

Source: Siemens AG**Title:** Formal Analysis of the 3G Authentication Protocol with
Modified Sequence Number Management*

Contents

1	Introduction	2
2	The TLA Notation	2
3	Notation	3
3.1	Domains, Constants and Functions	4
3.2	The variables of the system	6
3.3	The Messages: the Transitions of the System	7
4	Transitions of the normal System	10
4.1	Changing the Location	10
4.2	The Serving Network	11
4.3	The Home Environment	12
4.4	The Communication Channel	14
4.5	The Mobile Station	15
5	Definition of Normal Behavior	16
6	Transitions of the incorrect System	18
6.1	Events: more Transitions	18
6.2	Changing the Location	21
6.3	The Serving Network	22
6.4	The Home Environment	22
6.5	The Communication Channel	23
6.6	The Mobile Station	25
7	Definition of Incorrect Behavior	25
8	Theorems	28

*This document is based on work carried out in the EU-sponsored collaborative research project AC336 USECA. Nevertheless, only the author is responsible for the views expressed here.

1 Introduction

TLA is a specification language for the compositional specification and verification of distributed programs. The complete protocol was specified in TLA [1], a formal language used mainly for writing specifications of concurrent systems and proving properties of the system. TLA is a state based, first-order temporal logic. The main part of a specification of a system is typically given by a set of events or transitions, each one being a first-order logic predicate that describes the relation between the variables in one state and the next. The specification is completed by expressing the conditions under which the system should start (initial condition) and how a part of the system will eventually respond or act, the so called fairness properties.

The goal of this paper is to give a formal description of the specification of the protocol, of the assumptions, failure models, properties of the system or parts of the system, scenarios and theorems in TLA.

The first theorem presented has the following form: if some conditions on the observable behavior hold during a certain period of time, then at the end of that interval some condition on the internal state of the system holds. We call those conditions on observable behavior *scenarios* (examples: loss of messages, crashes, etc.) and the conditions on the internal state of the system (example: synchronicity of counters) we simply call *(internal) conditions of the system*. Therefore, the first theorem may be expressed as follows: if a certain scenario holds, then a certain condition of the system is true. Other theorems have the following form: if a certain condition of the system is not true at certain time but from that time on a "good" scenario holds, the missing condition will become true again.

2 The TLA Notation

The simplest use of TLA is to describe a system as a set of initial conditions, Init , together with an "evolution" equation, \mathcal{S} . This resembles the way a physicist models a continuous system by initial conditions and a differential equation. A state of the system is any set of values (valuation) for some variables $\{x_1, x_2, \dots, x_n\}$. Let us call x the tuple $x = (x_1, x_2, \dots, x_n)$. The formula $\text{Init} = \text{Init}(x)$ is a (first order or higher order) formula of predicate logic on x_1, x_2, \dots, x_n , stating the conditions in which the system starts. The formula \mathcal{S} relates two states. Using "primed" versions of the variables x_i , (that is, using fresh variables x'_i of the same type as x_i), $\mathcal{S} = \mathcal{S}(x, x')$ is a formula on the set $\{x_1, x_2, \dots, x_n, x'_1, x'_2, \dots, x'_n\}$.

In TLA this discrete dynamical system is written as:

$$\mathcal{A} : \Leftrightarrow \text{Init} \wedge \Box[\mathcal{S}]_x$$

The symbol \Box is read: "box" or "always". $[\mathcal{S}]_x$ is just an abbreviation of $\mathcal{S} \vee x' = x$. Using the convention $x \uparrow : \Leftrightarrow x' \neq x$, $[\mathcal{S}]_x$ is equivalent to $x \uparrow \Rightarrow \mathcal{S}$. We will write

$$\mathcal{A} : \Leftrightarrow \text{Init} \wedge \Box(x \uparrow \Rightarrow \mathcal{S})$$

A sequence $(\pi_1, \pi_2, \dots, \pi_n, \dots)$ of states satisfies \mathcal{A} if and only if π_1 satisfies Init , and each pair (π_i, π_{i+1}) satisfies \mathcal{S} or π_i is equal to π_{i+1} . (This is a so called "stutter step"). This is exactly the purpose of writing the subindex x in $[\mathcal{S}]_x$ (or the condition $x \uparrow$ in $(x \uparrow \Rightarrow \mathcal{S})$): allowing stuttering steps. This is quite reasonable: without introducing a global "clock", you may view the system as a set of modules each of which is governed by an equation of the form

$$\mathcal{A}_i : \Leftrightarrow \text{Init}(X_i) \wedge \Box(X_i \uparrow \Rightarrow \mathcal{S}(\tilde{X}_i, \tilde{X}'_i))$$

where X_i, \tilde{X}_i are subsets of $\{x_1, x_2, \dots, x_n\}$ (or subtuples of x). Then the whole system is given by the conjunction:

$$\mathcal{A} = \bigwedge_i \text{Init}(X_i) \wedge \bigwedge_i \Box(X_i \uparrow \Rightarrow \mathcal{S}(\tilde{X}_i, \tilde{X}'_i))$$

We will describe the different versions (scenarios) of the system by formulas \mathcal{A}_{normal} , $\mathcal{A}_{critical}$, \mathcal{A}_{incorr} of this type. More precisely, we will introduce transition relations, (\mathcal{N} with some indexes) of the form $\mathcal{N} : \Leftrightarrow (X_i \uparrow \Rightarrow \mathcal{S}(\tilde{X}_i, \tilde{X}'_i))$ to build up (using conjunction or all-quantification) the formulas \mathcal{A} .

Our modules do not (explicitely) share variables, but communicate via “actions” (events or messages). This may be modeled in TLA by introducing a variable for each message. The variable changes exactly when the message (or event) happens. Therefore if IN is an input message with parameter x then IN(x) happens exactly when a suitable variable $n_{\text{IN}}(x)$ changes:

$$\text{IN}(x) \Leftrightarrow n_{\text{IN}}(x) \uparrow$$

Typically, the next step relations \mathcal{N} that we will use are of the form¹:

$$\mathcal{N} : \Leftrightarrow \text{IN}(x) \wedge \text{cond} \Rightarrow \text{OUT}(g(x)) \wedge y' = f(x, y)$$

(if the input IN(x) happens and the conditions *cond* are true, the module produces the output OUT(y), with $y = g(x)$ and changes the local variable y according to formula f) or of the form:

$$\mathcal{N} : \Leftrightarrow \text{OUT}(y) \Rightarrow \text{IN} \quad \text{or :} \quad \mathcal{N} : \Leftrightarrow y \uparrow \Rightarrow \text{IN}$$

(if the output OUT(y) happens (or y changes), the only reason is that IN(x) has also happened. The “dummy” variable “ x ” or “ y ” in those formulas is not a variable of the system: the formula $\mathcal{N} : \Leftrightarrow \text{IN}(x) \wedge \text{cond} \Rightarrow \dots$ is equivalent to $\mathcal{N} : \Leftrightarrow \forall_x \text{IN}(x) \wedge \text{cond} \Rightarrow \dots$.

3 Notation

In this section we set our notation for the specification. First, we list the data types or, more properly, domains that will be used in the sequel. This also includes the introduction of constants and functions. Then we introduce the variables of the program that we are interested in. We conclude this section by introducing some notation for the “messages” and “events” of the program.

¹If \mathcal{S} is of the form $\text{cond} \Rightarrow \mathcal{S}_1$, then $[\mathcal{S}]_x$ is equivalent to $x \uparrow \wedge \text{cond} \Rightarrow \mathcal{S}_1$.

3.1 Domains, Constants and Functions

The domains (“data types”) that we need are:

- $\mathbb{B} = \{\underline{0}, \underline{1}\}$
- $\mathbb{N} = \{1, 2, 3, \dots\}$
= the set of natural numbers
- $\mathcal{SEQ} := \{1, \dots, \text{MaxSEQ}\} \subseteq \mathbb{N}$
= the set of possible values for the sequence number
- \mathcal{SN} = the identifier set of possible service networks
- \mathcal{RAND} = the set of possible values for the random numbers
- \mathcal{AUTN} = the set of possible values for the variable $AUTN$
- \mathcal{AV} = the set of admissible authentication vectors
- \mathcal{CHAC} = the set of admissible authentication challenges
- \mathcal{RESP}_A = the set of admissible authentication responses
- \mathcal{RESP}_J = the set of admissible authentication reject responses
- \mathcal{RESP}_S = the set of admissible authentication synchronisation
fail responses
- $\mathcal{FAIL} := \{\text{Loss, DB, Crash, Steal, Race}\}$

For boolean variables x or boolean-valued functions f (i.e., with domain \mathbb{B}) we will use the following shorthand, if no confusion arises: instead of writing $x = 0, f(v) = 0$ or $x = 1, f(v) = 1$ we will write simply $\neg x, \neg f(v)$, or $x, f(v)$ respectively. The numerical constants that we need are:

- MaxSEQ = the maximal possible value for the sequence number.
- Δ = the normal maximal difference between the counters
 seq_{MS} and seq_{HE} .
- N = the maximal increment of seq_{HE} when a batch of
authentication vectors is produced.
- N is much smaller than Δ , we will assume: $N < \Delta/2$.

In the specification in [2], (together with the CRs [3], [4], and [5] accepted at 3GPPSA3 London meeting) an AV is a tuple (“vector”) $AV = (\text{Rand}, \text{resp}, CK, IK, \text{seq} \oplus AK, \text{MODE}, MAC)$. The only values that we are explicitly interested in are: Rand , resp and seq . We will not use the components CK, IK in this specification, and we abstract away from MODE (say, this is part of the user ID and this is encoded in the secret key K). The secret key K as well as the mac MAC are only used implicitly to define further functions, as will become clear below. Instead of assuming that Rand , resp and seq are components of AV , we assume the existence of functions: $\underline{\text{Rand}}_{AV} : AV \mapsto \text{Rand}$, $\underline{\text{Resp}}_{AV} : AV \mapsto \text{resp}$, and $\underline{\text{Seq}}_{AV} : AV \mapsto \text{seq}$. The service network, \mathbf{SN} receives from the home environment the complete AV and sends to \mathbf{MS} , the mobile station, $\text{chall} := \underline{\text{Chall}}(AV)$ (in the original specification, chall is part of the authentication vector: $= (\text{Rand}, \text{seq} \oplus AK, \text{MODE}, MAC)$). The \mathbf{MS} is able to check the consistency of the challenge chall and to calculate the original parameter resp of the AV . Thus we assume the existence of functions: $\text{cons}_{\text{chall}}$ (to check the consistency of chall) and $\underline{\text{Resp}}_{\text{chall}}$ (to calculate resp , given chall). (Those functions, and most of the ones that we will introduce now, depend on the secret key K ; the function $\text{cons}_{\text{chall}}$ depends also in particular on the parameter MAC). Further, the \mathbf{MS} is able to calculate the

sequence number seq with a function Seq_{MS} applied to chall , and, in case something goes wrong, also the responses $\text{RejResp}(\text{chall})$ and $\text{SynResp}(\text{la_chall}, \text{chall})$ for an user authentication reject or user authentication synchronisation failure. In this last case, in the response $\text{SynResp} = \text{SynResp}(\text{la_chall}, \text{chall})$ the current value of the sequence number of the **MS** (= the sequence number of la_chall , as will be explained later) is encoded. The home environment **HE** is able to decode this value via a function Seq_{MS} and to verify the freshness of the response SynResp sent by the mobile station, comparing it to the random number Rand used by the **SN** in the last challenge. We call this verification function verif . In the case of a normal response, the **SN** uses a function cons_{res} to check that the response resp is consistent with the challenge $\text{Chall}(\text{AV})$. Also, let $\text{cons}_{AV}(\text{AV})$ denote that the authentication vector AV is consistent. Last, let synchronr be the function used by the **MS** to determine if the two sequence numbers, seq_{MS} , seq are or not “synchronous”, (seq_{MS} is the sequence number in the **MS**, and seq is the sequence number of the challenge). What “synchronous” exactly means, is for the most part of the specification, irrelevant, except that 1. if not too many AV s get lost, then all new challenges are synchronous, and 2. old (for instance, used or lost) challenges become non-synchronous with the passage of time or with successful authentications. But for the statements and proofs of the properties of the system, we will assume that $\text{synchronr}(\text{seq}_1, \text{seq}_2) := (\text{seq}_1 < \text{seq}_2) \wedge (\text{seq}_2 < \text{seq}_1 + \Delta)$.

The (constant, i.e rigid) functions that we need are:

$$\begin{aligned}
\text{Seq}_{AV} &: \mathcal{AV} \rightarrow \mathcal{SEQ} \\
\text{Seq}_{ch} &: \mathcal{CHAL} \rightarrow \mathcal{SEQ} \\
\text{Seq}_{MS} &: \mathcal{RESP}_S \rightarrow \mathcal{SEQ} \\
\text{Chall} &: \mathcal{AV} \rightarrow \mathcal{CHAL} \\
\text{Resp}_{AV} &: \mathcal{AV} \rightarrow \mathcal{RESP}_A \\
\text{Resp}_{ch} &: \mathcal{CHAL} \rightarrow \mathcal{RESP}_A \\
\text{Rand}_{AV} &: \mathcal{AV} \rightarrow \mathcal{RAND} \\
\text{Rand}_{ch} &: \mathcal{CHAL} \rightarrow \mathcal{RAND} \\
\text{RejResp} &: \mathcal{CHAL} \rightarrow \mathcal{RESP}_J \\
\text{SynResp} &: \mathcal{CHAL} \times \mathcal{CHAL} \rightarrow \mathcal{RESP}_S \\
\text{cons}_{AV} &: \mathcal{AV} \rightarrow \mathbb{B} \\
\text{cons}_{chall} &: \mathcal{CHAL} \rightarrow \mathbb{B} \\
\text{cons}_{res} &: \mathcal{CHAL} \times \mathcal{RESP}_A \rightarrow \mathbb{B} \\
\text{synchronr} &: \mathcal{SEQ} \times \mathcal{SEQ} \rightarrow \mathbb{B} \\
\text{verif} &: \mathcal{RESP}_S \times \mathcal{RAND} \rightarrow \mathbb{B}
\end{aligned}$$

The function Seq_{AV} defines a transitive, irreflexive relation \prec in \mathcal{AV} :

$$\text{AV}_1 \prec \text{AV}_2 :\Leftrightarrow \text{Seq}_{AV}(\text{AV}_1) < \text{Seq}_{AV}(\text{AV}_2)$$

We will assume some properties of these functions. First, the trivial commutations:

$$\begin{aligned}
\text{Seq}_{ch} \circ \text{Chall} &= \text{Seq}_{AV} \\
\text{Resp}_{ch} \circ \text{Chall} &= \text{Resp}_{AV} \\
\text{Rand}_{ch} \circ \text{Chall} &= \text{Rand}_{AV}
\end{aligned}$$

At its proper place, in Sections 4 and 6 (in the definitions of $\mathcal{N}_{normal}^{HE}$ and $\mathcal{N}_{critical}^{HE}$), it will be assumed that any AV generated by the **HE** is consistent.

Now, if AV is consistent, then its challenge is also consistent and also consistent to its corresponding response. One challenge has only one consistent corresponding response.

$$\begin{aligned}
& cons_{AV}(AV) \Rightarrow cons_{chall}(\underline{Chall}(AV)) \wedge cons_{res}(\underline{Chall}(AV), \underline{Resp}(AV)) \\
& cons_{res}(chall, resp) \wedge resp_1 \neq resp \Rightarrow \neg cons_{res}(chall, resp_1) \\
& \text{verif}(\text{SynResp}, \text{Rand}) \Leftrightarrow \\
& \quad \exists_{AV, chall_1} \text{SynResp} = \underline{SynResp}(chall_1, \underline{Chall}(AV)) \wedge \text{Rand} = \underline{Rand}(AV) \\
& \underline{Seq}_{MS}(\underline{SynResp}(chall_1, chall_2)) = \underline{Seq}_{ch}(chall_1)
\end{aligned}$$

In the sequel, if no confusion arises, we omit the subscripts, writing \underline{Seq} instead of \underline{Seq}_{ch} , \underline{Seq}_{AV} or \underline{Seq}_{MS} , \underline{Resp} instead of \underline{Resp}_{ch} or \underline{Resp}_{AV} , \underline{Rand} instead of \underline{Rand}_{ch} or \underline{Rand}_{AV} and $cons$ instead of $cons_{AV}$, $cons_{chall}$ or $cons_{res}$.

3.2 The variables of the system

First let us introduce some rather standard notation for two higher-order constructs that we need: \mathcal{AV}^* is the set of all *words* $AV_1 AV_2 AV_3 \dots AV_n$ built with “letters” from \mathcal{AV} : $AV_i \in \mathcal{AV}$. The basic operations in this domain are: $Head : \mathcal{AV}^* \rightarrow \mathcal{AV}$ that chooses the first letter of the word: $Head(AV_1 AV_2 AV_3 \dots AV_n) = AV_1$ and $Tail : \mathcal{AV}^* \rightarrow \mathcal{AV}^*$ is the rest of word: $Tail(AV_1 AV_2 AV_3 \dots AV_n) = (AV_2 AV_3 \dots AV_n)$. ϵ is the empty word. On the other hand $\wp(\mathcal{AV})$ is the power-set of \mathcal{AV} : the set of all subsets of \mathcal{AV} .

The variables that we will need are:

$$\begin{aligned}
seq_{HE} & : \mathcal{SEQ} \\
DB & : \mathcal{SN} \rightarrow \mathcal{AV}^* \quad \text{called the database of AVs} \\
la_chall & : \mathcal{CHAL} \quad \text{the last accepted challenge, that is, the} \\
& \quad \text{last challenge accepted by the MS}
\end{aligned}$$

Thus, for SN in \mathcal{SN} , the database $DB(SN)$ of AVs stored in the node SN is a *word* $AV_1 AV_2 AV_3 \dots AV_n$ of authentication vectors AV_i . We will denote by $Set(\omega)$ the set $\{AV_1, AV_2, AV_3, \dots, AV_n\}$ of letters in the word $\omega = AV_1 AV_2 AV_3 \dots AV_n$. By abuse of notation we will use sometimes $DB(SN)$ in a context where a *set* is expected instead of a *word*, meaning: $Set(DB(SN))$. Thus $\dots \cup DB(SN)$ is $\dots \cup Set(DB(SN))$ and $\dots \subseteq DB(SN)$ is $\dots \subseteq Set(DB(SN))$.

The auxiliary variables, defined later in Sections 4 and 6 are:

$$\begin{aligned}
Gen & : \wp(\mathcal{AV}) \quad \text{the set of generated AVs} \\
Used & : \wp(\mathcal{AV}) \quad \text{the set of used (sent) AVs} \\
Stolen_{HE} & : \wp(\mathcal{AV}) \quad \text{the set of AVs that were stolen in the HE} \\
Stolen_{SN} & : \wp(\mathcal{AV}) \quad \text{the set of AVs that were stolen in an SN} \\
Stolen & : \wp(\mathcal{AV}) \quad \text{the set of stolen AVs} \\
Accepted & : \wp(\mathcal{AV}) \quad \text{the set of AVs accepted by the MS} \\
Successful & : \wp(\mathcal{AV}) \quad \text{the set of AVs accepted by the MS and correctly replied} \\
Lost & : \wp(\mathcal{AV}) \quad \text{the set of lost AVs} \\
last_SN & : \mathcal{SN} \quad \text{in normal behavior, the SN where the user is registered.} \\
curr_SN & : \wp(\mathcal{SN}) \quad \text{the current set of SNs where the user is registered} \\
& \quad \text{in normal behavior, it is } \{last_SN\}, \text{ in incorrect behavior} \\
& \quad \text{it may contain no or several SNs.}
\end{aligned}$$

Definition 3.1. *The state functions are:*

$$seq_{MS} := \underline{Seq}(la_chall) : \mathcal{SEQ}$$

Definition 3.2.

$$Init :\Leftrightarrow seq_{MS} = 0 \wedge seq_{HE} = 0 \wedge \forall_{SN} \quad DB(SN) = \epsilon \wedge Stolen = \emptyset$$

3.3 The Messages: the Transitions of the System

There is a simple way of modeling the occurrence of messages in a purely state-based approach like TLA: for each message or event MESSAGE_X introduce a variable n_x that changes exactly when MESSAGE_X occurs. For convenience, if MESSAGE_X is a message with parameters of types $\mathcal{X}_1, \mathcal{X}_2, \dots, \mathcal{X}_n$ we take the variable n_x to be of type $\mathcal{X}_1 \times \mathcal{X}_2 \times \dots \times \mathcal{X}_n \rightarrow \mathbb{N}$. $n_x(x_1, x_2, \dots, x_n)$ may for instance count (in \mathbb{N} or modulo a convenient number) how often the message (or event) MESSAGE_X with parameters x_1, x_2, \dots, x_n happens. Instead of using the variable n_x in our specification, we introduce a new predicate, say $X(x_1, x_2, \dots, x_n)$, which is an abbreviation:

$$X(x_1, x_2, \dots, x_n) :\Leftrightarrow n_x(x_1, x_2, \dots, x_n) \uparrow$$

(If x is a variable, we denote by $x\uparrow$ the transition predicate $x' \neq x$.)

If MESSAGE_X is a message between **SN** and **MS**, then this message may get lost. Therefore, we have to distinguish the two events: sending MESSAGE_X and receiving MESSAGE_X, which may happen independently of each other.

For instance, USER AUTHENT. REQUEST gives rise to two different events, USER AUTHENT. REQUEST SEND (short: UAR_s) and USER AUTHENT. REQUEST RECEIVE (UAR_r):

1. Normally, if a UAR_s happens, then a UAR_r also happens, with the same parameters.
2. Due to an attack, the UAR_r may contain different parameters than the corresponding Send.
3. A sent UAR_s may get lost in the transmission channel, thus producing no UAR_r event.
4. Due to an attack, the USIM may receive a UAR_r that was not sent at all by the SN.

The SN receives (or produces) a TIME OUT, if the response to the USER AUTHENT. REQUEST SEND is lost or delayed. MVAV (“Move Authentication Vectors”) is the closed action of SEND ID REQ and SEND ID RESP.

<i>Message</i>	<i>Trans. Pred.</i>	<i>Param. Name</i>	<i>Param. Type</i>	<i>Var. Name</i>
AUTHENT. DATA REQUEST (no syn. fail)	ADR ₀	SN	\mathcal{SN}	$n_{\text{ADR},0}$
AUTHENT. DATA REQUEST (syn. fail)	ADR ₁	(SynResp, Rand, SN)	(\mathcal{RESP}_S , \mathcal{RAND} , \mathcal{SN})	$n_{\text{ADR},1}$
AUTHENT. DATA RESPONSE	ADS	(AVs_new, SN)	(\mathcal{AV}^* , \mathcal{SN})	n_{ADS}
USER AUTHENT. REQUEST	UAR _s	(chall, SN)	(\mathcal{CHAL} \mathcal{SN})	$n_{\text{UAR},s}$
	UAR _r	(chall, SN)	(\mathcal{CHAL} \mathcal{SN})	$n_{\text{UAR},r}$
USER AUTHENT. RESPONSE	UAS _s	(resp, SN)	(\mathcal{RESP}_A \mathcal{SN})	$n_{\text{UAS},s}$
	UAS _r	(resp, SN)	(\mathcal{RESP}_A \mathcal{SN})	$n_{\text{UAS},r}$
USER AUTHENT. REJECT	UAJ _s	(RejResp, SN)	(\mathcal{RESP}_J \mathcal{SN})	$n_{\text{UAJ},s}$
	UAJ _r	(RejResp, SN)	(\mathcal{RESP}_J \mathcal{SN})	$n_{\text{UAJ},r}$
USER AUTHENT. SYNCHRON. FAIL INDICATION	UASF _s	(SynResp, SN)	(\mathcal{RESP}_S \mathcal{SN})	$n_{\text{UASF},s}$
	UASF _r	(SynResp, SN)	(\mathcal{RESP}_S \mathcal{SN})	$n_{\text{UASF},r}$

Table 1: Messages of the Protocol

<i>Message or Event</i>	<i>Trans. Pred.</i>	<i>Param. Name</i>	<i>Param. Type</i>	<i>Var. Name</i>
LOCATION UPDATE REQUEST	LUR	SN SN ₁	\mathcal{SN} \mathcal{SN}	$n_{\text{LUR},s}$
CANCEL LOCATION	CANLOC _s	SN	\mathcal{SN}	$n_{\text{CanLoc},s}$
	CANLOC _r	SN	\mathcal{SN}	$n_{\text{CanLoc},r}$
MOVE AVs (SEND ID REQ and SEND ID RESP)	MvAV	SN SN ₁	\mathcal{SN} \mathcal{SN}	n_{MvAV}
TIME OUT	TiO	SN	\mathcal{SN}	n_{TiO}

Table 2: Messages or Events outside of the protocol

Definition 3.3. (The Messages)

$$\begin{aligned}
\text{ADR}_0(\text{SN}) &:\Leftrightarrow n_{\text{ADR},0}(\text{SN})\uparrow \\
\text{ADR}_1(\text{SynResp}, \text{Rand}, \text{SN}) &:\Leftrightarrow n_{\text{ADR},1}(\text{SynResp}, \text{Rand}, \text{SN})\uparrow \\
\text{ADS}(\text{AVs_new}, \text{SN}) &:\Leftrightarrow n_{\text{ADS}}(\text{AVs_new}, \text{SN})\uparrow \\
\text{UAR}_s(\text{chall}, \text{SN}) &:\Leftrightarrow n_{\text{UAR},s}(\text{chall}, \text{SN})\uparrow \\
\text{UAR}_r(\text{chall}, \text{SN}) &:\Leftrightarrow n_{\text{UAR},r}(\text{chall}, \text{SN})\uparrow \\
\text{UAS}_s(\text{resp}, \text{SN}) &:\Leftrightarrow n_{\text{UAS},s}(\text{resp}, \text{SN})\uparrow \\
\text{UAS}_r(\text{resp}, \text{SN}) &:\Leftrightarrow n_{\text{UAS},r}(\text{resp}, \text{SN})\uparrow \\
\text{UAJ}_s(\text{RejResp}, \text{SN}) &:\Leftrightarrow n_{\text{UAJ},s}(\text{RejResp}, \text{SN})\uparrow \\
\text{UAJ}_r(\text{RejResp}, \text{SN}) &:\Leftrightarrow n_{\text{UAJ},r}(\text{RejResp}, \text{SN})\uparrow \\
\text{UASF}_s(\text{SynResp}, \text{SN}) &:\Leftrightarrow n_{\text{UASF},s}(\text{SynResp}, \text{SN})\uparrow \\
\text{UASF}_r(\text{SynResp}, \text{SN}) &:\Leftrightarrow n_{\text{UASF},r}(\text{SynResp}, \text{SN})\uparrow \\
\text{LUR}(\text{SN}, \text{SN}_1) &:\Leftrightarrow n_{\text{LUR}}(\text{SN}, \text{SN}_1)\uparrow \\
\text{CANLOC}_s(\text{SN}) &:\Leftrightarrow n_{\text{CANLOC},s}(\text{SN})\uparrow \\
\text{CANLOC}_r(\text{SN}) &:\Leftrightarrow n_{\text{CANLOC},r}(\text{SN})\uparrow \\
\text{MvAV}(\text{SN}, \text{SN}_1) &:\Leftrightarrow n_{\text{MvAV}}(\text{SN}, \text{SN}_1)\uparrow \\
\text{TIO}(\text{SN}) &:\Leftrightarrow n_{\text{TIO}}(\text{SN})\uparrow
\end{aligned}$$

By abuse of notation, we will use the predicates $\text{ADR}_0, \text{ADR}_1, \text{ADS}, \dots$ *without parameters* to intend an implicit existential quantification:

Convention 3.1.

$$\begin{aligned}
\text{ADR}_0 &:\Leftrightarrow \exists_{\text{SN}} \text{ADR}_0(\text{SN}) \\
\text{ADR}_1 &:\Leftrightarrow \exists_{\text{SynResp}, \text{Rand}, \text{SN}} \text{ADR}_1(\text{SynResp}, \text{Rand}, \text{SN}) \\
\text{ADS} &:\Leftrightarrow \exists_{\text{AVs_new}, \text{SN}} \text{ADS}(\text{AVs_new}, \text{SN}) \\
&\dots
\end{aligned}$$

Further we will use the predicates $\text{ADR}_1(\text{SN}), \text{ADS}(\text{SN}), \dots$ *without other parameters* to intend an implicit existential quantification over the non mentioned parameters:

Convention 3.2.

$$\begin{aligned}
\text{ADR}_1(\text{SN}) &:\Leftrightarrow \exists_{\text{SynResp}, \text{Rand}} \text{ADR}_1(\text{SynResp}, \text{Rand}, \text{SN}) \\
\text{ADS}(\text{SN}) &:\Leftrightarrow \exists_{\text{AVs_new}} \text{ADS}(\text{AVs_new}, \text{SN}) \\
&\dots
\end{aligned}$$

We will not really use the variables $n_{\text{ADR},0}(\text{SN})$, etc. any further. Their only purpose is to accommodate to TLA. One note on TLA: instead of using the conventional syntax $[\mathcal{A}]_x$ of TLA, we prefer the equivalent more readable form: $x\uparrow \Rightarrow \mathcal{A}$.

Notice also that $x\uparrow \wedge \mathcal{P} \Rightarrow \mathcal{A}$ is $[\mathcal{P} \Rightarrow \mathcal{A}]_x$

It is impossible that a message MESSAGE_X happens at the same time with two different sets of parameters: $X(x_1, x_2, \dots x_n) \wedge X(y_1, y_2, \dots y_n) \wedge (x_1, x_2, \dots x_n) \neq$

$(y_1, y_2, \dots, y_n):$

$$\begin{aligned}
\mathcal{A}_{normal}^{interleave} : \Leftrightarrow & \\
\Box(\forall \text{SN, SynResp, Rand, AVs_new, chall, resp, RejResp, SynResp} & \\
\forall \text{SN}_1, \text{SynResp}_1, \text{Rand}_1, \text{AVs_new}_1, \text{chall}_1, \text{resp}_1, \text{RejResp}_1, \text{SynResp}_1 & \\
\wedge \text{ADR}_0(\text{SN}) \wedge \text{ADR}_0(\text{SN}_1) \Rightarrow \text{SN} = \text{SN}_1 & \\
\wedge \text{ADR}_1(\text{SynResp, Rand, SN}) \wedge \text{ADR}_1(\text{SynResp}_1, \text{Rand}_1, \text{SN}_1) & \\
\Rightarrow \text{SynResp} = \text{SynResp}_1 \wedge \text{Rand} = \text{Rand}_1 \wedge \text{SN} = \text{SN}_1 & \\
\wedge \text{ADS}(\text{AVs_new, SN}) \wedge \text{ADS}(\text{AVs_new}_1, \text{SN}_1) & \\
\Rightarrow \text{AVs_new} = \text{AVs_new}_1 \wedge \text{SN} = \text{SN}_1 & \\
\wedge \text{UAR}_s(\text{chall, SN}) \wedge \text{UAR}_s(\text{chall}_1, \text{SN}_1) & \\
\Rightarrow \text{chall} = \text{chall}_1 \wedge \text{SN} = \text{SN}_1 & \\
\wedge \text{UAR}_R(\text{chall, SN}) \wedge \text{UAR}_R(\text{chall}_1, \text{SN}_1) & \\
\Rightarrow \text{chall} = \text{chall}_1 \wedge \text{SN} = \text{SN}_1 & \\
\wedge \text{UAS}_s(\text{resp, SN}) \wedge \text{UAS}_s(\text{resp}_1, \text{SN}_1) & \\
\Rightarrow \text{resp} = \text{resp}_1 \wedge \text{SN} = \text{SN}_1 & \\
\wedge \text{UAS}_R(\text{resp, SN}) \wedge \text{UAS}_R(\text{resp}_1, \text{SN}_1) & \\
\Rightarrow \text{resp} = \text{resp}_1 \wedge \text{SN} = \text{SN}_1 & \\
\wedge \text{UAJ}_s(\text{RejResp, SN}) \wedge \text{UAJ}_s(\text{RejResp}_1, \text{SN}_1) & \\
\Rightarrow \text{RejResp} = \text{RejResp}_1 \wedge \text{SN} = \text{SN}_1 & \\
\wedge \text{UAJ}_R(\text{RejResp, SN}) \wedge \text{UAJ}_R(\text{RejResp}_1, \text{SN}_1) & \\
\Rightarrow \text{RejResp} = \text{RejResp}_1 \wedge \text{SN} = \text{SN}_1 & \\
\wedge \text{UASF}_s(\text{SynResp, SN}) \wedge \text{UASF}_s(\text{SynResp}_1, \text{SN}_1) & \\
\Rightarrow \text{SynResp} = \text{SynResp}_1 \wedge \text{SN} = \text{SN}_1 & \\
\wedge \text{UASF}_R(\text{SynResp, SN}) \wedge \text{UASF}_R(\text{SynResp}_1, \text{SN}_1) & \\
\Rightarrow \text{SynResp} = \text{SynResp}_1 \wedge \text{SN} = \text{SN}_1 & \\
\wedge \text{UAS}_s \Rightarrow \neg \text{UAJ}_s \wedge \neg \text{UASF}_s & \\
\wedge \text{UAJ}_s \Rightarrow \neg \text{UAS}_s \wedge \neg \text{UASF}_s & \\
\wedge \text{UASF}_s \Rightarrow \neg \text{UAS}_s \wedge \neg \text{UAJ}_s) &
\end{aligned}$$

4 Transitions of the normal System

4.1 Changing the Location

Let us first define the auxiliary variable $\text{curr_SN} : \wp(\mathcal{SN})$ in the following way:

$$\begin{aligned}
\mathcal{A}_{normal}^{CurrSN} : \Leftrightarrow & \\
\wedge \exists \text{SN } \text{curr_SN} = \{\text{SN}\} & \\
\Box(\wedge \text{curr_SN} \uparrow \Rightarrow \text{LUR} \vee \text{CANLOC} & \\
\wedge \text{LUR}(\text{SN, SN}_1) \wedge \text{CANLOC}(\text{SN}_2) \Rightarrow & \\
\text{curr_SN}' = (\text{curr_SN} \setminus \{\text{SN}_2\}) \cup \{\text{SN}_1\} & \\
\wedge \text{LUR}(\text{SN, SN}_1) \wedge \neg \text{CANLOC} \Rightarrow & \\
\text{curr_SN}' = \text{curr_SN} \cup \{\text{SN}_1\} & \\
\wedge \text{CANLOC}(\text{SN}) \wedge \neg \text{LUR} \Rightarrow & \\
\text{curr_SN}' = (\text{curr_SN} \setminus \{\text{SN}\})) &
\end{aligned}$$

The intuition is that, under ideal² behavior, a $\text{LUR}(\text{SN}, \text{SN}_1)$ implies a $\text{CANLOC}(\text{SN})$. In this case, in the set of current SNs the old SN, SN , is replaced by the new one, SN_1 : $\text{curr_SN}' = (\text{curr_SN} \setminus \{\text{SN}\}) \cup \{\text{SN}_1\}$. Thus curr_SN would always be a singleton. We will allow *in normal conditions* that a $\text{CANLOC}(\text{SN})$ occurs without a $\text{LUR}(\text{SN}, \text{SN}_1)$, thus curr_SN is always a singleton or empty. In more critical situations we will allow curr_SN to be an arbitrary (finite) set: it is the set of SNs for which a $\text{LUR}(\text{SN}, \text{SN}_1)$ has not been followed by a $\text{CANLOC}(\text{SN})$.

With this definition, our specification of the location update step may be written as:

$$\begin{aligned}
\mathcal{N}_{normal}^{LU} : \Leftrightarrow & \\
& \wedge \text{curr_SN}' = \emptyset \vee \exists_{\text{SN}_0} \text{curr_SN}' = \{\text{SN}_0\} \\
& \wedge \text{LUR}(\text{SN}, \text{SN}_1) \Rightarrow \text{MvAV}(\text{SN}, \text{SN}_1) \vee \text{DB}'(\text{SN}_1) = \epsilon \\
& \wedge \text{MvAV}(\text{SN}, \text{SN}_1) \Rightarrow \text{LUR}(\text{SN}, \text{SN}_1) \\
& \wedge \text{ADS} \Rightarrow \text{curr_SN}' = \text{curr_SN} \\
& \wedge \text{MvAV}(\text{SN}, \text{SN}_1) \Rightarrow \wedge \text{DB}'(\text{SN}_1) = \text{DB}(\text{SN}) \\
& \quad \wedge \text{DB}'(\text{SN}) = \epsilon \\
& \quad \wedge \forall_{\text{SN}_2} (\text{SN}_2 \neq \text{SN} \wedge \text{SN}_2 \neq \text{SN}_1 \Rightarrow \\
& \quad \quad \text{DB}'(\text{SN}_2) = \text{DB}'(\text{SN}_2))
\end{aligned}$$

The five points in this requirement are:

first, as explained before, a CANLOC may happen without a LUR , (resulting in $\text{curr_SN}' = \emptyset$). On the other hand, a LUR can happen without a CANLOC only if $\text{curr_SN} = \emptyset$, (resulting in $\text{curr_SN}'$ being a singleton, that is, $\exists_{\text{SN}_0} \text{curr_SN}' = \{\text{SN}_0\}$), or in other words, if CANLOC has already happened. In any case, both a LUR and its corresponding CANLOC can happen simultaneously.

Second, a LUR may trigger a MvAV , but not necessarily; if no MvAV happens, then $\text{DB}'(\text{SN}_1) = \epsilon$. If MvAV happens, then $\text{DB}'(\text{SN}_1) = \text{DB}(\text{SN})$. Thus, in any case, any old existing AVs are to be discarded.

Third, a MvAV is always produced by a LUR .

Fourth, no race condition happens. This type of race condition will be discussed later in Section 6.

And last, when a MvAV happens, the AVs of the old SN are moved to the new SN .

Let us now define the auxiliary variable $\text{last_SN} : \mathcal{SN}$ in the following way:

$$\begin{aligned}
\mathcal{A}_{normal}^{LastSN} : \Leftrightarrow & \\
& \wedge \text{curr_SN} = \{\text{last_SN}\} \\
& \wedge \Box (\wedge \text{last_SN} \uparrow \Rightarrow \text{curr_SN} \uparrow) \\
& \wedge \forall_{\text{SN}_0} (\text{curr_SN} \uparrow \wedge \text{curr_SN}' = \{\text{SN}_0\} \Rightarrow \text{last_SN}' = \text{SN}_0) \\
& \wedge (\text{curr_SN} \uparrow \wedge \forall_{\text{SN}_0} \text{curr_SN}' \neq \{\text{SN}_0\}) \Rightarrow \text{last_SN}' = \text{last_SN}
\end{aligned}$$

Notice that we in the context of $\Box \mathcal{N}_{normal}^{LU}$ the predicate $\forall_{\text{SN}_0} \text{curr_SN}' \neq \{\text{SN}_0\}$ in the last line of the last formula, is equivalent to $\text{curr_SN}' = \emptyset$. Thus, in this context, even if curr_SN is empty, last_SN is the last SN where the user was registered.

4.2 The Serving Network

Let us consider first the $\text{AUTHENT. DATA REQUEST}$ with the synchronisation flag turned off (ADR_0 , that is, no synchronisation fail has happened). The reason for

²We do not model explicitly “ideal behavior”. We let our best scenario, “normal behavior”, to contain already “normal” errors, like an LUR without a CANLOC .

issuing this message is that the SN has only few or no authentication vectors left. For simplicity, we assume the last case, i.e., $ADR_0 \Rightarrow DB(SN) = \epsilon$.

On the other hand, the only reason for asking AUTHENT. DATA REQUEST with the synchronisation flag turned on (ADR_1), is that a synchronisation fail has happened, or, more precisely, a UASF has been obtained as response to a UAR_s .

The **SN** reacts to AUTHENT. DATA RESPONSE by updating the database of AVs ($DB(SN)$).

When the **SN** sends a USER AUTHENT. REQUEST SEND, it updates the database of AVs by deleting the first AV in the list $DB(SN)$. (This AV is now the “current AV”, and the values are used to compare with the expected response, $UAS_r(resp, SN)$). If, sending a user authentication request, no answer (UAS_r or UAJ_r or $UASF_r$) is received, then a TiO happens.

$$\begin{aligned}
\mathcal{N}_{normal}^{SN} : \Leftrightarrow & \\
& \wedge ADR_0(SN) \Rightarrow DB(SN) = \epsilon \wedge SN \in curr_SN \\
& \wedge ADR_1(SynResp, Rand, SN) \Rightarrow \\
& \quad \wedge UASF_r(SynResp, SN) \\
& \quad \wedge SN \in curr_SN \\
& \quad \wedge \exists_{AV} (UAR_s(Chall(AV), SN) \wedge Rand = Rand(AV)) \\
& \wedge ADS(AVs_new, SN) \Rightarrow \wedge AVs_new \neq \epsilon \Rightarrow DB'(SN) = AVs_new \\
& \quad \wedge AVs_new = \epsilon \Rightarrow DB'(SN) = DB(SN) \\
& \wedge UAR_s(chall, SN) \Rightarrow \wedge SN \in curr_SN \wedge DB(SN) \neq \epsilon \\
& \quad \wedge DB'(SN) = Tail(DB(SN)) \\
& \quad \wedge chall = Chall(Head(DB(SN))) \\
& \wedge UAR_s(chall, SN) \Rightarrow \vee \exists_{resp} UAS_r(resp, SN) \\
& \quad \vee \exists_{RejResp} UAJ_r(RejResp, SN) \\
& \quad \vee \exists_{SynResp} UASF_r(SynResp, SN) \\
& \quad \vee TiO \\
& \wedge DB(SN) \neq \epsilon \Rightarrow \vee \exists_{AVs_new, SN} ADS(AVs_new, SN) \wedge AVs_new \neq \epsilon \\
& \quad \vee \exists_{chall, SN} UAR_s(chall, SN) \\
& \quad \vee \exists_{SN_1} MvAV(SN, SN_1) \\
& \quad \vee \exists_{SN_1} MvAV(SN_1, SN) \\
& \wedge [\wedge UASF_r(SynResp, SN) \\
& \quad \wedge SN \in curr_SN \\
& \quad \wedge UAR_s(Chall(AV), SN) \\
& \quad \wedge Rand = Rand(AV)] \Rightarrow ADR_1(SynResp, Rand, SN)
\end{aligned}$$

4.3 The Home Environment

In the next definition we use a new (bound) variable seq_{he} that contains a temporary value for seq_{HE} . The reader may understand the specification of the step $\mathcal{N}_{normal}^{HE}$ as the sequential composition of two “micro-steps”:

$$\begin{aligned}
\mathcal{N}_{normal}^{HE}(seq_{HE}, seq_{HE}') = & \exists_{seq_{he}} \\
& (\mathcal{N}_{normal}^{1, HE}(seq_{HE}, seq_{he}) \wedge \mathcal{N}_{normal}^{2, HE}(seq_{he}, seq_{HE}'))
\end{aligned}$$

Notice, by the way, that if $\mathcal{N}_{normal}^{HE} \wedge (\text{ADR}_0 \vee \text{ADR}_1)$ the value of seq_{HE} uniquely determines the value of seq_{he} .

Recall that AVs_new is a word (or ordered sequence) of AVs. We write $\text{AV}_1 \ll_{\text{AVs_new}} \text{AV}_2$ iff both AV_1 and AV_1 appear in AVs_new and AV_1 appears (anywhere) *left* of AV_2 .

Here we write \ll instead of $\ll_{\text{AVs_new}}$.

$$\begin{aligned}
\mathcal{N}_{normal}^{HE} : \Leftrightarrow \exists_{seq_{he}} [& \\
& \wedge \text{ADS}(\text{AVs_new}, \text{SN}) \Rightarrow \vee \text{ADR}_0(\text{SN}) \\
& \quad \vee \exists_{\text{SynResp}, \text{Rand}} \text{ADR}_1(\text{SynResp}, \text{Rand}, \text{SN}) \\
& \wedge \text{ADR}_0 \vee \text{ADR}_1 \Rightarrow \text{ADS} \\
& \wedge \text{ADR}_0 \Rightarrow seq_{he} = seq_{HE} \\
& \wedge \text{ADR}_1(\text{SynResp}, \text{Rand}, \text{SN}) \Rightarrow \\
& \quad \wedge [\text{verif}(\text{SynResp}, \text{Rand}) \wedge \\
& \quad \quad \neg \text{synchron}_1(\underline{Seq}_{MS}(\text{SynResp}), seq_{HE})] \Rightarrow seq_{he} = \underline{Seq}_{MS}(\text{SynResp}) \\
& \quad \wedge [\neg \text{verif}(\text{SynResp}, \text{Rand}) \vee \\
& \quad \quad \text{synchron}_1(\underline{Seq}_{MS}(\text{SynResp}), seq_{HE})] \Rightarrow seq_{he} = seq_{HE} \\
& \wedge \text{ADS}(\text{AVs_new}, \text{SN}) \Rightarrow \\
& \quad \wedge \text{AVs_new} \neq \epsilon \\
& \quad \wedge \text{AV} \in \text{AVs_new} \Rightarrow \text{cons}(\text{AV}) \\
& \quad \wedge \forall_{\text{AV}_1, \text{AV}_2 \in \text{AVs_new}} (\text{AV}_1 \prec \text{AV}_2 \Leftrightarrow \text{AV}_1 \ll \text{AV}_2) \\
& \quad \wedge \forall_{\text{AV} \in \text{AVs_new}} (seq_{he} < \underline{Seq}(\text{AV}) \leq seq'_{HE}) \\
& \quad \wedge \forall_{i \in \mathbb{N}} \exists_{\text{AV} \in \text{AVs_new}} (seq_{he} < i \leq seq'_{HE} \Rightarrow \underline{Seq}(\text{AV}) = i) \\
& \quad \wedge seq'_{HE} - seq_{he} \leq N \\
& \wedge seq_{HE} \uparrow \Rightarrow \exists_{\text{AVs_new}, \text{SN}} \text{ADS}(\text{AVs_new}, \text{SN}) \wedge \text{AVs_new} \neq \epsilon]
\end{aligned}$$

In this specification we have used a new function synchron_1 , instead of our old synchron . The reason is the following: we want not only that the current value of seq_{HE} is in the correct range: $\text{synchron}(seq_{MS}, seq_{HE})$, but also that the new value of seq_{HE} is also in the correct range (else, although seq_{HE} is in the correct range the HE could generate AVs which are outside of this range). Thus we also want: $\text{synchron}(seq_{MS}, seq_{HE}')$, or in other words: $\text{synchron}(seq_{MS}, seq_{HE} + N)$. The definition of $\text{synchron}_1(x, y)$ is therefore:

$$\text{synchron}_1(x, y) := \text{synchron}(x, y) \wedge \text{synchron}(x, y + N)$$

This specification says nothing about where do the AVs in AVs_new come from. They can be generated in the moment in which they are sent (through an Authentication Data Response), or “pre-generated” and kept in an internal HE Database.

It is important for our proofs that, in normal behavior, when ADR_0 or $\text{ADR}_1(\text{SynResp}, \text{Rand}, \text{SN})$ with $\text{verif}(\text{SynResp}, \text{Rand}) \wedge \neg \text{synchron}_1(\underline{Seq}_{MS}(\text{SynResp}), seq_{HE})$, the parameter AVs_new in $\text{ADS}(\text{AVs_new}, \text{SN})$ is not the empty word. In other cases it could be empty without changing our properties or proofs. For the meantime, we follow the original specification, in which AVs_new is never ϵ . Later, for the incorrect system, we will weaken this assumption.

4.4 The Communication Channel

Recall from Convention 3.2 that for instance $UAR_s(SN)$ means $\exists_{resp} UAR_s(resp, SN)$, i.e. an implicit existential quantification over the non mentioned parameters. Let us say that the mobile station communicates with the SN if in any one of the two direction a message is sent or received.

$$\begin{aligned} Comm(SN) : \Leftrightarrow & \vee UAR_s(SN) \vee UAR_s(SN) \\ & \vee UAS_s(SN) \vee UAS_s(SN) \\ & \vee UAJ_s(SN) \vee UAJ_s(SN) \\ & \vee UASF_s(SN) \vee UASF_s(SN) \end{aligned}$$

We will assume that the MS communicates at the same time with only one SN: $Comm(SN) \wedge Comm(SN_1) \Rightarrow SN = SN_1$

The message USER AUTHENT. REQUEST may be received correctly (OKR), or it may be corrupted during the transmission ($CorrR$), or it may get lost ($LossR$):

$$\begin{aligned} OKR : \Leftrightarrow & \exists_{chall, SN} \wedge UAR_s(chall, SN) \\ & \wedge UAR_R(chall, SN) \\ CorrR : \Leftrightarrow & \exists_{chall, SN} \wedge UAR_s(chall, SN) \\ & \wedge \exists_{chall_1} \neg cons(chall_1) \wedge UAR_R(chall_1, SN) \\ LossR : \Leftrightarrow & \exists_{chall, SN} \wedge UAR_s(chall, SN) \\ & \wedge \neg UAR_R(SN) \end{aligned}$$

We will assume that during each step of the normal system, $UAR_s \Rightarrow OKR \vee CorrR \vee LossR$. In other words, our assumption is that the challenge $chall$ in $UAR_s(chall, SN)$ can not be replaced during the communication by another challenge $chall_1$ (in $UAR_R(chall_1, SN)$) which is also consistent. This sort of situation will be discussed later in Section 6.

On the other direction, the message USER AUTHENT. RESPONSE may be received correctly (OKS), or it may be corrupted during the transmission ($CorrS$), or it may get lost ($LossS$). As in the other directions, our assumption is that the response can not be replaced during the communication by another consistent or verifiable response. For the case of a normal response, this amounts to nothing, because there is only one consistent response. For the case of a synchronisation fail, we have to state explicitly, that if $UAR_s(\underline{Chall}(AV), SN)$ happens in the same step, then the corrupted response is not verifiable (with respect to the random number of this AV). This is exactly what we ask in the Assumption 4.1. Another possibility would be to impose $\mathcal{N}_{critical}^{Ass_3}$, discussed later in Assumption 6.3.

$$\begin{aligned} OKS : \Leftrightarrow & \vee \exists_{resp, SN} \wedge UAS_s(resp, SN) \\ & \wedge UAS_R(resp, SN) \\ & \vee \exists_{RejResp, SN} \wedge UAJ_s(RejResp, SN) \\ & \wedge UAJ_R(RejResp, SN) \\ & \vee \exists_{SynResp, SN} \wedge UASF_s(SynResp, SN) \\ & \wedge UASF_R(SynResp, SN) \end{aligned}$$

$$\begin{aligned}
CorrS &:\Leftrightarrow \vee \exists_{resp, SN} \wedge UAS_s(resp, SN) \\
&\quad \wedge \exists_{resp_1} resp_1 \neq resp \wedge UAS_r(resp_1, SN) \\
&\vee \exists_{RejResp, SN} \\
&\quad \wedge UAJ_s(RejResp, SN) \\
&\quad \wedge \exists_{RejResp_1} RejResp_1 \neq RejResp \wedge UAJ_r(RejResp_1, SN) \\
&\vee \exists_{SynResp, SN} \\
&\quad \wedge UASF_s(SynResp, SN) \\
&\quad \wedge \exists_{SynResp_1} \wedge SynResp_1 \neq SynResp \\
&\quad \quad \wedge UASF_r(SynResp_1, SN) \\
\\
LossS &:\Leftrightarrow \wedge \vee UAS_s(SN) \\
&\quad \vee UAJ_s(SN) \\
&\quad \vee UASF_s(SN) \\
&\quad \wedge \neg UAS_r(SN) \\
&\quad \wedge \neg UAJ_r(SN) \\
&\quad \wedge \neg UASF_r(SN)
\end{aligned}$$

The corruption of messages does not generate consistent fail synchronisation responses to the challenge.

Assumption 4.1.

$$\begin{aligned}
\mathcal{N}_{normal}^{Ass} &:\Leftrightarrow \\
&[\wedge UAR_s(chall, SN) \wedge UASF_r(SynResp, SN) \\
&\quad \wedge \neg UASF_s(SynResp, SN)] \\
&\Rightarrow \neg \text{verif}(SynResp, \underline{Rand}(AV))
\end{aligned}$$

We will assume that during each non-stutter step of the communication channel, either the channel is OK or there is a corruption or a loss of a challenge/response:

$$\begin{aligned}
\mathcal{N}_{normal}^{CC} &:\Leftrightarrow \\
&\wedge \forall_{SN, SN_1} Comm(SN) \wedge Comm(SN_1) \Rightarrow SN = SN_1 \\
&\wedge UAR_s \Rightarrow OKR \vee CorrR \vee LossR \\
&\wedge UAR_r \Rightarrow OKR \vee CorrR \vee LossR \\
&\wedge UAS_s \vee UAJ_s \vee UASF_s \Rightarrow OKS \vee CorrS \vee LossS \\
&\wedge UAS_r \vee UAJ_r \vee UASF_r \Rightarrow OKS \vee CorrS \vee LossS \\
&\wedge \mathcal{N}_{normal}^{Ass}
\end{aligned}$$

4.5 The Mobile Station

Definition 4.1. *The system is during the lifetime of the USIM if the number of User Authentication Responses is less than $SQNmax/\Delta$:*

$$Lifetime :\Leftrightarrow n_{UAS, s} \leq SQNmax/\Delta$$

When the mobile station receives a USER AUTHENT. REQUEST, if the challenge is consistent and synchronous. it updates the variable *la_chall* and sends the corresponding response, USER AUTHENT. RESPONSE. But if the challenge is not consistent, it sends a USER AUTHENT. REJECT, and if the challenge is not synchronous,

it sends a USER AUTHENT. RESPONSE: The only reason for updating the variable la_chall is the one given above:

$$\begin{aligned}
\mathcal{N}_{normal}^{MS} &:\Leftrightarrow \\
&\wedge \text{UAR}_R(\text{chall}, \text{SN}) \Rightarrow \wedge \text{cons}(\text{chall}) \wedge \text{synchron}(seq_{MS}, \underline{Seq}(\text{chall})) \\
&\quad \Rightarrow \text{UAS}_S(\underline{Resp}(\text{chall}), \text{SN}) \\
&\quad \wedge \neg \text{cons}(\text{chall}) \\
&\quad \Rightarrow \text{UAJ}_S(\underline{RejResp}(\text{chall}), \text{SN}) \\
&\quad \wedge \text{cons}(\text{chall}) \wedge \neg \text{synchron}(seq_{MS}, \underline{Seq}(\text{chall})) \\
&\quad \Rightarrow \text{UASF}_S(\underline{SynResp}(la_chall, \text{chall}), \text{SN}) \\
&\wedge \text{UAS}_S \vee \text{UAJ}_S \vee \text{UASF}_S \Rightarrow \text{UAR}_R \\
&\wedge \text{UAR}_R(\text{chall}, \text{SN}) \wedge \text{UAS}_S \Rightarrow la_chall' = \text{chall} \\
&\wedge \text{UAR}_R(\text{chall}, \text{SN}) \wedge \neg \text{UAS}_S \Rightarrow la_chall' = la_chall \\
&\wedge la_chall \Downarrow \Rightarrow \text{UAS}_S(\text{resp}, \text{SN}) \\
&\wedge \text{Lifetime}'
\end{aligned}$$

5 Definition of Normal Behavior

Definition 5.1. An AV is called generated (by the home environment) if the home environment has sent this AV in an Authentication Data Response. Formally, the variable Gen , of type $\wp(\mathcal{AV})$ is defined by the temporal formula:

$$\begin{aligned}
\mathcal{A}_{normal}^{Gen} &:\Leftrightarrow \\
&\wedge Gen = \emptyset \\
&\wedge \Box(\wedge Gen \Downarrow \Rightarrow \exists_{AVs_new, SN} \text{ADS}(AVs_new, SN) \wedge AVs_new \neq \epsilon \\
&\quad \wedge \exists_{AVs_new, SN} \text{ADS}(AVs_new, SN) \Rightarrow Gen' = Gen \cup AVs_new)
\end{aligned}$$

Definition 5.2. An AV copy is lost if it is either:

1. lost or corrupted in the communication Channel from the SN to the USIM, or
2. lost or intentionally discarded during a Location Update

Formally, the variable $Lost$, of type $\wp(\mathcal{AV})$ is defined by:

$$\begin{aligned}
\mathcal{A}_{normal}^{Lost} &:\Leftrightarrow \\
&\wedge Lost = \emptyset \\
&\wedge \Box(\wedge Lost \Downarrow \Rightarrow \vee \text{UAR}_S \wedge (\text{CorrR} \vee \text{LossR}) \\
&\quad \vee \text{LUR}(\text{SN}, \text{SN}_1) \wedge \neg \text{MvAV}(\text{SN}, \text{SN}_1) \\
&\quad \wedge \text{UAR}_S(\underline{Chall}(\text{AV}), \text{SN}) \wedge (\text{CorrR} \vee \text{LossR}) \\
&\quad \Rightarrow Lost' = Lost \cup \{\text{AV}\} \\
&\quad \wedge \text{LUR}(\text{SN}, \text{SN}_1) \wedge \neg \text{MvAV}(\text{SN}, \text{SN}_1) \Rightarrow \\
&\quad \quad Lost' = Lost \cup DB(\text{SN}))
\end{aligned}$$

It is not necessary to explicitly model losses of AVs (1.) inside of an SN or during the (2.) communication between the home environment and the serving network or

(3.) between two serving networks (during a MvAV). From the point of view of the **HE** and the **MS**, at least, it is equivalent to loose the AV in any one of those three situations or to loose it in the communication Channel from the SN to the USIM.

Definition 5.3. An AV copy is used if its challenge was sent in an authentication request. More precisely, the variable *Used*, of type $\wp(\mathcal{AV})$ is defined by:

$$\begin{aligned} \mathcal{A}_{normal}^{Used} : &\Leftrightarrow \\ &\wedge Used = \emptyset \\ &\wedge \Box(\wedge Used \Downarrow \Rightarrow UAR_s \\ &\quad \wedge UAR_s(\underline{Chall}(\mathbf{AV}), SN) \Rightarrow Used' = Used \cup \{\mathbf{AV}\} \end{aligned}$$

Definition 5.4. An AV copy is accepted if its challenge was accepted by the mobile station. Accepted, of type $\wp(\mathcal{AV})$ is defined by:

$$\begin{aligned} \mathcal{A}_{normal}^{Accepted} : &\Leftrightarrow \\ &\wedge Accepted = \emptyset \\ &\wedge \Box(\wedge Accepted \Downarrow \Rightarrow la_chal \Downarrow \\ &\quad \wedge la_chal \Downarrow \Rightarrow Accepted' = Accepted \cup \\ &\quad \quad \{\mathbf{AV} \in Gen' \mid \underline{Chall}(\mathbf{AV}) = la_chal'\}) \end{aligned}$$

Definition 5.5. An unused AV copy is usable if its location is the current SN where the user is registered (or where the user was last registered), that is, it is an element of $DB(last_SN)$.

Definition 5.6. The sequence numbers seq_{MS} in the USIM and seq_{HE} in the home environment are called synchronous iff $synchron(seq_{MS}, seq_{HE} + 1)$. In this case we call the system weakly-synchronous:

$$WeakSynchron : \Leftrightarrow synchron(seq_{MS}, seq_{HE} + 1)$$

Definition 5.7. An unused AV copy is called synchronous (with respect to seq_{MS}) if $synchron(seq_{MS}, \underline{Seq}(\mathbf{AV}))$

Definition 5.8. The system is strongly-synchronous if it is weakly-synchronous and all usable AV copies are also synchronous (w.r. to seq_{MS}).

$$StrongSynchron : \Leftrightarrow WeakSynchron \wedge \forall_{\mathbf{AV} \in DB(last_SN)} synchron(seq_{MS}, \underline{Seq}(\mathbf{AV}))$$

Definition 5.9. Let $\mathcal{A} \subseteq \mathcal{AV}$. \mathcal{A} is said to have no m consecutive AVs or to be interrupted each m elements iff between any two elements of \mathcal{A} whose sequence numbers differ by at least $m - 1$ there is a number k between those two sequence numbers such that no element of \mathcal{A} has k as its sequence number.

$$\begin{aligned} Interr_m(\mathcal{A}) : &\Leftrightarrow \\ &\forall_{\mathbf{AV}_1, \mathbf{AV}_2 \in \mathcal{A}} (\underline{Seq}(\mathbf{AV}_2) - \underline{Seq}(\mathbf{AV}_1) \geq m - 1 \Rightarrow \\ &\quad \exists_k (\underline{Seq}(\mathbf{AV}_1) < k < \underline{Seq}(\mathbf{AV}_2) \wedge \forall_{\mathbf{AV} \in \mathcal{A}} \underline{Seq}(\mathbf{AV}) \neq k)) \end{aligned}$$

Definition 5.10. "Normal Behavior Scenario": The system behaves normally (from the beginning on) if for any $(\Delta - N - 1)$ AVs in sequence, at least 1 AV is not lost, and on each transition step, the formulas $\mathcal{N}_{normal}^{LU}$, $\mathcal{N}_{normal}^{SN}$, $\mathcal{N}_{normal}^{HE}$, $\mathcal{N}_{normal}^{CC}$, and $\mathcal{N}_{normal}^{MS}$ hold:

$$\begin{aligned} \mathcal{N}_{normal}^{Step} : &\Leftrightarrow \mathcal{N}_{normal}^{LU} \wedge \mathcal{N}_{normal}^{SN} \wedge \mathcal{N}_{normal}^{HE} \wedge \mathcal{N}_{normal}^{CC} \wedge \mathcal{N}_{normal}^{MS} \\ \mathcal{A}_{normal} : &\Leftrightarrow \\ &Init \wedge \mathcal{A}_{normal}^{interleave} \wedge \mathcal{A}_{normal}^{CurrSN} \wedge \mathcal{A}_{normal}^{LastSN} \wedge \mathcal{A}_{normal}^{Gen} \wedge \mathcal{A}_{normal}^{Lost} \wedge \mathcal{A}_{normal}^{Used} \\ &\wedge \Box(\mathcal{N}_{normal}^{Step} \wedge Interr_{\Delta - N - 1}(Lost')) \end{aligned}$$

6 Transitions of the incorrect System

6.1 Events: more Transitions

<i>Message or Event</i>	<i>Trans. Pred.</i>	<i>Param. Name</i>	<i>Param. Type</i>	<i>Var. Name</i>
ERROR HE	XHE	Failure	\mathcal{FAIL}	n_{XHE}
ERROR SN	XSN	SN Failure	\mathcal{SN} \mathcal{FAIL}	n_{XSN}
ERROR LU	XLU	SN Failure	\mathcal{SN} \mathcal{FAIL}	n_{XLU}

Table 3: Failure Events

Definition 6.1. (The Failure Events)

$$\begin{aligned}
\text{XHE(Failure)} &:\Leftrightarrow n_{\text{XHE}}(\text{Failure})\uparrow \\
\text{XSN(SN, Failure)} &:\Leftrightarrow n_{\text{XSN}}(\text{SN, Failure})\uparrow \\
\text{XLU(SN, Failure)} &:\Leftrightarrow n_{\text{XLU}}(\text{SN, Failure})\uparrow
\end{aligned}$$

We also use conventions similar to the ones in Conventions 3.1 and 3.2. We do not write them explicitly.

Some remarks to the assumptions/failure models: Most race conditions (the non-intended ordering of the processing of events due to concurrency and communication delays) are non-critical. This is due to the fact that the protocol is constructed as a set of requests and responses (or timeouts). In our modeling we use as atomic granularity *complete* actions (request+response or time-out). Nevertheless it is possible to formulate race conditions as the simultaneous performance of two actions (that should happen in order and such that the simultaneous performance is not equivalent to any of the two orderings) or by adding events (like $\text{XLU}(\text{SN, Race})$), that have some unexpected consequences.

In our case, the unexpected consequence of $\text{XLU}(\text{SN, Race})$ is that the USIM may change its location simultaneously to a ADR (or equivalently, to an ADS).

Also in that case, the data-base of authentication vectors may have been updated in an unexpected order. There is no real need for explicitly requiring this (as a single transition step) since it is equivalent to a sequential composition of the transitions (in any order): update the database DB correctly once, loose, eventually several times, the order of the DB (event: $\text{XSN}(\text{SN, DB})$) and loose AVs (event: $\text{XSN}(\text{SN, Loss})$).

Another more drastic but simple way of modeling this type of situation, allowing even more strange race conditions in which many different SNs are involved (but not changing our properties or proofs), is to allow in the event $\text{XSN}(\text{DB})$ (without a parameter SN) to mix the different DB s of the different SNs in an arbitrary way:

$$\text{XSN}(\text{DB}) \Rightarrow \bigcup_{\text{SN}} \text{Set}(DB'(\text{SN})) = \bigcup_{\text{SN}} \text{Set}(DB(\text{SN}))$$

instead of, as we will have now (see the definition of $\mathcal{N}_{critical}^{SN}$):

$$\text{XSN}(\text{SN, DB}) \Rightarrow \text{Set}(DB'(\text{SN})) = \text{Set}(DB(\text{SN}))$$

Component	Assumption/Failure Model	Description
USIM	(only case)	The USIM always works correctly. The lifetime of the USIM is not exceeded. (See Def. 4.1).
SN	SN 1. No failure	SN works correctly
	SN 2. AV loss	Loss or corruption of AVs (event: XSN(Loss))
	SN 3. AV disordering	Disordering of AVs (event: XSN(DB))
	SN 4. Crash SN	Use of old AVs (event: XSN(Crash))
	SN 5. SN is compromised	AVs are stolen (event: XSN(Steal))
HE	HE 1. No failure	HE works correctly
	HE 2. DB-failures	SQN is reset to an older value (event: XHE(DB))
	HE 3. HE crash	Critical failures: SQN is set to an arbitrary value (event: XHE(Crash))
	HE 4. HE is compromised	An attacker sets SQN to an arbitrarily chosen value; then AVs are generated and stolen and eventually SQN is set to a new less suspicious value. (But: not generated AVs are never compromised) (event: XHE(Steal))

Table 4: Assumptions and Failure Models. Part I

Component	Assumption/Failure	Description
Transmission channel (between SN and USIM)	Ch 1. normal situation	In a sequence of transmissions, a certain maximal number of consecutive failures happen (loss or corruption of messages)
	Ch 2. critical situation, probably due to attacks	A huge amount of consecutive messages are lost or corrupted
	Ch 3. replay attacks	Old (=seen) messages are inserted
	Ch 4. complex attacks	Messages using unseen AVs are inserted. Those AVs have been stolen.
Location Update	LU 1. normal situation	Cancel location implies all AVs are deleted. With a Location update request all old AVs are deleted, fresh AVs are requested from the old SN or from the HE/AuC. No race condition happens
	LU 2. failure	After a Location update request old AVs are still present and will be used (event: XLU(SN,DB))
	LU 3. race conditions	There are several race conditions, for instance: when an SN asks for Authentication Data, ADR, (and in particular, after a synchronisation failure is detected), the USIM changes SN (location update) and the new SN collects new AVs, before the HE is able to process the old ADR. (event: XLU(SN,Race))

Table 5: Assumptions and Failure Models: Part II

disordering the DB of only one SN independently of all other SN s.

It is in principle possible that several errors happen within the same transition, but sometimes the specifications of them contradict each other. In any case it is always possible that errors occur immediately after another.

For simplicity, we defined all three types of error (XHE,XSN,XLU) as being of the same type. But each one may happen only for certain parameter values:

$$\begin{aligned} \mathcal{A}_{critical}^{interleave} &:\Leftrightarrow \mathcal{A}_{normal}^{interleave} \wedge \\ &\Box(\wedge \text{XHE(Failure)} \Rightarrow \text{Failure} \in \{\text{DB, Crash, Steal}\} \\ &\quad \wedge \text{XSN(SN, Failure)} \Rightarrow \text{Failure} \in \{\text{Loss, DB, Crash, Steal}\} \\ &\quad \wedge \text{XLU(SN, Failure)} \Rightarrow \text{Failure} \in \{\text{DB, Race}\}) \end{aligned}$$

6.2 Changing the Location

Recall the definition of $curr_SN : \wp(\mathcal{SN})$ given in Def. 4.1. This definition imposes no restriction in our specification and remains as it is. The definition of $last_SN : \mathcal{SN}$ will also be left unchanged: the value of $last_SN$ is of no interest to us when $curr_SN$ is a set with two or more elements. But as soon as $curr_SN$ is a singleton or empty, $last_SN$ has the meaning that we intend: either is $curr_SN = \{last_SN\}$ or it is the last SN where the user was registered.

$$\begin{aligned} \mathcal{A}_{incorr}^{CurrSN} &:\Leftrightarrow \mathcal{A}_{critical}^{CurrSN} :\Leftrightarrow \mathcal{A}_{normal}^{CurrSN} \\ \mathcal{A}_{incorr}^{LastSN} &:\Leftrightarrow \mathcal{A}_{critical}^{LastSN} :\Leftrightarrow \mathcal{A}_{normal}^{LastSN} \end{aligned}$$

$$\begin{aligned} \mathcal{N}_{critical}^{LU} &:\Leftrightarrow \\ &\wedge \text{LUR}(\text{SN}, \text{SN}_1) \wedge \neg \text{XLU}(\text{SN}, \text{DB}) \Rightarrow \text{MvAV}(\text{SN}, \text{SN}_1) \vee \text{DB}'(\text{SN}_1) = \epsilon \\ &\wedge \text{MvAV}(\text{SN}, \text{SN}_1) \Rightarrow \text{LUR}(\text{SN}, \text{SN}_1) \\ &\wedge (\text{ADS} \wedge \neg \exists_{\text{SN}} \text{XLU}(\text{SN}, \text{Race})) \Rightarrow curr_SN' = curr_SN \\ &\wedge \text{MvAV}(\text{SN}, \text{SN}_1) \Rightarrow \wedge \text{DB}'(\text{SN}_1) = \text{DB}(\text{SN}) \\ &\quad \wedge \text{DB}'(\text{SN}) = \epsilon \\ &\quad \wedge \forall_{\text{SN}_2} (\text{SN}_2 \neq \text{SN} \wedge \text{SN}_2 \neq \text{SN}_1 \Rightarrow \\ &\quad \quad \text{DB}'(\text{SN}_2) = \text{DB}'(\text{SN}_2)) \end{aligned}$$

The definition of $\mathcal{N}_{critical}^{LU}$ is very close to the one of $\mathcal{N}_{normal}^{LU}$. There we had (rewriting a bit the original formula):

$$\text{LUR}(\text{SN}, \text{SN}_1) \wedge \neg \text{MvAV}(\text{SN}, \text{SN}_1) \Rightarrow \text{DB}'(\text{SN}_1) = \epsilon$$

but now, if $\text{XLU}(\text{SN}, \text{DB})$ happens, $\text{LUR}(\text{SN}, \text{SN}_1) \wedge \neg \text{MvAV}(\text{SN}, \text{SN}_1)$ may imply $\text{DB}'(\text{SN}_1) \neq \epsilon$ (thus old AVs may be used: LU 2.). It is not necessary to explicitly state what happens if $\text{LUR}(\text{SN}, \text{SN}_1) \wedge \text{XLU}(\text{SN}, \text{DB})$: either $\text{MvAV}(\text{SN}, \text{SN}_1)$ (in which case DB changes in the prescribed way) or $DB(\text{SN}_1)$ does not change, unless there is another reason for changing $DB'(\text{SN}_1)$ (those reasons are given in the definition of $\mathcal{N}_{critical}^{SN}$ after $DB(\text{SN}) \Rightarrow \dots$).

The other difference to $\mathcal{N}_{normal}^{LU}$ is that if the race condition happens, then while ADS is performed, $(\text{ADS} \wedge \neg \exists_{\text{SN}} \text{XLU}(\text{SN}, \text{Race}))$, then it may not be excluded that either a LUR or a $CANLOC$ happen, the mobile station thus changing the location.

6.3 The Serving Network

$$\begin{aligned}
\mathcal{N}_{critical}^{SN} : \Leftrightarrow & \\
& \wedge \text{ADR}_0(\text{SN}) \Rightarrow \text{DB}(\text{SN}) = \epsilon \wedge \text{SN} \in \text{curr_SN} \\
& \wedge \text{ADR}_1(\text{SynResp}, \text{Rand}, \text{SN}) \Rightarrow \\
& \quad \wedge \text{UASF}_R(\text{SynResp}, \text{SN}) \\
& \quad \wedge \text{SN} \in \text{curr_SN} \\
& \quad \wedge \exists_{AV} (\text{UAR}_s(\underline{\text{Chall}}(\text{AV}), \text{SN}) \wedge \text{Rand} = \underline{\text{Rand}}(\text{AV})) \\
& \wedge \text{ADS}(\text{AVs_new}, \text{SN}) \Rightarrow \wedge \text{AVs_new} \neq \epsilon \Rightarrow \text{DB}'(\text{SN}) = \text{AVs_new} \\
& \quad \wedge \text{AVs_new} = \epsilon \Rightarrow \text{DB}'(\text{SN}) = \text{DB}(\text{SN}) \\
& \wedge \text{UAR}_s(\text{chall}, \text{SN}) \wedge \neg \text{XSN}(\text{SN}, \text{Loss}) \Rightarrow \\
& \quad \wedge \text{SN} \in \text{curr_SN} \wedge \text{DB}(\text{SN}) \neq \epsilon \\
& \quad \wedge \text{DB}'(\text{SN}) = \text{Tail}(\text{DB}(\text{SN})) \\
& \quad \wedge \text{chall} = \underline{\text{Chall}}(\text{Head}(\text{DB}(\text{SN}))) \\
& \wedge \text{XSN}(\text{SN}, \text{Crash}) \Rightarrow \text{UAR}_s \\
& \wedge \text{UAR}_s(\text{chall}, \text{SN}) \wedge \text{XSN}(\text{SN}, \text{Crash}) \Rightarrow \\
& \quad \exists_{AV \in \text{Used}} \text{chall} = \underline{\text{Chall}}(\text{AV}) \\
& \wedge \text{XSN}(\text{SN}, \text{DB}) \Rightarrow \text{Set}(\text{DB}'(\text{SN})) = \text{Set}(\text{DB}(\text{SN})) \\
& \wedge \text{XSN}(\text{SN}, \text{Loss}) \Rightarrow \wedge \text{Set}(\text{DB}'(\text{SN})) \subseteq \text{Set}(\text{DB}(\text{SN})) \\
& \quad \wedge \text{AV}_1 \ll_{\text{DB}'(\text{SN})} \text{AV}_2 \Rightarrow \text{AV}_1 \ll_{\text{DB}(\text{SN})} \text{AV}_2 \\
& \wedge \text{DB}(\text{SN}) \Downarrow \Rightarrow \vee \exists_{\text{SN}_1} \text{LUR}(\text{SN}_1, \text{SN}) \wedge \neg \text{XLU}(\text{SN}_1, \text{DB}) \\
& \quad \vee \text{XSN}(\text{SN}, \text{DB}) \vee \text{XSN}(\text{SN}, \text{Loss}) \\
& \quad \vee \exists_{\text{AVs_new}, \text{SN}} \text{ADS}(\text{AVs_new}, \text{SN}) \wedge \text{AVs_new} \neq \epsilon \\
& \quad \vee \exists_{\text{chall}, \text{SN}} \text{UAR}_s(\text{chall}, \text{SN}) \wedge \neg \text{XSN}(\text{SN}, \text{Loss}) \\
& \quad \vee \exists_{\text{SN}_1} \text{MvAV}(\text{SN}, \text{SN}_1) \\
& \quad \vee \exists_{\text{SN}_1} \text{MvAV}(\text{SN}_1, \text{SN}) \\
& \wedge [\wedge \text{UASF}_R(\text{SynResp}, \text{SN}) \\
& \quad \wedge \text{SN} \in \text{curr_SN} \\
& \quad \wedge \text{UAR}_s(\underline{\text{Chall}}(\text{AV}), \text{SN}) \\
& \quad \wedge \text{Rand} = \underline{\text{Rand}}(\text{AV})] \Rightarrow \text{ADR}_1(\text{SynResp}, \text{Rand}, \text{SN})
\end{aligned}$$

6.4 The Home Environment

In the real system it seems to be the case that if a race condition happens:

$$(\text{ADR}_0 \vee \text{ADR}_1) \wedge \text{XLU}(\text{SN}, \text{Race}) \wedge \text{LUR}(\text{SN}, \text{SN}_1)$$

then a $\text{CANLOC}(\text{SN})$ can be produced, instead of the ADS expected by the serving network. But we insist that $(\text{ADR}_0 \vee \text{ADR}_1) \Rightarrow \text{ADS}$. We model the described situation as follows: first send a $\text{ADS}(\text{AVs_new}, \text{SN})$ with $\text{AVs_new} = \epsilon$ and then send a CANLOC . This sequence is equivalent to just sending one CANLOC . Notice that our specification does not constrain at all the occurrences of CANLOC : they may happen anytime. (They are seen as inputs to the system).

It is also assumed that AVs which have not been generated can not be stolen (the

code for the generation of AVs is secure).

$$\begin{aligned}
\mathcal{N}_{critical}^{HE} : \Leftrightarrow & \exists_{seq_{he}} [\\
& \wedge \text{ADS}(\text{AVs_new}, \text{SN}) \Rightarrow \vee \text{ADR}_0(\text{SN}) \\
& \quad \vee \exists_{\text{SynResp}, \text{Rand}} \text{ADR}_1(\text{SynResp}, \text{Rand}, \text{SN}) \\
& \wedge (\text{ADR}_0 \vee \text{ADR}_1) \Rightarrow \text{ADS} \\
& \wedge \text{ADR}_0 \Rightarrow seq_{he} = seq_{HE} \\
& \wedge \text{ADR}_1(\text{SynResp}, \text{Rand}, \text{SN}) \Rightarrow \\
& \quad \wedge [\text{verif}(\text{SynResp}, \text{Rand}) \wedge \\
& \quad \quad \neg \text{synchron}_1(\underline{Seq}_{MS}(\text{SynResp}), seq_{HE})] \Rightarrow seq_{he} = \underline{Seq}_{MS}(\text{SynResp}) \\
& \quad \wedge [\neg \text{verif}(\text{SynResp}, \text{Rand}) \vee \\
& \quad \quad \text{synchron}_1(\underline{Seq}_{MS}(\text{SynResp}), seq_{HE})] \Rightarrow seq_{he} = seq_{HE} \\
& \wedge \text{ADS}(\text{AVs_new}, \text{SN}) \Rightarrow \\
& \quad \wedge \neg \text{XLU}(\text{SN}, \text{Race}) \Rightarrow \text{AVs_new} \neq \epsilon \\
& \quad \wedge \text{AV} \in \text{AVs_new} \Rightarrow \text{cons}(\text{AV}) \\
& \quad \wedge \forall_{\text{AV}_1, \text{AV}_2 \in \text{AVs_new}} (\text{AV}_1 \prec \text{AV}_2 \Leftrightarrow \text{AV}_1 \ll \text{AV}_2) \\
& \quad \wedge \forall_{\text{AV} \in \text{AVs_new}} (seq_{he} < \underline{Seq}(\text{AV}) \leq seq'_{HE}) \\
& \quad \wedge \forall_{i \in \mathbb{N}} \exists_{\text{AV} \in \text{AVs_new}} (seq_{he} < i \leq seq'_{HE} \Rightarrow \underline{Seq}(\text{AV}) = i) \\
& \quad \wedge seq'_{HE} - seq_{he} \leq N \\
& \wedge \text{XHE}(\text{DB}) \Rightarrow seq_{HE}' < seq_{HE} \\
& \wedge seq_{HE} \uparrow \Rightarrow \vee \exists_{\text{AVs_new}, \text{SN}} \text{ADS}(\text{AVs_new}, \text{SN}) \wedge \text{AVs_new} \neq \epsilon \\
& \quad \vee \text{XHE}(\text{DB}) \\
& \quad \vee \text{XHE}(\text{Steal}) \\
& \quad \vee \text{XHE}(\text{Crash})]
\end{aligned}$$

Notice that $\text{XHE}(\text{Steal})$ or $\text{XHE}(\text{Crash})$ do not impose any restriction on the value of seq_{HE}' . Therefore, after this sort of failures the sequence number of the home environment may assume an arbitrary value.

6.5 The Communication Channel

The definitions of OKR , $CorrR$, $LossR$, OKS , $CorrS$, and $LossS$ were given in Section 4.4. These definitions are still valid for the incorrect and the critical system. As before, the message $\text{USER AUTHENT. REQUEST}$ may be received correctly (OKR), or it may be corrupted during the transmission ($CorrR$), or it may get lost ($LossR$). But now there is one possibility more: it may be also replaced by another $\text{USER AUTHENT. REQUEST}$ with another challenge ($ATTR$).

$$\begin{aligned}
ATTR : \Leftrightarrow & \exists_{\text{chall}, \text{SN}} \wedge \text{UAR}_s(\text{chall}, \text{SN}) \\
& \wedge \exists_{\text{chall}_1 \neq \text{chall}} \text{cons}(\text{chall}_1) \wedge \text{UAR}_r(\text{chall}_1, \text{SN})
\end{aligned}$$

Notice that the following is a tautology:

$$\begin{aligned}
\text{UAR}_s(\text{chall}, \text{SN}) \Rightarrow & \vee \text{UAR}_r(\text{chall}, \text{SN}) \\
& \vee \exists_{\text{chall}_1} \neg \text{cons}(\text{chall}_1) \wedge \text{UAR}_r(\text{chall}_1, \text{SN}) \\
& \vee \neg \text{UAR}_r(\text{SN}) \\
& \vee \exists_{\text{chall}_1 \neq \text{chall}} \text{cons}(\text{chall}_1) \wedge \text{UAR}_r(\text{chall}_1, \text{SN})
\end{aligned}$$

Thus, $UAR_s \Rightarrow OKR \vee CorrR \vee LossR \vee ATTR$ is a tautology.

There is another form of attack, $ATTR_i$, the *insertion* of a message that was not sent. In this situation, the only interesting case is when the inserted challenge is consistent:

$$ATTR_i : \Leftrightarrow \exists_{\text{chall}, \text{SN}} \wedge UAR_R(\text{chall}, \text{SN}) \wedge \text{cons}(\text{chall}) \\ \wedge \neg UAR_s$$

On the other direction, the message USER AUTHENT. RESPONSE may be received correctly (OKS), or it may be corrupted during the transmission ($CorrS$), or it may get lost ($LossS$), or it may be replaced by another USER AUTHENT. RESPONSE with another response ($ATTR$). Notice that in the definition of $\mathcal{N}_{normal}^{CC}$, if a message was received, then a corresponding message was also sent (perhaps with different parameter values, they can be corrupted). For instance, if UAS_R happens, then either OKR or $CorrR$ or $LossR$ happens, and in any case, UAS_s happens as well. This is not true anymore. Notice that we do not have to model extra an attack $ATTS$, since it is indistinguishable from a corruption $CorrS$. (In the other direction $ATTR$ is needed, since $CorrR$ implies that the corrupted challenge is inconsistent). The insertion attack for messages from the mobile station to the service network are only interesting when the service network has issued an authentication request (else the insertion of the message has no consequences):

$$ATTS_i(\text{SN}) : \Leftrightarrow \wedge \exists_{\text{chall}} UAR_s(\text{chall}, \text{SN}) \\ \wedge \neg \exists_{\text{resp}} UAS_s(\text{resp}, \text{SN}) \\ \wedge \neg \exists_{\text{RejResp}} UAJ_s(\text{RejResp}, \text{SN}) \\ \wedge \neg \exists_{\text{SynResp}} UASF_s(\text{SynResp}, \text{SN}) \\ \wedge \vee \exists_{\text{resp}} UAS_R(\text{resp}, \text{SN}) \\ \vee \exists_{\text{RejResp}} UAJ_R(\text{RejResp}, \text{SN}) \\ \vee \exists_{\text{SynResp}} UASF_R(\text{SynResp}, \text{SN}) \\ ATTS_i : \Leftrightarrow \exists_{\text{SN}} ATTS_i(\text{SN})$$

The attacker is not able to generate consistent challenges that he has not seen, that is, either have been transmitted already, or he has stolen. (The definition of *Stolen* is given in Definition 5.2).

Assumption 6.1.

$$\mathcal{N}_{critical}^{Ass_1} : \Leftrightarrow \\ [UAR_R(\text{chall}, \text{SN}) \wedge \neg UAR_s(\text{chall}, \text{SN}) \wedge \text{cons}(\text{chall})] \\ \Rightarrow \exists_{\text{AV} \in \text{Stolen} \cup \text{Used}} \text{chall} = \underline{\text{Chall}}(\text{AV})$$

The attacker is not able to generate consistent responses to challenges that he has not seen.

Assumption 6.2.

$$\mathcal{N}_{critical}^{Ass_2} : \Leftrightarrow \\ [UAR_s(\text{chall}, \text{SN}) \wedge \neg UAS_s(\text{resp}, \text{SN}) \wedge UAS_R(\text{resp}, \text{SN}) \wedge \text{cons}(\text{chall}, \text{resp})] \\ \Rightarrow \exists_{\text{AV} \in \text{Stolen} \cup \text{Used}} \text{chall} = \underline{\text{Chall}}(\text{AV}) \wedge \text{resp} = \underline{\text{Resp}}(\text{AV})$$

The attacker is not able to generate consistent fail synchronisation responses to fresh challenges.

Assumption 6.3.

$$\begin{aligned}
\mathcal{N}_{critical}^{Ass_3} : \Leftrightarrow & \\
& [\wedge \text{UAR}_s(\text{chall}, \text{SN}) \wedge \text{UASF}_R(\text{SynResp}, \text{SN}) \\
& \wedge \neg \text{UASF}_s(\text{SynResp}, \text{SN}) \wedge \text{verif}(\text{SynResp}, \underline{\text{Rand}}(\text{AV}))] \\
& \Rightarrow (\text{AV} \in \text{Stolen} \cup \text{Used}) \wedge \text{SynResp} = \underline{\text{SynResp}}(\text{AV})
\end{aligned}$$

Those assumptions are the specification of $\mathcal{N}_{critical}^{CC}$:

$$\mathcal{N}_{critical}^{CC} : \Leftrightarrow \mathcal{N}_{critical}^{Ass_1} \wedge \mathcal{N}_{critical}^{Ass_2} \wedge \mathcal{N}_{critical}^{Ass_3}$$

6.6 The Mobile Station

The mobile station is assumed to work always correctly, therefore,

$$\mathcal{N}_{critical}^{MS} : \Leftrightarrow \mathcal{N}_{normal}^{MS}$$

7 Definition of Incorrect Behavior

Definition 7.1. *The stealing of AVs generates a clone (not a "copy") of an AV. Stolen^3 , the set of clones, is defined by the formulas:*

$$\begin{aligned}
\text{Stolen} &:= \text{Stolen}_{HE} \cup \text{Stolen}_{SN} \\
\text{Stolen}_{HE} &= \emptyset \wedge \Box(\wedge \text{Stolen}_{HE} \uparrow \Rightarrow \text{XHE}(\text{Steal}) \\
&\quad \wedge \text{XHE}(\text{Steal}) \Rightarrow \text{Stolen}_{HE}' \supseteq \text{Stolen}_{HE}) \\
\text{Stolen}_{SN} &= \emptyset \wedge \Box(\wedge \text{Stolen}_{SN} \uparrow \Rightarrow \text{XSN}(\text{SN}, \text{Steal}) \\
&\quad \wedge \text{XSN}(\text{SN}, \text{Steal}) \Rightarrow \\
&\quad \text{Stolen}_{SN} \subseteq \text{Stolen}_{SN}' \subseteq \text{Stolen}_{SN} \cup \text{DB}(\text{SN}))
\end{aligned}$$

Definition 7.2. *As before (Def. 5.5), if curr_SN is a singleton or empty, an unused AV copy is usable if its location is last_SN , the current SN where the user is registered (or where the user was last registered), that is, it is an element of $\text{DB}(\text{last_SN})$. If curr_SN contains more than one element, then an unused AV is usable if its location is contained in curr_SN , that is, it is an element of $\cup_{\text{SN} \in \text{curr_SN}} \text{DB}(\text{SN})$.*

In the Definition 5.2, we have defined the variable *Lost*, the set of lost authentication vectors. This definition is now extended to the case where the protocol is not running under normal conditions, but under incorrect or critical ones. Now, the system may also loose AVs through the event XSN, or through attacks. Notice that also the disordering of AVs (or, if you prefer, the usage of AVs in disorder) leads to losing AVs.

Definition 7.3. *An AV copy is lost if it is either:*

1. *lost or corrupted by an error in SN (SN 2. or SN 3.)*
2. *lost or corrupted in the communication Channel between the SN and the USIM, perhaps also due to an attack (Ch. 1 or Ch. 2)*

³In our formal specification we do not distinguish between AVs and *occurrences* of AVs. Thus, in the formal specification one AV may be at the same time in *Stolen* and in *Used* or *Lost*.

3. *lost or intentionally discarded during a Location Update (typically LU 1, but also LU 2 and LU 3)*

Formally, the variable *Lost*, of type $\wp(\mathcal{AV})$ is defined by:

$$\begin{aligned}
\mathcal{A}_{critical}^{Lost} : \Leftrightarrow & \\
& \wedge \text{Lost} = \emptyset \\
& \wedge \Box (\wedge \text{Lost} \Rightarrow \vee \text{UAR}_s \wedge \neg OKR \\
& \quad \vee \text{LUR}(\text{SN}, \text{SN}_1) \wedge \neg \text{MvAV}(\text{SN}, \text{SN}_1) \\
& \quad \vee \exists_{\text{SN}} \text{XSN}(\text{SN}, \text{Loss}) \\
& \quad \vee \exists_{\text{SN}} \text{XSN}(\text{SN}, \text{DB}) \\
& \wedge \text{UAR}_s(\underline{\text{Chall}}(\text{AV}), \text{SN}) \wedge \neg OKR \\
& \quad \Rightarrow \text{Lost}' = \text{Lost} \cup \{\text{AV}\} \\
& \wedge \text{LUR}(\text{SN}, \text{SN}_1) \wedge \neg \text{MvAV}(\text{SN}, \text{SN}_1) \Rightarrow \\
& \quad \text{Lost}' = \text{Lost} \cup \text{DB}(\text{SN}) \\
& \wedge \text{XSN}(\text{SN}, \text{Loss}) \Rightarrow \text{Lost}' = \text{Lost} \cup (\text{DB}(\text{SN}) \setminus \text{DB}'(\text{SN})) \\
& \wedge \text{XSN}(\text{SN}, \text{DB}) \Rightarrow \text{Lost}' = \text{Lost} \cup \text{DB}(\text{SN}))
\end{aligned}$$

This definition of *Lost* is only one of several possible choices. We could say that if $\text{XSN}(\text{SN}, \text{DB})$ happens, not all AVs in $\text{DB}(\text{SN})$ are lost, only those AV for which there is an AV_1 in $\text{DB}'(\text{SN})$, such that AV_1 is left of AV (it will be used earlier than AV) but AV_1 has a larger sequence number than AV:

$$\begin{aligned}
& \text{XSN}(\text{SN}, \text{DB}) \Rightarrow \\
& \text{Lost}' = \text{Lost} \cup \{\text{AV} \in \text{DB}(\text{SN}) \mid \exists_{\text{AV}_1} \text{AV}_1 \ll \text{AV} \wedge \text{AV} \prec \text{AV}_1\}
\end{aligned}$$

Or we could also say: using an AV with a sequence number larger than one already used (or, accepted) is loosing this AV. The “exact” definition of “lost” is not so important. But: we *need* such a definition (to be able to define what it means to return to normal behavior) and this definition has to be consistent with the one given for normal behavior, which should be a particular case.

Definition 7.4. *The definitions of generated and used copy remain the same:*

$$\mathcal{A}_{critical}^{Gen} : \Leftrightarrow \mathcal{A}_{normal}^{Gen} \quad \mathcal{A}_{normal}^{Used} : \Leftrightarrow \mathcal{A}_{normal}^{Used}$$

Definition 7.5. *An AV clone is obsolete if $\text{seq}_{MS} \geq \underline{\text{Seq}}(\text{AV})$. The set of obsolete clones is denoted by *Obsolete*. By definition,*

$$\text{Obsolete} \subseteq \text{Stolen} = \text{Stolen}_{HE} \cup \text{Stolen}_{SN}.$$

Definition 7.6. *An AV clone is called synchronous (with respect to seq_{MS}) if $\text{synchron}(\text{seq}_{MS}, \underline{\text{Seq}}(\text{AV}))$*

Notice that this is the same definition as 5.7 but for clones.

Definition 7.7. *The system is in perfect conditions (at a certain moment of time) if it is strongly-synchronous and any AV clone is obsolete:*

$$\text{Perfect} : \Leftrightarrow \text{StrongSynchron} \wedge \text{Stolen} \subseteq \text{Obsolete}$$

Notice that in the case that there are no clones (and in particular, if from the beginning the system was behaving normally) then $\text{Perfect} : \Leftrightarrow \text{StrongSynchron}$.

Definition 7.8. "Critical Behavior Scenario": *The system behaves critically if an arbitrary combination of assumptions or failure models (SN 1 – LU 3) may occur:*

$$\begin{aligned} \mathcal{N}_{critical}^{Step} &: \Leftrightarrow \mathcal{N}_{critical}^{LU} \wedge \mathcal{N}_{critical}^{SN} \wedge \mathcal{N}_{critical}^{HE} \wedge \mathcal{N}_{critical}^{CC} \wedge \mathcal{N}_{critical}^{MS} \\ \mathcal{A}_{critical} &: \Leftrightarrow \\ &\text{Init} \wedge \mathcal{A}_{critical}^{interleave} \wedge \mathcal{A}_{critical}^{CurrSN} \wedge \mathcal{A}_{critical}^{LastSN} \wedge \mathcal{A}_{critical}^{Gen} \wedge \mathcal{A}_{critical}^{Lost} \wedge \mathcal{A}_{critical}^{Used} \\ &\wedge \Box(\mathcal{N}_{critical}^{Step}) \end{aligned}$$

Definition 7.9. "Incorrect Behavior Scenario": *The system behaves incorrectly if*

- For any Δ AVs in sequence, at most $\Delta - 1$ are lost,
- disordering of AVs occur, (SN 3) but no SN-crashes or SN-steal
- a failure in the Location Update may happen (LU 2), but no race condition
- no errors in the home environment happen.

$$\begin{aligned} \mathcal{A}_{incorr} &: \Leftrightarrow \mathcal{A}_{critical} \wedge \Box(\wedge \text{Interr}_{\Delta-N-1}(Lost') \\ &\wedge \neg \text{XSN}(\text{Crash}) \\ &\wedge \neg \text{XSN}(\text{Steal}) \\ &\wedge \neg \text{XLU}(\text{Race}) \\ &\wedge \neg \text{XHE}) \end{aligned}$$

After the system has been behaving incorrectly, it may return to normal:

Definition 7.10. "Return to Normal Behavior": *Let x be a boolean variable (or state predicate) with the property that if it is $\underline{1}$, it remains $\underline{1}$: $\Box(x \Rightarrow x' = \underline{1})$. Then we say that the system behaves normally when x if during the time that $x = \underline{1}$ for any $(\Delta - N - 1)$ AVs in sequence, at least 1 AV is not lost, and on each transition step, the formulas $\mathcal{N}_{normal}^{LU}$, $\mathcal{N}_{normal}^{SN}$, $\mathcal{N}_{normal}^{HE}$, $\mathcal{N}_{normal}^{CC}$, and $\mathcal{N}_{normal}^{MS}$ hold:*

$$\begin{aligned} \mathcal{A}_{normal}^x &: \Leftrightarrow \\ &\text{Init} \wedge \mathcal{A}_{critical}^{interleave} \wedge \mathcal{A}_{critical}^{CurrSN} \wedge \mathcal{A}_{critical}^{LastSN} \wedge \mathcal{A}_{critical}^{Gen} \wedge \mathcal{A}_{critical}^{Lost} \wedge \mathcal{A}_{critical}^{Used} \\ &\wedge \forall_{Lost_0: \wp(AV)} [(\neg x \wedge x' \Rightarrow Lost' = Lost_0) \\ &\Rightarrow \Box\{ x \Rightarrow \mathcal{N}_{normal}^{Step} \wedge \text{Interr}_{\Delta-N-1}(Lost' \setminus Lost_0) \}] \end{aligned}$$

Note that "normal behavior" is more a property of the environment of the system (attacks, loosing messages, race conditions, failures in data-bases, etc.) as of the proper system itself. Even if the system returns to "normal behavior", the old failures may still have consequences, for instance, AVs with an old sequence number may be used. Often, only a "succesfull" synchronisation failure will "clean up" the system".

Notice also that the definition of return to normal behavior does not exclude the possibility that some messages get lost. (There is no bound on how many messages from the MS to the SN may get lost!) In particular if the system is not synchronous, this condition will remain unnoticed as long as the messages User Authentication Request and User Authentication Synchronisation Fail Indication get lost. In this case a "succesfull" synchronisation failure is not only helpful, it is necessary:

Definition 7.11. *We say that a Synchronisation Failure is successful, if*

1. the corresponding messages *User Authentication Request* and *User Authentication Synchronisation Fail Indication* do not get lost or corrupted, and if
2. this *Fail Indication* is processed by the *HE* before the *USIM* changes the *SN* location, i.e. no race condition *LU 3* happens.

Formally, a successful Synchronisation Failure is given by the formula:

$$\begin{aligned}
 \text{UASF}_{\text{successful}} : & \Leftrightarrow \exists_{\text{chall}, \text{SN}, \text{SynResp}} \\
 & \wedge \text{UAR}_s(\text{chall}, \text{SN}) \wedge \text{UAR}_r(\text{chall}, \text{SN}) \\
 & \wedge \text{UASF}_s(\text{SynResp}, \text{SN}) \wedge \text{UASF}_r(\text{SynResp}, \text{SN}) \\
 & \wedge \neg \exists_{\text{SN}} \text{XLU}(\text{SN}, \text{Race})
 \end{aligned}$$

8 Theorems

Lemma 8.1.

$$\begin{aligned}
 \mathcal{A}_{\text{normal}}^{\text{interleave}} \wedge \mathcal{N}_{\text{normal}}^{MS} \Rightarrow \\
 & \wedge \text{UAS}_s(\text{resp}, \text{SN}) \Rightarrow \exists_{\text{chall}} \wedge \text{UAR}_r(\text{chall}, \text{SN}) \\
 & \wedge \text{cons}(\text{chall}) \\
 & \wedge \text{synchron}(\text{seq}_{MS}, \underline{\text{Seq}}(\text{chall})) \\
 & \wedge \text{resp} = \underline{\text{Resp}}(\text{chall}) \\
 & \wedge \text{UAJ}_s(\text{RejResp}, \text{SN}) \Rightarrow \exists_{\text{chall}} \text{UAR}_r(\text{chall}, \text{SN}) \wedge \neg \text{cons}(\text{chall}) \\
 & \wedge \text{UASF}_s(\text{SynResp}, \text{SN}) \Rightarrow \exists_{\text{chall}} \wedge \text{UAR}_r(\text{chall}, \text{SN}) \\
 & \wedge \text{cons}(\text{chall}) \\
 & \wedge \neg \text{synchron}(\text{seq}_{MS}, \underline{\text{Seq}}(\text{chall})) \\
 & \wedge \text{SynResp} = \underline{\text{SynResp}}(\text{la_chall}, \text{chall})
 \end{aligned}$$

PROOF: The proof is done by simple predicate logic. All three claims are proven in exactly the same way. Let us prove the second one, which is the shortest one. It amounts to showing

$$\begin{aligned}
 \mathcal{A}_{\text{normal}}^{\text{interleave}} \wedge \mathcal{N}_{\text{normal}}^{MS} \wedge \text{UAJ}_s(\text{RejResp}, \text{SN}) \Rightarrow \\
 \exists_{\text{chall}} \text{UAR}_r(\text{chall}, \text{SN}) \wedge \neg \text{cons}(\text{chall})
 \end{aligned}$$

$$\begin{aligned}
 & \mathcal{A}_{\text{normal}}^{\text{interleave}} \wedge \mathcal{N}_{\text{normal}}^{MS} \wedge \text{UAJ}_s(\text{RejResp}, \text{SN}) \\
 & \Rightarrow \text{UAJ}_s \quad (\text{Def of } \text{UAJ}_s) \\
 & \Rightarrow \text{UAS}_s \vee \text{UAJ}_s \vee \text{UASF}_s \quad (\text{Conjunction Rules}) \\
 & \Rightarrow \text{UAR}_r \quad (\text{Def of } \mathcal{N}_{\text{normal}}^{MS}) \\
 & \Rightarrow \exists_{\text{chall}, \text{SN}_1} \text{UAR}_r(\text{chall}, \text{SN}_1) \quad (\text{Def of } \text{UAR}_s) \\
 & \Rightarrow \text{UAR}_r(\text{chall}, \text{SN}_1) \quad (\text{Skolemisation: Introd. of fresh variables})
 \end{aligned}$$

$$\begin{aligned}
& [\text{Assume } \text{cons}(\text{chall}) \wedge \text{synchron}(seq_{MS}, \underline{Seq}(\text{chall})) \\
& \quad \Rightarrow \text{UAS}_s(\underline{Resp}(\text{chall}), \text{SN}_1) \quad (\text{Def of } \mathcal{N}_{normal}^{MS}) \\
& \quad \Rightarrow \text{UAS}_s \quad (\text{Def of } \text{UAS}_s) \\
& \quad \Rightarrow \neg \text{UAJ}_s \quad (\text{Def of } \mathcal{A}_{normal}^{interleave}) \\
& \quad \Rightarrow \text{Contradiction} \quad (\text{UAJ}_s)]
\end{aligned}$$

$$\begin{aligned}
& \Rightarrow \neg(\text{cons}(\text{chall}) \wedge \text{synchron}(seq_{MS}, \underline{Seq}(\text{chall}))) \quad (\text{Assumption false}) \\
& \Rightarrow \neg \text{cons}(\text{chall}) \vee \neg \text{synchron}(seq_{MS}, \underline{Seq}(\text{chall})) \quad (\text{De Morgan})
\end{aligned}$$

$$\begin{aligned}
& [\text{Assume } \text{cons}(\text{chall}) \wedge \neg \text{synchron}(seq_{MS}, \underline{Seq}(\text{chall})) \\
& \quad \Rightarrow \text{UASF}_s(\underline{SynResp}(la_chall, \text{chall}), \text{SN}) \quad (\text{Def of } \mathcal{N}_{normal}^{MS}) \\
& \quad \Rightarrow \text{UASF}_s \quad (\text{Def of } \text{UASF}_s) \\
& \quad \Rightarrow \neg \text{UAJ}_s \quad (\text{Def of } \mathcal{A}_{normal}^{interleave}) \\
& \quad \Rightarrow \text{Contradiction} \quad (\text{UAJ}_s)] \\
& \Rightarrow \neg(\text{cons}(\text{chall}) \wedge \neg \text{synchron}(seq_{MS}, \underline{Seq}(\text{chall}))) \quad (\text{Assumption false}) \\
& \Rightarrow \neg \text{cons}(\text{chall}) \vee \text{synchron}(seq_{MS}, \underline{Seq}(\text{chall})) \quad (\text{De Morgan}) \\
& \Rightarrow \neg \text{cons}(\text{chall}) \quad (\text{Resolution}) \\
& \Rightarrow \text{UAJ}_s(\underline{RejResp}(\text{chall}), \text{SN}_1) \quad (\text{Def of } \mathcal{N}_{normal}^{MS} \text{ and } \text{UAR}_R(\text{chall}, \text{SN}_1)) \\
& \Rightarrow \text{RejResp} = \underline{RejResp}(\text{chall}) \wedge \text{SN} = \text{SN}_1 \quad (\text{UAJ}_s(\underline{RejResp}(\text{chall}), \text{SN}_1) \text{ and Def of } \mathcal{A}_{normal}^{interleave}) \\
& \quad \text{UAR}_R(\text{chall}, \text{SN}) \quad (\text{SN} = \text{SN}_1) \\
& \Rightarrow \text{UAR}_R(\text{chall}, \text{SN}) \wedge \neg \text{cons}(\text{chall}) \quad (\text{Conjunction}) \\
& \Rightarrow \exists_{\text{chall}} \text{UAR}_R(\text{chall}, \text{SN}) \wedge \neg \text{cons}(\text{chall}) \quad (\text{Intro of Ex.})
\end{aligned}$$

Lemma 8.2.

$$\begin{aligned}
& \mathcal{A}_{normal}^{CurrSN} \wedge \mathcal{A}_{normal}^{LastSN} \Rightarrow \\
& \quad \Box((\mathcal{N}_{normal}^{LU} \wedge \text{curr_SN}' \neq \emptyset) \Rightarrow \text{curr_SN}' = \{\text{last_SN}\})
\end{aligned}$$

Lemma 8.3.

$$\begin{aligned}
& \mathcal{A}_{normal} \Rightarrow \Box(\wedge DB(\text{last_SN}) \neq \epsilon \Rightarrow seq_{HE} = \underline{Seq}(\max(DB(\text{last_SN}))) \\
& \quad \wedge seq_{MS} = \underline{Seq}(\max(\text{Accepted})) \\
& \quad \wedge \text{UAR}_s(\underline{Chall}(\text{AV}), \text{SN}) \Rightarrow \text{AV} = \min(DB(\text{last_SN})))
\end{aligned}$$

PROOF: 1. The first goal is to prove

$$\mathcal{A}_{normal} \Rightarrow \Box(DB(\text{last_SN}) \neq \epsilon \Rightarrow seq_{HE} = \underline{Seq}(\max(DB(\text{last_SN}))))$$

This follows if in any transition where seq_{HE} or DB or $last_SN$ changes,

$$DB'(last_SN') \neq \epsilon \Rightarrow seq_{HE}' = \underline{Seq}(\max(DB'(last_SN'))))$$

holds.

1.1. Assume $seq_{HE} \uparrow$. First use the definition of $\mathcal{N}_{normal}^{HE}$. seq_{HE} changes only when ADS happens. Choosing fresh variables for the parameters we may assume $ADS(AVs_new, SN)$. It is easy to see that $AVs_new \neq \epsilon$, (else seq_{HE} does not change). Recalling the definition of $\mathcal{N}_{normal}^{HE} : \Leftrightarrow \exists_{seq_{he}} []$, choose seq_{he} to be any value that makes the predicate in the square brackets to be true. (Skolemisation). Now, since

$$\forall_{i \in \mathbb{N}} \exists_{AV \in AVs_new} (seq_{he} < i \leq seq_{HE}' \Rightarrow \underline{Seq}(AV) = i)$$

letting $i = seq_{HE}'$ we have

$$\exists_{AV \in AVs_new} \underline{Seq}(AV) = seq_{HE}'$$

Choose AV_0 with $\underline{Seq}(AV_0) = seq_{HE}'$. Now, from

$$\forall_{AV \in AVs_new} (seq_{he} < \underline{Seq}(AV) \leq seq_{HE}')$$

it follows that $\forall_{AV \in AVs_new} (\underline{Seq}(AV) \leq \underline{Seq}(AV_0))$, which may be written as $AV_0 = \max(AVs_new)$.

Using the definition of $\mathcal{N}_{normal}^{SN}$, we have that $ADS(AVs_new, SN)$ implies $DB'(SN) = AVs_new$ and therefore $AV_0 = \max(DB'(SN))$. Then

$$\underline{Seq}(AV_0) = \underline{Seq}(\max(DB'(SN))) = seq_{HE}'$$

proving the claim, since $SN \in curr_SN = curr_SN'$ (no race condition in $\mathcal{N}_{normal}^{LU}$) and $curr_SN' = \{last_SN'\}$ imply that $SN = \{last_SN'\}$.

1.2. Now assume that $last_SN \downarrow \wedge seq_{HE}' = seq_{HE}$, and let us show:

$$DB'(last_SN') \neq \epsilon \Rightarrow seq_{HE}' = \underline{Seq}(\max(DB'(last_SN'))))$$

Since

$$last_SN \downarrow \Rightarrow curr_SN \downarrow \wedge (\exists_{SN_1} curr_SN' = \{SN_1\} \vee curr_SN' = \emptyset)$$

but $curr_SN' = \emptyset$ implies $last_SN' = last_SN$. Choosing a new fresh variable, we conclude that $curr_SN \downarrow \wedge curr_SN' = \{SN_1\}$.

From $\mathcal{A}_{normal}^{CurrSN} \wedge \mathcal{A}_{normal}^{LastSN}$ we obtain that LUR \vee CANLOC and from $\mathcal{N}_{normal}^{LU}$ we know that CANLOC \Rightarrow LUR, proving LUR.

Consider now two cases: if $\neg MvAV$, then $DB'(last_SN') = \epsilon$, in the other case, if $MvAV$, then $DB'(last_SN') = DB(last_SN)$. In both cases our claim is valid.

1.3. Now assume that $DB \downarrow \wedge last_SN' = last_SN \wedge seq_{HE}' = seq_{HE}$, and let us show:

$$DB'(last_SN') \neq \epsilon \Rightarrow seq_{HE}' = \underline{Seq}(\max(DB'(last_SN'))))$$

If DB changes, but seq_{HE} does not, then UAR_s or $MvAV$ happen ($\mathcal{N}_{normal}^{SN}$). In the first one, only the smallest element of $DB(last_SN)$ is taken out, leaving $DB(last_SN)$ empty or its largest element unchanged. In both cases our goal is shown.

2. The second goal is that in each transition,

$$seq_{MS}' = \underline{Seq}(\max(Accepted')).$$

This follows easily from the definition of *Accepted* and $\mathcal{N}_{normal}^{MS}$.

3. The third goal is that in each transition,

$$\text{UAR}_s(\underline{\text{Chall}}(\text{AV}), \text{SN}) \Rightarrow \text{AV} = \min(\text{DB}(\text{last_SN})).$$

The proof is similar to the proof of the first goal and uses the fact that \ll and \prec coincide: when $\text{ADS}(\text{AVs_new}, \text{SN})$ happens, the elements of $\text{AVs_new} = \text{DB}'(\text{SN})$ are in order (i.e.: $\ll \Rightarrow \prec$). On each UAR_s , the smallest AV is used, and the remaining elements of $\text{DB}(\text{SN})$ continue in order.

Lemma 8.4.

$$\mathcal{A}_{normal} \Rightarrow \Box (\forall_{0 < i < \text{seq}_{HE}} \exists_{\text{AV} \in \text{Gen}} i = \underline{\text{Seq}}(\text{AV}))$$

Lemma 8.5. *If the system behaves normally, then the set of generated AVs is the union of the used AVs, the usable ones, and the lost ones:*

$$\mathcal{A}_{normal} \Rightarrow \Box (\text{Gen} = \text{Accepted} \cup \text{DB}(\text{last_SN}) \cup \text{Lost})$$

A simple consequence of the last two lemmas is:

Lemma 8.6.

$$\mathcal{A}_{normal} \Rightarrow \Box (\forall_{\text{seq}_{MS} < i < \underline{\text{Seq}}(\min(\text{DB}(\text{last_SN})))} \exists_{\text{AV} \in \text{Lost}} i = \underline{\text{Seq}}(\text{AV}))$$

Lemma 8.7. *If the system behaves normally, then the set of usable AVs has never more than N elements:*

$$\mathcal{A}_{normal} \Rightarrow \Box (|\text{DB}(\text{last_SN})| \leq N)$$

Lemma 8.8.

$$\mathcal{A}_{normal} \Rightarrow \Box (\text{UAR}_s(\text{chall}, \text{SN}) \Rightarrow \underline{\text{Seq}}(\text{chall}) - \text{seq}_{MS} < \Delta)$$

PROOF: This follows from $\text{chall} = \min(\text{DB}(\text{SN}))$ and $(\text{SN}) = \text{last_SN}$

Lemma 8.9.

$$\begin{aligned} \mathcal{N}_{normal}^{CC} \wedge \text{UAR}_s(\underline{\text{Chall}}(\text{AV}), \text{SN}) \Rightarrow \\ \vee \wedge \text{Accepted}' = \text{Accepted} \cup \{\text{AV}\} \\ \wedge \text{seq}_{MS}' = \underline{\text{Seq}}(\text{AV}) \\ \wedge \text{Lost}' = \text{Lost} \\ \vee \wedge \text{Accepted}' = \text{Accepted} \cup \{\text{AV}\} \\ \wedge \text{seq}_{MS}' = \underline{\text{Seq}}(\text{AV}) \\ \wedge \text{Lost}' = \text{Lost} \cup \{\text{AV}\} \\ \vee \wedge \text{Accepted}' = \text{Accepted} \\ \wedge \text{seq}_{MS}' = \text{seq}_{MS} \\ \wedge \text{Lost}' = \text{Lost} \cup \{\text{AV}\} \end{aligned}$$

Lemma 8.10.

$$\begin{aligned} \mathcal{N}_{normal}^{CC} \wedge \text{UAR}_s(\underline{\text{Chall}}(\text{AV}), \text{SN}) \wedge \text{UAS}_R(\underline{\text{Resp}}(\text{AV}), \text{SN}) \Rightarrow \\ \wedge \text{Accepted}' = \text{Accepted} \cup \{\text{AV}\} \\ \wedge \text{seq}_{MS}' = \underline{\text{Seq}}(\text{AV}) \\ \wedge \text{Lost}' = \text{Lost} \end{aligned}$$

Proposition 8.11. *Initially the system is in perfect conditions. And as long as the system behaves normally, it remains in perfect conditions and no synchronisation failures happen. This may be formalised as follows⁴:*

$$\mathcal{A}_{normal} \Rightarrow \Box(Perfect) \wedge \Box(\neg \text{UASF}_s)$$

PROOF: First let us see why *Perfect* is an invariant, i.e. $\mathcal{A}_{normal} \Rightarrow \Box(Perfect)$. It is clear that initially, *Perfect* holds, i.e. $\text{Init} \Rightarrow Perfect$. Now, if *Perfect* holds and \mathcal{N}_{normal} holds then also *Perfect'* holds. This follows from Lemma 8.8.

Proposition 8.12. *If the system behaves incorrectly, and then behaves normally, then after the first successful Synchronisation Fail Indication the system is in perfect conditions. This is formalised as follows:*

$$\mathcal{A}_{incorr} \wedge \mathcal{A}_{normal}^x \Rightarrow \Box(\text{UASF}_{successful} \wedge x \Rightarrow Perfect')$$

Proposition 8.13. *If the system behaves critically, and then behaves normally, then after the first successful Synchronisation Fail Indication the system is strongly-synchronous. This is formalised as follows:*

$$\mathcal{A}_{normal}^x \Rightarrow \Box(\text{UASF}_{successful} \wedge x \Rightarrow StrongSynchr')$$

Proposition 8.14. *If the system strongly-synchronous but not in perfect conditions, and from that point on it behaves normally, then after the stolen AVs have been used or become obsolete, at most one successful Synchronisation Fail Indication is needed to return to perfect conditions.*

Proposition 8.15. *If the system weakly-synchronous but not strongly-synchronous, and from that point on it behaves normally, then after the non-synchronous usable AVs have been used or lost, at most one successful Synchronisation Fail Indication is needed to return to a strongly-synchronous state.*

References

- [1] L. Lamport. The Temporal Logic of Actions. *ACM Transactions on Programming Languages and Systems*, 16(3): 872–923, May 1994.
- [2] 3G TS 33.102 Version 3.0.0. *3G Security Architecture*
- [3] S3-99179 (CR to [2]), *Conditions on use of Authentication Information*.
- [4] S3-99180 (CR to [2]), *Modified re-synchronisation procedure for AKA-protocol*.
- [5] S3-99181 (CR to [2]), *Sequence number management scheme protecting against USIM lockout*.

⁴The formalisation states something slightly different, namely that if the system always behaves normally, then it is always in perfect conditions and never a synchronisation failure happens. This is slightly weaker than the formulation in the theorem. But the induction proof given in the text also proves the stronger assertion: the proof shows that initially the system is in perfect conditions and that as long as normal conditions hold, the system remains in perfect conditions and no synchronisation failure happens.