite is transparent, we set two basic roles (i.e., *ncc*, *uav*) representing the NCC, UAV. In the implementing process, the pre-shared parameters (i.e., *S*, *U*, *R*, *Hash*, *C*, *PID*), local variables (i.e., *Nu*, *Nn*, *PIDnew*, *Rnew*, *SK*, *MAC1*, *MAC2*, *Cnew*) and the transitions between two basic roles are in accordance with the corresponding protocols. The necessary roles (i.e., *session*, *environment*, *goal*) are also specified. The role session composes of two instances of two roles. The role *environment* composes of the knowledge of the intruder, some sessions to be run in parallel, and some constants which initialize the knowledge and sessions. Referring to the security goal, we use six predicates *secret* to declare the confidentiality and agreement of *PIDnew*, *Rnew*, *SK* between two basic roles. We use four predicates *witness* and *request* to declare the authentication between two basic roles. The specification of the protocol was uploaded to GitHub [1]. We installed Security Protocol ANimator (SPAN) on virtual machine to run AVISPA and to verify the specification. The analysis results using different automatic analysis techniques (i.e., OFMC and CL-AtSe back-ends) are shown in Fig. 1. It can be seen that the scheme is safe and satisfies above security properties.

Similarly, referring to other two protocols, the specifications also can be found in [1], we ignore the details here and present the analysis results directly in Fig. 2 and Fig. 3. It can be seen that two schemes are also safe.

## II. Security Analysis using BAN-logic

At first, we present the preliminary of the BAN-logic in Tables I and II, respectively. We also present the goals of our protocols and the assumptions on the initial state. Then, we model the protocols using the BAN-logic language. Finally, we prove that these schemes achieve various goals. It is noted that we ignore the satellite role as the it is transparent for other entities during the analysis process.

TABLE I
BAN-Logic Notations

| Notation | Definition |
|---|---|
| $P\mid\equiv X$ | The entity P believes the formula X. |
| $P \triangleleft X$ | P sees X. |
| $P\mid\Rightarrow X$ | P has complete jurisdiction over X. |
| $P\mid\sim X$ | P has said X. |
| $\sharp(X)$ | X is fresh. |
| $< X >_K$ | X is integrated with shared secret K. |
| $P \xleftrightarrow{K} Q$ | The entities P and Q share a secret key K. |

TABLE II
BAN-Logic Rules

| Symbol | Name of the rule |
|---|---|
| $\frac{P\mid\equiv\sharp(X)}{P\mid\equiv\sharp(X,Y)}$ | The fresh-promotion rule. |
| $\frac{P\mid\equiv\sharp(X),P\mid\equiv Q\mid\sim X}{P\mid\equiv Q\mid\equiv X}$ | The nonce-verification rule. |
| $\frac{P\mid\equiv Q\mid\equiv(X,Y)}{P\mid\equiv Q\mid\equiv X},\frac{P\mid\equiv(X,Y)}{P\mid\equiv X}$ | The decomposition rule. |
| $\frac{P\mid\equiv X,P\mid\equiv Y}{P\mid\equiv(X,Y)}$ | The composition rule. |
| $\frac{P\mid\equiv Q\mid\Rightarrow X,P\mid\equiv Q\mid\equiv X}{P\mid\equiv X}$ | The jurisdiction rule. |
| $\frac{P\mid\equiv P\xleftrightarrow{K}Q,P\triangleleft< X >_K}{P\mid\equiv Q\mid\sim X}$ | The message-meaning rule. |
| $\frac{P\triangleleft(X,Y)}{P\triangleleft X},\frac{P\triangleleft< X >_Y}{P\triangleleft X}$ | The seeing rule. |

### A. Analysis for **Phase1_UAV**

(a) The goal of **Phase1_UAV**

The goal of the protocol is that each entity not only believes it shares the session key with the other one, but also has to believe that the other entity also believes the key. In the BAN-logic, the goals can be described as:

Goal1:$UAV\mid\equiv UAV\xleftrightarrow{SK}NCC$

Goal2:$NCC\mid\equiv NCC\xleftrightarrow{SK}UAV$

Goal3:$UAV\mid\equiv NCC\mid\equiv UAV\xleftrightarrow{SK}NCC$

Goal4:$NCC\mid\equiv UAV\mid\equiv NCC\xleftrightarrow{SK}UAV$

(b) Assumptions

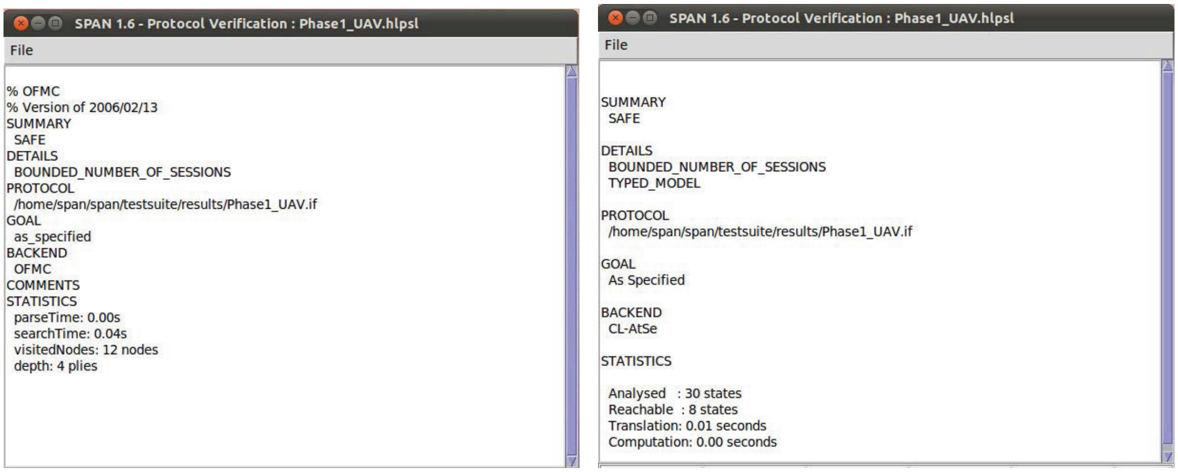
Assumption1: $NCC\mid\equiv UAV\mid\Rightarrow(N_U)$.

Assumption2: $UAV\mid\equiv NCC\mid\Rightarrow(N_N)$.

(c) Specification of the protocol

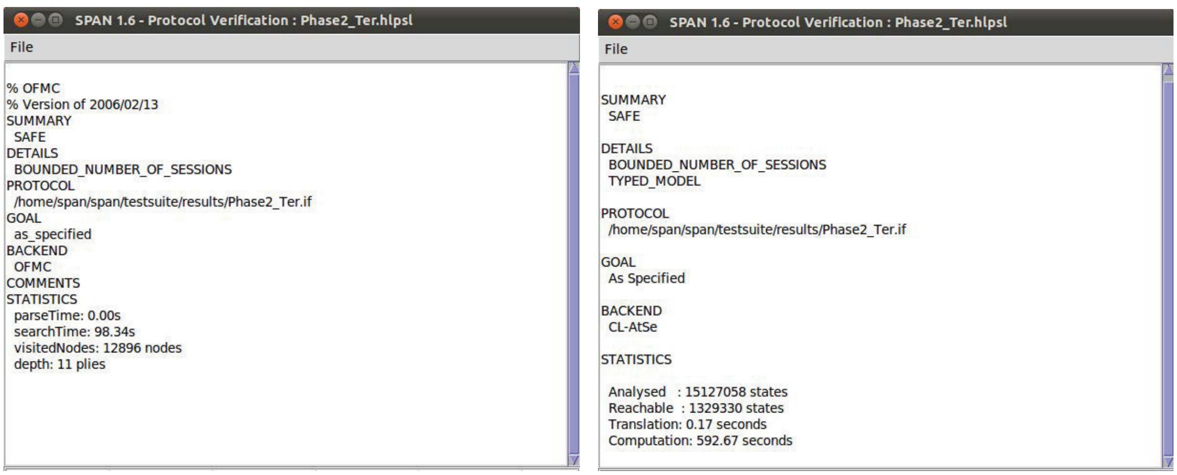
Message1: NCC $\triangleleft\ (N_U, PID_U)$.

Message2: UAV $\triangleleft\ (PID_U^*, N_N, AUTH_{N-U})$, where $AUTH_{N-U}$ can be seen as $< PID_U, ID_U, N_U, N_N, PID_U^*,$




(a) $using\ OFMC$ (b) $using\ CL-AtSe$

Fig. 1. Security verification results of **Phase1_UAV** using OFMC and CL-AtSe back-ends in AVISPA




(a) $using\ OFMC$ (b) $using\ CL-AtSe$

Fig. 2. Security verification results of **Phase2_Ter** using OFMC and CL-AtSe back-ends in AVISPA

$C_U >_R$, $R$ is the pre-shared PUF response between the UAV and the NCC.

Message3: NCC $\triangleleft$ $(R_U^*, AUTH_{U-N})$, where $AUTH_{U-N}$ can be seen as $< PID_U^{new}$, $C_U^{new}$, $R_U^{new}$, $ID_U$, $N_U$, $N_N$, $C_U >_R$.

(d) Inference procedure

According to the Message3 and the seeing rule, the NCC also believes that it shared secret $R$ with the UAV, we have

Step1: NCC $\triangleleft$ $AUTH_{U-N}$.

According to the message-meaning rule and step1, we have

Step2: NCC $|\equiv$ $UAV$ $|\sim$ $(PID_U^{new}$, $C_U^{new}$, $R_U^{new}$, $ID_U$, $N_U$, $N_N$, $C_U)$.

As the $N_N$ is generated by the NCC, we have

Step3: NCC $|\equiv \sharp N_N$.

According to the fresh-promotion rule and step3, we can have

Step4: NCC $|\equiv \sharp(PID_U^{new}$, $C_U^{new}$, $R_U^{new}$, $ID_U$, $N_U$, $N_N$, $C_U)$.

According to the nonce-verification rule and step2, step4, we can have

Step5: NCC $|\equiv$ $UAV$ $|\equiv$ $(PID_U^{new}$, $C_U^{new}$, $R_U^{new}$, $ID_U$, $N_U$, $N_N$, $C_U)$.

According to the decomposition rule and step5, we have

Step6: NCC $|\equiv UAV$ $|\equiv N_U$.

According to the jurisdiction rule, step6 and assumption1, we have

Step7: NCC $|\equiv NCC \xleftrightarrow{N_U} UAV$.

As the $N_N$ is generated by the NCC and $C_U, R$ is pre-shared each other, we have

Step8: NCC $|\equiv$ $NCC \xleftrightarrow{N_N} UAV$, NCC $|\equiv$ $NCC \xleftrightarrow{C_U} UAV$, NCC $|\equiv NCC \xleftrightarrow{R} UAV$.

According to the composition rule and step7, step8, as $SK = H(N_U, N_N, C_U, R)$, we have

Step9: NCC$|\equiv$ NCC$\xleftrightarrow{SK}$ UAV. **(Goal2 is achieved)**

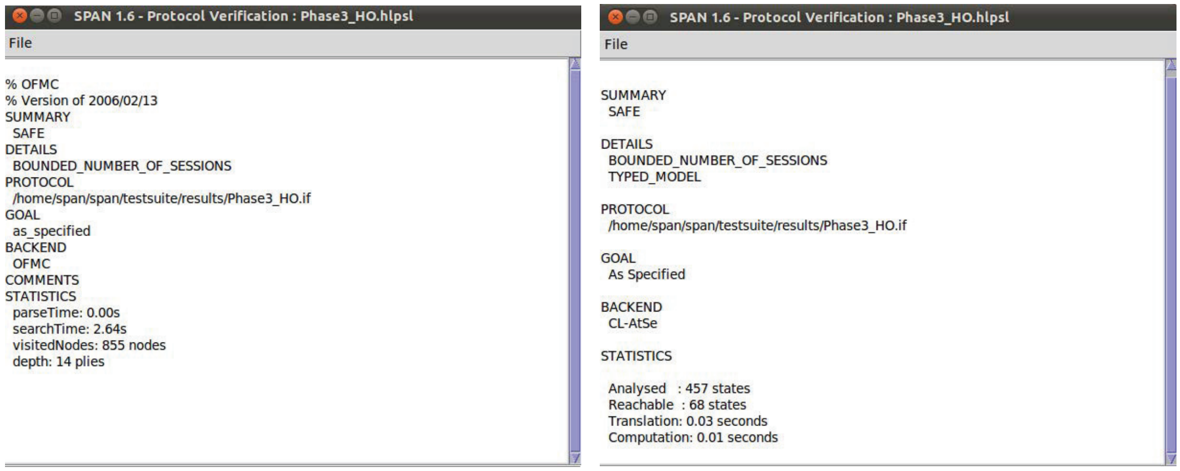
According to the message2, we have

Step10: UAV $\triangleleft$ $AUTH_{N-U}$.

According to the message-meaning rule and step10, we have

Step11: UAV $|\equiv NCC$ $|\sim (PID_U, ID_U, N_U, N_N, PID_U^*$, $C_U)$.

As the $N_U$ is generated by the UAV, we have




(a) $using\ OFMC$ (b) $using\ CL-AtSe$

Fig. 3. Security verification results of **Phase3_HO** using OFMC and CL-AtSe back-ends in AVISPA

Step12: UAV $|\equiv \sharp N_U$.

According to the fresh-promotion rule and step12, we can have

Step13: UAV $|\equiv \sharp(PID_U, ID_U, N_U, N_N, PID_U^*, C_U)$.

According to the nonce-verification rule and step11, step13, we can have

Step14: UAV $|\equiv NCC |\equiv (PID_U, ID_U, N_U, N_N, PID_U^*, C_U)$.

According to the decomposition rule and step14, we have

Step15: UAV $|\equiv NCC |\equiv N_N$.

According to the jurisdiction rule, step15 and assumption2, we have

Step16: UAV $|\equiv UAV \overset{N_N}{\longleftrightarrow} NCC$.

As the $N_U$ is generated by the UAV and $C_U, R$ is pre-shared each other, we have

Step17: UAV $|\equiv UAV \overset{N_U}{\longleftrightarrow} NCC$, UAV $|\equiv UAV \overset{C_U}{\longleftrightarrow} NCC$, UAV $|\equiv UAV \overset{R}{\longleftrightarrow} NCC$.

According to the composition rule and step16, step17, as $SK = H(N_U, N_N, C_U, R)$, we have

Step18: UAV$|\equiv$ UAV$\overset{SK}{\longleftrightarrow}$ NCC. **(Goal1 is achieved)**

As the NCC verified the $AUTH_{U-N}$ which is binded with $N_N$ successfully and according to the step3 and the fresh-promotion rule, we have

Step19: NCC $|\equiv UAV\ |\sim AUTH_{U-N}$, NCC $|\equiv \sharp AUTH_{U-N}$.

According to the message-meaning rule and step19, we have

Step20: NCC $|\equiv UAV |\equiv AUTH_{U-N}$.

As $AUTH_{U-N} = h(PID_U^{new}, C_U^{new}, R_U^*, SK)$, according to the decomposition rule and step20, we have

Step21: NCC $|\equiv UAV |\equiv NCC \overset{SK}{\longleftrightarrow} UAV$. **(Goal4 is achieved)**

As the UAV verified the $AUTH_{N-U}$ which is binded with $N_U$ successfully and according to step12 and the fresh-promotion rule, we have

Step22: UAV $|\equiv NCC\ |\sim AUTH_{N-U}$, UAV $|\equiv \sharp AUTH_{N-U}$.

According to the message-meaning rule and step22, we have

Step23: UAV $|\equiv NCC |\equiv AUTH_{N-U}$.

As $AUTH_{N-U} = h(PID_U, ID_U, N_U, N_N, PID_U^*, C_U, SK)$, according to the decomposition rule and step23, we have

Step24: UAV $|\equiv NCC |\equiv UAV \overset{SK}{\longleftrightarrow} NCC$. **(Goal3 is achieved)**

In summary, four goals are achieved.

### B. *Analysis for* ***Phase2_Ter***

(a) The goal of **Phase2_Ter**

The goal of the protocol is that each entity not only believes it shares the session key with the other one, but also has to believe that the other entity also believes the key. In the BAN-logic, the goals can be described as:

Goal1:$Ter |\equiv Ter \overset{SK1}{\longleftrightarrow} NCC$

Goal2:$NCC |\equiv NCC \overset{SK1}{\longleftrightarrow} Ter$

Goal3:$Ter |\equiv NCC |\equiv NCC \overset{SK1}{\longleftrightarrow} Ter$

Goal4:$NCC |\equiv Ter |\equiv Ter \overset{SK1}{\longleftrightarrow} NCC$

Goal5:$Ter |\equiv Ter \overset{SK2}{\longleftrightarrow} UAV$

Goal6:$UAV |\equiv UAV \overset{SK2}{\longleftrightarrow} Ter$

Goal7:$Ter |\equiv UAV |\equiv UAV \overset{SK2}{\longleftrightarrow} Ter$

Goal8:$UAV |\equiv Ter |\equiv Ter \overset{SK2}{\longleftrightarrow} UAV$

(b) Assumptions

Assumption1: $NCC |\equiv Ter |\Rightarrow (N_T)$.

Assumption2: $Ter |\equiv NCC |\Rightarrow (N_N, ID_U)$.

Assumption3: $Ter |\equiv UAV |\Rightarrow (N_U)$.

(c) Specification of the protocol

Message1: UAV $\triangleleft (N_T, PID_T)$.

Message2: NCC $\triangleleft (N^T, PID_T, N_U)$.

Message3: UAV $\triangleleft (PID_T^*, N_N, AUTH_{N-T}, SK2)$, where $AUTH_{N-T}$ can be seen as $< PID_T, ID_T, ID_U, N_T\ N_U, N_N, PID_T^*, C_T >_R$, where $R$ is the pre-shared PUF response between the Ter and the NCC.

Message4: Ter $\triangleleft (PID_T^*, N_N, N_U, CID_U, AUTH_{N-T})$.

Message5: UAV $\triangleleft (R_T^*, AUTH_{T-N}, AUTH_{T-U})$, where $AUTH_{T-N}$ can be seen as $< PID_T^{new}, N_T, N_N, C_T^{new}, >_R$, $AUTH_{T-U}$ can be seen as $< R_T^*, AUTH_{T-N}, ID_U, N_U, N_T, N_N, C_T >_R$.

Message6: NCC $\triangleleft (R_T^*, AUTH_{T-N})$.

(d) Inference procedure

According to the Message6 and the seeing rule, the NCC also believes that it shared secret $R$ with the Ter, we have

Step1: NCC $\triangleleft$ $AUTH_{T-N}$.

According to the message-meaning rule and step1, we have

Step2: NCC $|\equiv Ter\ |\sim (PID_T^{new},\ N_T,\ N_N,\ C_T^{new})$.

As the $N_N$ is generated by the NCC, we have

Step3: NCC $|\equiv \sharp N_N$.

According to the fresh-promotion rule and step3, we can have

Step4: NCC $|\equiv \sharp(PID_T^{new},\ N_T,\ N_N,\ C_T^{new})$.

According to the nonce-verification rule and step2, step4, we can have

Step5: NCC $|\equiv Ter\ |\equiv (PID_T^{new},\ N_T,\ N_N,\ C_T^{new})$.

According to the decomposition rule and step5, we have

Step6: NCC $|\equiv Ter\ |\equiv N_T$.

According to the jurisdiction rule, step6 and assumption1, we have

Step7: NCC $|\equiv NCC \xleftrightarrow{N_T} Ter$.

As the $N_N$ is generated by the NCC and $C_T, R$ is pre-shared each other, we have

Step8: NCC $|\equiv NCC \xleftrightarrow{N_N} Ter$, NCC $|\equiv NCC \xleftrightarrow{C_T} Ter$, NCC $|\equiv NCC \xleftrightarrow{R} Ter$.

According to the composition rule and step7, step8, as $SK1 = H(N_T,\ N_N,\ C_T,\ R)$, we have

Step9: NCC$|\equiv$ NCC$\xleftrightarrow{SK1}$ Ter. **(Goal2 is achieved)**

According to the message4, we have

Step10: Ter $\triangleleft$ $AUTH_{N-T}$.

According to the message-meaning rule and step10, we have

Step11: Ter $|\equiv NCC\ |\sim (PID_T,\ ID_T,\ ID_U,\ N_T\ N_U,\ N_N,\ PID_T^*,\ C_T)$.

As the $N_T$ is generated by the Ter, we have

Step12: Ter $|\equiv \sharp N_T$.

According to the fresh-promotion rule and step12, we can have

Step13: Ter $|\equiv \sharp(PID_T, ID_T, ID_U, N_T\ N_U, N_N, PID_T^*, C_T)$.

According to the nonce-verification rule and step11, step13, we can have

Step14: Ter $|\equiv NCC\ |\equiv (PID_T,\ ID_T,\ ID_U,\ N_T\ N_U,\ N_N,\ PID_T^*,\ C_T)$.

According to the decomposition rule and step14, we have

Step15: Ter $|\equiv NCC\ |\equiv N_N$. Ter $|\equiv NCC\ |\equiv ID_U$. Ter $|\equiv NCC\ |\equiv N_U$.

As the NCC trusts with the UAC, then Ter $|\equiv UAV\ |\equiv N_U$. According to the jurisdiction rule, step15 and assumption2, we have

Step16: Ter $|\equiv Ter \xleftrightarrow{N_N} NCC$. Ter $|\equiv Ter \xleftrightarrow{ID_U} NCC$. Ter $|\equiv Ter \xleftrightarrow{N_U} NCC$.

As the $N_T$ is generated by the Ter and $C_T, R$ is pre-shared each other, we have

Step17: Ter $|\equiv Ter \xleftrightarrow{N_T} NCC$, Ter $|\equiv Ter \xleftrightarrow{C_T} NCC$, Ter $|\equiv Ter \xleftrightarrow{R} NCC$.

According to the composition rule and step16, step17, as $SK1 = H(N_T,\ N_N,\ C_T,\ R)$, we have

Step18: Ter$|\equiv$ Ter$\xleftrightarrow{SK1}$ NCC. **(Goal1 is achieved)**

As the NCC verified the $AUTH_{T-N}$ which is binded with $N_N$ successfully and according to step3 the fresh-promotion rule, we have

Step19: NCC $|\equiv\ Ter\ \ |\sim\ AUTH_{T-N}$, NCC $|\equiv \sharp AUTH_{T-N}$.

According to the message-meaning rule and step19, we have

Step20: NCC $|\equiv Ter\ |\equiv AUTH_{T-N}$.

As $AUTH_{T-N} = h(PID_T^{new},\ N_T,\ N_N,\ C_T^{new},\ R_T^*,\ SK1)$, according to the decomposition rule and step20, we have

Step21: NCC $|\equiv\ Ter\ |\equiv\ Ter \xleftrightarrow{SK1} NCC$. **(Goal4 is achieved)**

As the Ter verified the $AUTH_{N-T}$ which is binded with $N_T$ successfully and according to the step12 and the fresh-promotion rule, we have

Step22: Ter $|\equiv\ NCC\ \ |\sim\ AUTH_{N-T}$, Ter $|\equiv \sharp AUTH_{N-T}$.

According to the message-meaning rule and step22, we have

Step23: Ter $|\equiv NCC\ |\equiv AUTH_{N-T}$.

As $AUTH_{N-T} = h(PID_T,\ ID_T,\ ID_U,\ N_T,\ N_U,\ N_N,\ PID_T^*,\ C_T,\ SK1)$, according to the decomposition rule and step23, we have

Step24: Ter $|\equiv\ NCC\ |\equiv\ Ter \xleftrightarrow{SK1} NCC$. **(Goal3 is achieved)**

According to the step17, step18 and the composition rule, as $SK2 = H(N_T,\ N_U,\ SK1)$, we have

Step25: Ter$|\equiv$ Ter$\xleftrightarrow{SK2}$ NCC.

According to the step17 and the protocol procedures, we can have that the Ter believes that it is interacting with the UAV and the following result:

Step26: Ter$|\equiv$ Ter$\xleftrightarrow{SK2}$ UAV. **(Goal5 is achieved)**

According to the protocol procedures and the step24, we have

Step27: Ter$|\equiv$ Ter$|\equiv\xleftrightarrow{SK2}$ UAV. **(Goal7 is achieved)**

As the NCC has authenticated with the Ter in advcance, and according to the step9 and the message3 in which the NCC will send $SK2$ to the UAV, we have

Step28: UAV$|\equiv$ UAV$\xleftrightarrow{SK2}$ Ter. **(Goal6 is achieved)**

Step29: As the UAV verified the $AUTH_{T-U}$ which is binded with $N_U$ successfully, the UAV believes $N_U$ is fresh and according to step3 the fresh-promotion rule, we have

Step30: UAV $|\equiv\ Ter\ \ |\sim\ AUTH_{T-U}$, UAV $|\equiv \sharp AUTH_{T-U}$.

According to the message-meaning rule and step30, we have

Step31: UAV $|\equiv Ter\ |\equiv AUTH_{T-U}$.

As $AUTH_{T-U} = h(N_T,\ N_U,\ SK2)$, according to the decomposition rule and step31, we have

Step32: UAV $|\equiv\ Ter\ |\equiv\ Ter \xleftrightarrow{SK2} UAV$. **(Goal8 is achieved)**

In summary, eight goals are achieved.

### *C. Analysis for* ***Phase3_HO***

(a) The goal of **Phase3_HO**

The goal of the protocol is that each entity not only believes it shares the session key with the other one, but also has to believe that the other entity also believes the key. In the BAN-logic, the goals can be described as:

Goal1:$Ter \mid\equiv Ter \overset{SK1}{\longleftrightarrow} UAV$

Goal2:$UAV \mid\equiv UAV \overset{SK1}{\longleftrightarrow} Ter$

Goal3:$Ter \mid\equiv UAV \mid\equiv UAV \overset{SK1}{\longleftrightarrow} Ter$

Goal4:$UAV \mid\equiv Ter \mid\equiv Ter \overset{SK1}{\longleftrightarrow} UAV$

(b) Assumptions

Assumption1: $UAV \mid\equiv Ter \mid\Rightarrow (N_T)$.

Assumption2: $Ter \mid\equiv UAV \mid\Rightarrow (N_U)$.

Assumption3: $Ter \mid\equiv NCC \mid\Rightarrow (ID_U)$.

(c) Specification of the protocol

Message1: UAV $\triangleleft$ $(PID_T)$.

Message2: NCC $\triangleleft$ $(PID_T, N_U)$.

Message3: UAV $\triangleleft$ $(CID_{nU},\ PID_T^*,\ SK)$.

Message4: Ter $\triangleleft$ $(N_U,\ CID_U,\ PID_T^*,\ AUTH_{nU-T})$, where $AUTH_{nU-T}$ can be seen as $< PID_T,\ ID_nU,\ N_U,\ PID_T^* >_R$, where $R$ is the pre-shared secret between the Ter and the NCC.

Message5: UAV $\triangleleft$ $(N_T,\ AUTH_{T-nU})$, where $AUTH_{T-nU}$ can be seen as $< ID_nU,\ N_T,\ N_U,\ PID_T^*, >_R$.

(d) Inference procedure

As the NCC has authenticated with the Ter in advcance, and according to the message3 in which the NCC will send $SK$ to the UAV, we have

Step1: UAV$\mid\equiv$ UAV$\overset{SK}{\longleftrightarrow}$ Ter. **(Goal2 is achieved)**

According to the Message4 and the seeing rule, the Ter also believes that it shared secret $R$ with the NCC, we have

Step2: Ter $\triangleleft$ $AUTH_{nU-T}$.

According to the message-meaning rule and step2, we have

Step3: Ter $\mid\equiv NCC \mid\sim (PID_T,\ ID_nU,\ N_U,\ PID_T^*)$.

As the $PID_T$ is generated by the Ter and is updated after each run, we have

Step4: Ter $\mid\equiv \sharp PID_T$.

According to the fresh-promotion rule and step4, we can have

Step5: Ter $\mid\equiv \sharp(PID_T,\ ID_nU,\ N_U,\ PID_T^*)$.

According to the nonce-verification rule and step3, step5, we can have

Step6: Ter $\mid\equiv NCC \mid\equiv (PID_T,\ ID_{nU},\ N_U,\ PID_T^*)$.

According to the decomposition rule and step6, we have

Step7: Ter $\mid\equiv NCC \mid\equiv N_U$. Ter $\mid\equiv NCC \mid\equiv ID_{nU}$.

As the NCC has authenticated with the UAV and they trust each other, according to the step7, we have

Step8: Ter $\mid\equiv UAV \mid\equiv N_U$.

According to the jurisdiction rule, step7, step8, assumption2 and assumption3, we have

Step9: Ter $\mid\equiv Ter \overset{ID_{nU}}{\longleftrightarrow} NCC$. Ter $\mid\equiv Ter \overset{N_U}{\longleftrightarrow} UAV$.

As the NCC has authenticated with the UAV and they trust each other, according to the step9, we have

Step10: Ter $\mid\equiv Ter \overset{N_U}{\longleftrightarrow} NCC$.

According to the step9, step10 and $R$ is pre-shared each other, as $SK = H(ID_{nU},\ N_U,\ R)$ we have

Step11: Ter $\mid\equiv Ter \overset{SK}{\longleftrightarrow} NCC$.

According to the step9 and the protocol procedures, we can have that the Ter believes that it is interacting with the UAV and the following result:

Step12: Ter$\mid\equiv$ Ter$\overset{SK}{\longleftrightarrow}$ UAV. **(Goal1 is achieved)**

As the Ter verified the $AUTH_{nU-T}$ which is binded with $PID_T$ successfully and according to the step4 and the fresh-promotion rule, we have

Step13: Ter $\mid\equiv$ $UAV$ $\mid\sim$ $AUTH_{nU-T}$, Ter $\mid\equiv$ $\sharp AUTH_{nU-T}$.

According to the message-meaning rule and step13, we have

Step14: Ter $\mid\equiv UAV \mid\equiv AUTH_{nU-T}$.

As $AUTH_{nU-T} = h(PID_T,\ ID_{nU},\ N_U,\ PID_T^*,\ SK)$, according to the decomposition rule and step14, we have

Step15: Ter $\mid\equiv$ $UAV$ $\mid\equiv$ $Ter \overset{SK}{\longleftrightarrow} UAV$. **(Goal3 is achieved)**

As the UAV verified the $AUTH_{T-nU}$ which is binded with $N_U$ successfully and the UAV believed $N_U$ is fresh, and the fresh-promotion rule, we have

Step16: UAV $\mid\equiv$ $Ter$ $\mid\sim$ $AUTH_{T-nU}$, UAV $\mid\equiv$ $\sharp AUTH_{T-nU}$.

According to the message-meaning rule and step16, we have

Step17: UAV $\mid\equiv Ter \mid\equiv AUTH_{T-nU}$.

As $AUTH_{T-nU} = h(ID_{nU},\ N_T,\ N_U,\ PID_T^*,\ SK)$, according to the decomposition rule and step17, we have

Step18: UAV $\mid\equiv$ $Ter$ $\mid\equiv$ $UAV \overset{SK}{\longleftrightarrow} Ter$. **(Goal4 is achieved)**

In summary, four goals are achieved.

## REFERENCES

[1] NAHAS_SecurityAnalysis. [Online]. Available: https://github.com/xiongpengren/NAHAS_SecurityAnalysis.