Analysis and Modeling of False Synchronizations in 3G-WLAN Integrated Networks

Christoforos Ntantogian[1], Christos Xenakis[1], and Ioannis Stavrakakis[2]

[1] Department of Digital Systems, University of Piraeus, Greece
{dadoyan,xenakis}@unipi.gr
[2] Department of Informatics and Telecommunications, University of Athens, Greece
ioannis@di.uoa.gr

Abstract. Recently, a set of problems have been solved analytically, in order to improve various aspects of the authentication procedure in mobile networks. In these problems, an analytical model is derived, which is used to draw guidelines on the selection of the appropriate value of various system parameters. We observe that all these problems can be solved using a generic modeling procedure that is based on Markov chains assuming exponential distributions. In this paper we apply this generic modeling procedure to the problem of false synchronizations in 3G-WLAN integrated networks. To this end, we first elaborate on false synchronization using a numerical example that facilitates the better understanding of the presented notions. Then, an analytical model based on a four dimensional Markov chain is developed, using the generic modeling procedure, whose accuracy is verified through simulations.

Keywords: Markov chains, analytical modeling, false synchronizations, 3G-WLAN networks, authentication.

1 Introduction

In third generation (3G) mobile networks, authentication is executed between the mobile station (MS) and the home network where MS is subscribed. The MS initiates the authentication procedure by sending an authentication request to the access network. If the latter has authentication credentials, called authentication vectors (AV), available for the specific MS, then the access network authenticates the MS. The authentication procedure of 3G networks includes a security mechanism, which ensures that each AV is used only once (freshness property). This protects both the MS and access network from what is known as replay attacks: that is, an attempt by an adversary to use a compromised previously used AV in order to authenticate itself either as a valid MS or as a valid access network. To detect such attacks, the MS and the access network try to keep track of previously used AVs using either counters or timestamps [1]. This paper considers the first case.

Although this protection mechanism defeats replay attacks, at the same time it creates negative side effects from a performance point of view. More specifically, in some circumstances an MS that changes frequently access networks, may receive AVs that have not been previously used, but the employed mechanism rejects them as

D. Gritzalis, S. Furnell, and M. Theoharidou (Eds.): SEC 2012, IFIP AICT 376, pp. 475–488, 2012.

outdated. This phenomenon defined as false synchronization impose signaling overhead that: (i) increases significantly the authentication latency, especially in cases that the MS is located far away from its home network; (ii) increases the call blocking rate in cases that the MS has active real-time sessions (e.g., VoIP, videoconference); and (iii) overcharges the MS in cases that the access network and home network are located in different countries. Therefore, false synchronizations: (a) deteriorate the overall network performance, (b) lower the quality of service offered to MSs, and (c) increase the cost of the network use [4].

Apart from false synchronizations, recently a set of problems have been solved analytically, (such as [5], [6], [7], [8]) in order to improve various aspects of the authentication procedure in mobile networks. In all these problems, an analytical model is derived, which is used to draw guidelines on the selection of the appropriate value of various system parameters. We observe that all these problems can be solved using a generic modeling procedure that is based on Markov chains assuming exponential distributions. Specifically, this modeling procedure includes the following steps: 1) pinpoint the underlying Markov structure that models the system dynamics (i.e., identify the Markov chain dimension, states and its transitions); 2) in case of large or infinite Markov chains, apply a state space truncation to ensure that a steady state analysis can be performed; 3) develop the steady stake equations; 4) solve the system of linear equations, using numerical or analytical methods, to derive steady state probabilities. After the last step, the key performance metrics of each problem can be easily derived to provide insights into the specific system.

In order to put the aforementioned modeling procedure into effect, we apply it to the problem of false synchronizations in 3G-WLAN integrated networks [4]. For this purpose, we first elaborate on false synchronization using a numerical example that facilitates the better understanding of the presented notions. Based on the modeling procedure, we develop an analytical solution using a four dimensional Markov chain that captures the system dynamics. We notice that the derived Markov chain cannot be directly used to perform steady state analysis. To this end, we perform a state space truncation of the Markov chain. Finally, we derive the steady state equations and solve a linear system of equations to derive the probability of a false synchronization.

2 Background

2.1 3G-WLAN Network Architecture

As shown in Fig. 1, the 3G-WLAN integrated network architecture consists of four individual parts [2]: (i) the MS, (ii) the UMTS radio access network (UTRAN), (iii) the WLAN, and (iv) the 3G core network. The MS comprises the user's device (e.g., laptop, PDA) and the universal subscriber identity module (USIM), which contains the user's subscriber information. UTRAN consists of Nodes B that provide wireless connections to MS, and radio network controllers (RNCs) that provide radio channel management services. One or more Nodes B connect to an RNC, while one or more RNCs connect to a serving gateway support node (SGSN), which is located in the 3G-WLAN core network. WLAN includes wireless access points that provide Wi-Fi

access and act like authentication, authorization, accounting (AAA) clients, forwarding security related messages to a AAA server. Finally, the 3G core network includes SGSN, the AAA server and an authentication center (AuC). SGSN provides mobility and session management services in UMTS, while the AAA server provides authentication services in WLAN. Both SGSN and the AAA server are connected to AuC, which contains the AVs of MS. In case that a MS wants to gain access to UMTS, it should execute the UMTS authentication and key agreement (UMTS-AKA) protocol [1]. On the other hand, if it wants to have access to WLAN, it should carry out the extensible authentication protocol EAP-AKA [3]. We briefly analyze these two protocols below as well as the replay attack protection mechanism.

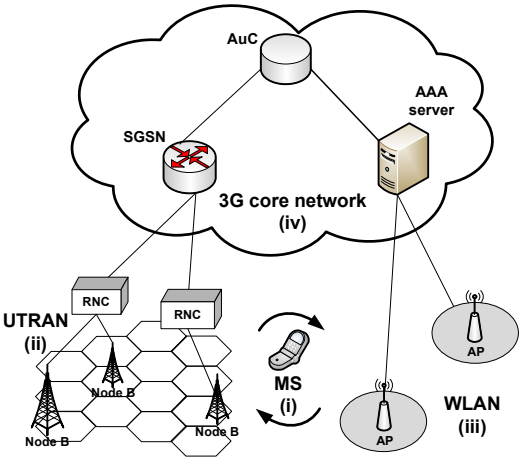

Fig. 1. 3G-WLAN integrated network architecture

2.2 UMTS-AKA

UMTS-AKA provides mutual authentication between MS and the UMTS network, based on the knowledge of a common secret key K, which is stored in USIM and AuC. In the initial step of UMTS-AKA, MS conveys a message that contains its identity to SGSN (see Fig. 2(a) – step a), and the latter conveys this identity to AuC, asking for fresh AVs for the specific MS (i.e., ADR procedure) (see Fig. 2(a) – step b). AuC fetches the permanent key K of MS and generates a batch of L_U ordered AVs [1]. Initially, it increments by one value the counter SQN_{HN} (i.e., SQN_{HN}=SQN_{HN} +1) and sets SQN_{AV} = SQN_{HN}. Then, AuC generates a random number (RAND) and calculates the following parameters using the retrieved secret key K and a set of one-way hash functions (i.e., f_1, f_2, f_3, f_4, f_5) as shown in Fig. 3:

1. Message authentication code $MAC = f_1(SQN_{AV}||RAND||AMF)$. (The authentication and key management field (AMF) is reserved to be used whenever the UMTS network wants to convey to a USIM values of parameters that change over time).
2. Expected response $XRES = f_2(RAND)$.

3. Encryption key $CK = f_3(RAND)$.
4. Integrity key $IK = f_4(RAND)$.
5. Anonymity key $AK = f_5(RAND)$.
6. Authentication token $AUTN = SQN_{AV} \oplus AK||AMF||MAC$.

This is repeated L_U times for the generation of the batch of L_U AVs. Next, AuC forwards the L_U AVs in an ordered form (based on SQN_{AV}) to SGSN (see Fig. 2(a) – step c). Upon receiving them, SGSN selects the one with the smallest SQN_{AV} and conveys the pair of RAND and AUTN from the selected AV to MS (see Fig. 2(a) – step d). SGSN stores the remaining $L_U - 1$ AVs to use them in future authentications of MS.

Upon receiving this pair (RAND, AUTN), MS forwards it to USIM. The latter use this pair with the secret key K to compute AK (i.e., $AK = f_5(RAND)$) and SQN_{AV} (i.e., $SQN_{AV} = \left(SQN_{AV} \oplus AK\right) \oplus AK$), where $\left(SQN_{AV} \oplus AK\right)$ is included in the received AUTN). Then, USIM checks whether $SQN_{AV} > SQN_{MS}$ or $SQN_{MS} - SQN_{AV} \leq \alpha$. The parameter α plays a key role in the replay attack protection mechanism and it is called offset in this paper. If one of the above two conditions is true, USIM accepts the received AV; otherwise, it rejects it as a suspicion of an attack. Thus, the value of offset α is used from USIM to verify whether the received SQN_{AV} is among the last α generated.

In case USIM accepts the received SQN_{AV} and $SQN_{AV} > SQN_{MS}$ then, SQN_{MS} is set equal to the received SQN_{AV} (otherwise, SQN_{MS} remains the same). Afterwards, USIM computes $XMAC = f_1(SQN_{AV}||RAND||AMF)$ and an AUTN′ value using the previously generated AK key and XMAC. If the computed AUTN′ is equal to the received AUTN, the UMTS network is authenticated to MS and USIM computes $RES = f_2(RAND)$, $CK = f_3(RAND)$ and $IK = f_4(RAND)$. After that, MS forwards the computed RES to SGSN (see Fig. 2(a) – step e), which verifies whether the received RES is equal to XRES, included in the AV. If it is true, MS is authenticated to SGSN. In the last step of UMTS-AKA, USIM and SGSN convey to MS and RNC, respectively, the computed CK and IK (see Fig. 2(a) – step f), which are used to provide confidentiality and integrity services between MS and RNC.

2.3 EAP-AKA

EAP-AKA works similarly to UTMS-AKA, as depicted in Fig. 2(b). First, MS requests for an AV from the AAA server, through the wireless AP. The AAA server executes the ADR procedure to fetch AVs from AuC, which generates and sends back to the AAA server L_W ordered AVs (note that the number of generated AVs in EAP-AKA and UMTS-AKA, (i.e., L_W and L_U respectively) are not necessarily equal). The AAA server selects the AV with the smallest SQN_{AV}, obtains the pair of RAND and AUTN from the selected AV and conveys them to MS (the remaining L_W-1 AVs are stored for future use). Upon receiving this pair (RAND, AUTN), MS forwards it to USIM, which verifies the associated SQN_{AV} and AUTN in order to authenticate the WLAN network, similarly to UMTS-AKA. Afterwards, USIM computes RES, CK and IK, and forwards them to MS. The latter calculates the master session key (MSK) using the CK and IK keys, and conveys RES to the AAA server. Upon receiving RES,

the AAA server authenticates MS (i.e., if XRES=RES), calculates MSK (using CK and IK keys), and sends it to the wireless AP. At the end of EAP-AKA, MS and WLAN are authenticated mutually, while MS and the wireless AP share MSK that is used to provide security services in WLAN

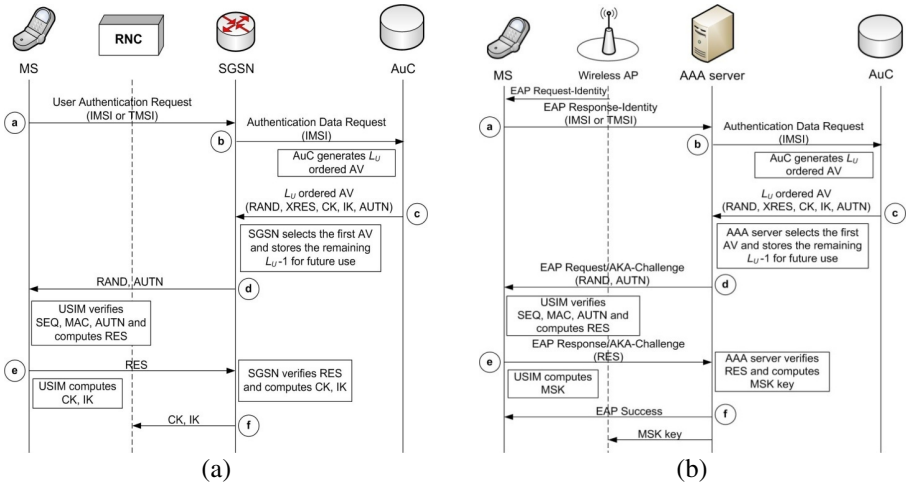

Fig. 2. Message exchange in (a) UMTS-AKA and (b) EAP-AKA

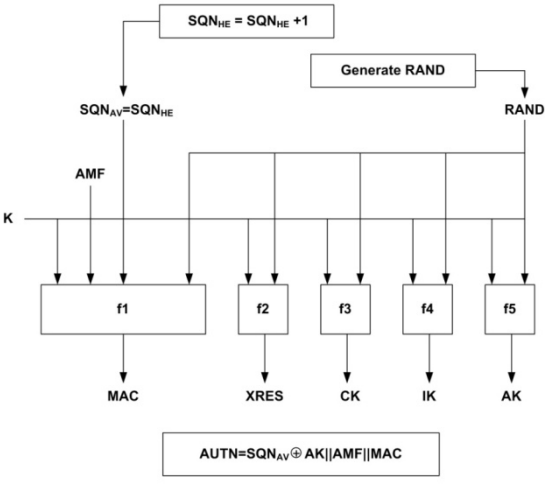

Fig. 3. AVs generation procedure

3 False Synchronizations in 3G-WLAN Integrated Networks

In this section we describe false synchronizations using a numerical example. Assume that: (a) a MS moves between UMTS and WLAN executing the UMTS-AKA and

EAP-AKA protocols, respectively (see Fig. 4); (b) the number of generated AVs in the UMTS and WLAN batch is $L_U = 6$ and $L_W = 4$, respectively; (c) the value of offset $\alpha = 7$. Initially, SGSN and the AAA server do not have any AV stored for the involved MS, and $SQN_{HN} = SQN_{MS} = 0$. Moreover, we use the term 'handover' to imply that: (i) a MS has an active connection and moves from UMTS to WLAN and vice versa, performing authentication or (ii) MS has no active connection and moves from UMTS to WLAN and vice versa, establishing a new connection in the newly visited network (executing UMTS-AKA or EAP-AKA).

We consider the time diagram of Fig. 4, assuming that the MS initially resides in UMTS and at the time t_1 executes UMTS-AKA. Since SGSN does not possess any stored AV for the involved MS, it executes the ADR procedure with AuC, which generates a batch of $L_U = 6$ AVs that contain $SQN_{AV} = 1, 2, 3, 4, 5, 6$, respectively and sets $SQN_{HN} = 6$. Next, AuC conveys the $L_U = 6$ newly generated AVs to SGSN, which selects the one with $SQN_{AV} = 1$ and conveys it to the MS (the remaining 5 AVs are stored for future use). The latter accepts the received AV and sets $SQN_{MS} = 1$. After five more successive UMTS-AKA authentications, at the time t_2, SGSN performs again ADR and thus, AuC generates a new batch of $L_U = 6$ AVs with $SQN_{AV} = 7, 8, 9, 10, 11, 12$ (i.e., $SQN_{HN} = 12$) and sends them to SGSN. At the time t_3, (after six more UMTS-AKA authentications) the SGSN has consumed all the previously generated AVs and MS has set $SQN_{MS} = 12$.

At the time t_4, the MS handovers from UMTS to WLAN and executes EAP-AKA. The AAA server performs ADR, since it does not possesses any AV for the involved MS. As a result, AuC generates a batch of $L_W = 4$ AVs with $SQN_{AV} = 13, 14, 15, 16$ respectively, sets $SQN_{HN} = 16$, and coveys them to the AAA server. The AAA sever

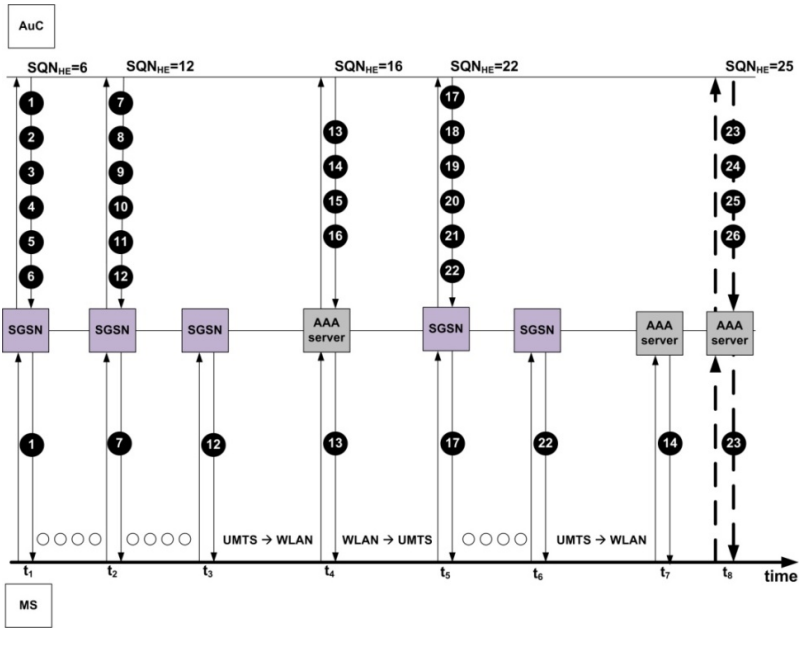

Fig. 4. Time diagram of the numerical example

sends the AV with SQN_{AV} = 13 to the MS, which is accepted since SQN_{MS} = 5 < SQN_{AV} = 13, and sets SQN_{MS} = 13. Then, the MS returns back to UMTS and at the time t_5 executes UMTS-AKA. As SGSN does not have any stored AV, it initiates ADR and thus, AuC generates a batch of AVs with SQN_{AV} = 17, 18, 19, 20, 21, 22 (SQN_{HN} = 22), which are forwarded to SGSN. The latter conveys the AV with SQN_{AV} = 17 to the MS, which accepts it (since SQN_{MS} = 13 < SQN_{AV} = 17) and sets SQN_{MS} = 17. After that, the MS executes five successive UMTS-AKA authentications, consuming all the above AVs that SGSN possess and sets SQN_{MS} = 22. At the time t_7, the MS returns to WLAN and executes EAP-AKA. The AAA server, which has stored AVs for the MS, conveys the AV with SQN_{AV} = 14 to the MS. The latter rejects it (SQN_{MS} - SQN_{AV} = 8 > 7), since the employed freshness mechanism, erroneously, indicates that the current AV has been used in the past (i.e., false synchronization). At this point a false synchronization has occurred and a re-synchronization procedure is initiated.

4 Modeling Procedure

In this section an analytical model based on a Markov chain is developed that leads to the derivation of the probability of false synchronizations P_{sync} in 3G-WLAN integrated networks.

Table 1. Analytical model parameters

Notation	Description
N_k	Random variable that denotes if the MS resides in UMTS or WLAN
D_k	Difference between SQN_{UMTS} and SQN_{WLAN}
U_k	Number of AVs stored in SGSN
W_k	Number of AVs stored in the AAA server
SQN_{UMTS}	The last SQN_{AV} that MS has received from UMTS
SQN_{WLAN}	The last SQN_{AV} that MS has received from WLAN
$1/\mu_u$	Mean residence time in UMTS
$1/\mu_w$	Mean residence time in WLAN
λ_u	Authentication rate in UMTS
λ_w	Authentication rate in WLAN
L	Number of AVs that AuC generates in a batch
a	Offset value
P_{sync}	Probabililty of false synchronization

4.1 Identifying the Markov Chain Structure

To facilitate the system modeling, it is assumed that the residence time of a MS in UMTS and WLAN are exponentially distributed, and the authentication request process is Poisson. The following definitions and notations will be used in the analysis that follows:

- The residence time of a MS in UMTS and WLAN is assumed to follow an exponential distribution with mean $1/\mu_u$ and $1/\mu_w$, respectively.
- The authentication request rate of a MS in UMTS and WLAN is assumed to be Poisson with rate λ_u and λ_w, respectively.
- The number of the generated AVs L_U and L_W in UMTS and WLAN, respectively, is assumed to be equal to L (i.e., $L_U = L_W = L$).
- The last SQN_{AV} that a MS has received from UMTS (i.e., SGSN) and WLAN (i.e., the AAA server), are denoted by SQN_{UMTS} and SQN_{WLAN}, respectively.
- Consider the following quantities or processes embedded at the time instances k at which a network handover or authentication request (referred to as an H-A event) occurs:
- Let $N_k \in \{0,1\}$ denote whether the MS resides in UMTS ($N_k = 0$) or in WLAN ($N_k = 1$) following the k[th] H-A request.
- Let $D_k \in (-\infty, +\infty)$, denote the difference between SQN_{UMTS} and SQN_{WLAN} (i.e., $D = SQN_{UMTS} - SQN_{WLAN}$), following the k[th] H-A event.
- Let $U_k \in [0, L)$ and $W_k \in [0, L)$ denote the number of AVs stored in SGSN and the AAA server, respectively, following the k[th] H-A event. All operations in the set $\{0,1,2..,L-1\}$ defined by the variables U_k and W_k use modular arithmetic with $modulo\ L$. To simplify notations, the symbol "$modL$" is omitted.

Table 1 summarizes the system and modeling parameters introduced above. In view of the aforementioned system modeling assumptions, it is not hard to show that the four dimensional process $E_k = \{N_k, D_k, U_k, W_k\}$ embedded at time instances k at which a network handover or authentication request occurs, is a discrete-time Markov chain.

It should be noted that the instances k at which an H-A event occurs are generated according to the following dynamics of handover and authentication requests: 1) Given that a MS is in UMTS (WLAN) in the current embedded instant, the next embedded time instant will be generated by an authentication request with probability $p_1 = \frac{\lambda_u}{\mu_u + \lambda_u}$ (with probability $p_2 = \frac{\lambda_w}{\mu_w + \lambda_w}$). 2) Given that MS is in UMTS in the current embedded instant, the next embedded time instant will be generated by a handover from UMTS to WLAN (and will also trigger an authentication in WLAN) with probability $p_3 = \frac{\mu_u}{\mu_u + \lambda_u}$. Similarly, given that a MS is in WLAN in the current embedded instant, the next embedded time instant will be generated by a handover from WLAN to UMTS (and will also trigger an authentication in UMTS) with probability $p_4 = \frac{\mu_w}{\mu_w + \lambda_w}$.

Before proceeding with the steady state analysis of the Markov chain, we elaborate on the conditions that trigger a false synchronization. Assume that the Markov chain is in some state (δ, i, j, z) with $N_k = \delta, D_k = i$, $U_k = j$ and $W_k = z$. A false synchronization occurs, if the following conditions are satisfied:

1. A handover from UMTS to WLAN takes place, i.e., $\delta: 0 \rightarrow 1$.
2. WLAN (i.e., the AAA server) has at least one AV to provide to the MS, i.e., $W_k = z > 0$.

3. WLAN (i.e., AAA server) provides to the MS an AV that includes a SQN_{AV}, which is at least $a + 1$ values smaller than the last SQN_{AV} that UMTS provided to the MS (i.e., $D_k = i > a$, which means $D_k = a + 1, a + 2, a + 3...$).

The above are defined as false synchronization conditions from UMTS to WLAN. Note that the second condition guarantees that the AAA server has at least one "old" AV to provide to MS. On the contrary, if the second condition is not satisfied (i.e., $W_k = z = 0$), then a false synchronization does not occur when the MS moves to WLAN, since the AAA server performs ADR and fetches a batch of fresh AVs from AuC.

When a false synchronization occurs upon the MS handover from UMTS to WLAN (referred to as false synchronization in WLAN), we argue that the Markov chain jumps from the state $(0, i, j, z)$ to state $(1, -(j + 1), j, L - 1)$ since:

1. The MS is located in WLAN after the handover and thus, $N_k = 1$.
2. The false synchronization initiates ADR in WLAN, and thus, the batch of AVs that resides in WLAN is fresher than this of UMTS, while it was the opposite just before the execution of ADR. Therefore, if the remaining j AVs in UMTS contain $SQN_{AV} = d + 1,\ d + 2, \dots, d + j$, then the newly generated AVs of WLAN contain $SQN_{AV} = d + j + 1,\ d + j + 2, \dots, d + j + L$, where $d \in N$. As a result, the difference between the last SQN_{AV} that UMTS has provided (i.e., $SQN_{AV} = d$) and the last SQN_{AV} that the MS receives from WLAN (i.e., $SQN_{AV} = d + j + 1,$) is $D_k = -(j + 1)$.
3. The value of U_k is the same, $U_k = j$.
4. From the newly generated AVs the performed authentication consumes one and thus, $W_k = L - 1$.

Summarizing the above we have:

Proposition 1: Upon a handover of MS from UMTS to WLAN, the Markov chain jumps from the state $(0, i, j, z)$ to $(1, -(j + 1), j, L - 1)$, if $i > a$. In addition, if $z > 0$ is satisfied, then the handover from UMTS to WLAN triggers a false synchronization in WLAN.

Similarly, we can infer that a false synchronization occurs upon a MS handover from WLAN to UMTS (referred to as false synchronization in UMTS) when the following conditions (referred to as false synchronization conditions from WLAN to UMTS) are satisfied:

1. A handover from WLAN to UMTS takes place, $\delta: 1 \rightarrow 0$.
2. $U_k = j > 0$.
3. $D_k = i < -a$ (i.e., $D_k = -(a + 1), -(a + 2), -(a + 3)...$).

Finally, similarly to proposition 1, we have:

Proposition 2: Upon a handover of MS from WLAN to UMTS, the Markov chain jumps from the state $(1, i, j, z)$ to $(0, z + 1, L - 1, z)$, if $i < -a$. Additionally, if $j > 0$, then the handover from WLAN to UMTS triggers a false synchronization in UMTS.

4.2 State Space Truncation

In order to derive the probability of false synchronizations, the steady state probabilities of the Markov chain E_k should be derived first. We notice that Markov chain E_k has a infinite state space as $D_k \in (-\infty, +\infty)$. Thus, we truncate its state space properly so that its dimensionality becomes finite, without compromising the accuracy of the resulting solution. The following proposition ensures that the original and the truncated Markov chains induce identical false synchronization events.

Proposition 3: Assume that $\widetilde{E_k}$ is a truncated Markov chain of E_k, where $\widetilde{E_k} = \{\widetilde{N_k}, \widetilde{D_k}, \widetilde{U_k}, \widetilde{W_k} : \widetilde{N_k} \in [0,1],\ \widetilde{D_k} \in [-(a+1), (a+1)],\ \widetilde{U_k} \in [0, L),\ \widetilde{W_k} \in [0, L)\}$. Then, the evolution of E_k and $\widetilde{E_k}$ is identical in the sub space that determines a false synchronization in UMTS or a false synchronization in WLAN and, thus, the two processes induce the same number of false synchronization events.

Proof: Notice that the values of D_k greater than $a+1$ (i.e., $D_k = a+2, a+3, ...$) or lower than $-(a+1)$ (i.e., $D_k = -(a+2), -(a+3), ...$) do not affect the evolution of the Markov chain in the sub space that determines the occurrence of a false synchronization in UMTS or a false synchronization in WLAN. Therefore, D_k parameter can be bounded between $-(a+1) \leq D_k \leq a+1$, as elaborated bellow.

If $-(a+1) \leq D_k \leq a+1$, it is evident that the two Markov chains $\widetilde{E_k}$ and E_k are identical, $\widetilde{E_k} \equiv E_k$. In case that both chains are in the state $(0, a+1, j, z)$ and an authentication in UMTS occurs, then E_k jumps to the state $(0, a+2, j-1, z)$, since UMTS consumes one of the stored AVs reducing in this way U_k ($U_k = j-1$), and increasing D_k ($D_k = a+2$). On the other hand, $\widetilde{E_k}$ jumps to the state $(0, a+1, j-1, z)$. After $n-1$ successive authentications in UMTS, E_k and $\widetilde{E_k}$ are in states $(0, a+n+1, j-n, z)$ and $(0, a+1, j-n, z)$, respectively. We observe that for authentication in UMTS, we have $\widetilde{N_k} = N_k, \widetilde{U_k} = U_k, \widetilde{W_k} = W_k$ and if $D_k > a$, then $\widetilde{D_k}$ remains equal to $a+1$ while D_k increases (i.e., $D_k = a+1, a+2, a+3, ...$).

Assume now that a handover from UMTS to WLAN occurs. If $z > 0$, then in both chains this handover triggers a false synchronization in WLAN. More specifically, E_k jumps from the state $(0, a+n+1, j-n, z)$ to state $(1, -(j+1), j-n, L-1)$, since $D_k = a+n+1 > a$ (see Proposition 1) and $\widetilde{E_k}$ jumps from the state $(0, a+1, j-n, z)$ to the state $(1, -(j+1), j-n, L-1)$, since $\widetilde{D_k} = a+1 > a$. It is observed that $D_k = \widetilde{D_k} = -(j+1)$ and thus, the two chains are identical. Therefore, it can be deduced that whenever a false synchronization in WLAN occurs in E_k, the same false synchronization in WLAN also occurs in $\widetilde{E_k}$. Similarly, we can prove that whenever a false synchronization in UMTS occurs in E_k, the same also happens in $\widetilde{E_k}$. Thus, we can conclude that the evolution of E_k and $\widetilde{E_k}$ are similar in the sub space that determines a false synchronization in UMTS or a false synchronization in WLAN. This ends the proof.

It is evident that the truncated Markov chain $\widetilde{E_k} = \{\widetilde{N_k}, \widetilde{D_k}, \widetilde{U_k}, \widetilde{W_k}\}$ is ergodic and converges to a steady state. Let $\pi\{N_k, D_k, U_k, W_k\}$ be the steady state probabilities of $\widetilde{E_k}$.

4.3 Steady State Equations

The truncated Markov chain $\widetilde{E_k} = \{\widetilde{N_k}, \widetilde{D_k}, \widetilde{U_k}, \widetilde{W_k}\}$ is ergodic and converges to a steady state. Let $\pi_{(\delta,i,j,z)}$ be the steady state probability of a generic state (δ, i, j, z), with $\widetilde{N_k} = \delta, \widetilde{D_k} = i, \widetilde{U_k} = j$ and $\widetilde{W_k} = z$. We divide the steady state equations of $\widetilde{E_k}$ into two main sets, SET I (i.e., $\delta = 0$) and SET II (i.e., $\delta = 1$):

SET I) $\delta = 0$: In this case, MS is located in UMTS. Depending on the values of i, j and z the following balance equations are satisfied.

I.1) If $i > 0$: The last SQN_{AV} that MS has received from UMTS is greater than the last one received from WLAN.

CASE I.1.A) $i = a + 1$: The Markov chain arrives at states with $i = a + 1$, only in cases that MS performs an authentication while it is in UMTS. We pinpoint two different sub-cases.

I.1.A.1) If $i - z \equiv -j(modL)$: The Markov chain arrives at the states $(0, a + 1, j, z)$ either from the states $(0, a + 1, j + 1, z)$ or from the states (0,a, j+1, z) (e.g., in Fig. 5(a) the state B arrives from A or Z). Thus,

$$\pi_{(0,i,j,z)} = \frac{\lambda_u}{\mu_u+\lambda_u}\pi_{(0,i,j+1,z)} + \frac{\lambda_u}{\mu_u+\lambda_u}\pi_{(0,i-1,j+1,z).} \quad (1)$$

I.1.A.2) Otherwise: The Markov chain arrives at the states $(0, a + 1, j, z)$, only from the states $(0, a + 1, j + 1, z)$, (e.g., in Fig.5(a) the state D can be reached only from C). Thus,

$$\pi_{(0,i,j,z)} = \frac{\lambda_u}{\mu_u+\lambda_u}\pi_{(0,i,j+1,z)} \quad (2)$$

CASE I.1.B) $i = z + 1$ and $j = L - 1$: The Markov chain arrives at states with $i = z + 1$ and $j = L - 1$, only if MS returns to UMTS and executes ADR. In this case, the states $(0, i, j, z)$ can be reached from the states with $(1, -a+1$, (0, 1, 2…L−1), $z)$, (e.g., in Fig. 5(b) the state A can be reached only from B, C, D,…, Z). Thus,

$$\pi_{(0,i,j,z)} = \frac{\mu_w}{\mu_w+\lambda_w}\pi_{(1,-(a+1),j*,z)} \quad (3)$$

CASE I.1.C) For all other values of i, with i>0 we recognize two sub-cases:

I.1.C.1) If $z \neq L - 1$: The states (0,i,j,z) can be reached either from the states $(1, i - 1, j + 1, z)$ in MS handover from WLAN to UMTS event, or from the states (0,i−1, j+1,z) in MS authentication in UMTS event. Thus,

$$\pi_{(0,i,j,z)} = \frac{\mu_w}{\mu_w+\lambda_w}\pi_{(1,i-1,j+1,z)} + \frac{\lambda_u}{\mu_u+\lambda_u}\pi_{(0,i-1,j+1,z)} \quad (4)$$

I.1.C.2) If $z = L - 1$: The states $(0, i, j, z)$ can be reached from the states $(0, i - 1, j + 1, z)$ in MS authentication in UMTS event. Therefore,

$$\pi_{(0,i,j,z)} = \frac{\lambda_u}{\mu_u+\lambda_u}\pi_{(0,i-1,j+1,z)} \quad (5)$$

I.2) If $i < 0$: The last SQN_{AV} that MS has received from UMTS is smaller than the last SQN_{AV} received from WLAN.

CASE I.2.A) $i = -(a-1)$ or $j = L-2$: The states $(0, i, j, z)$ can be reached from the states $(1, i-1, j+1, z)$ in MS handover from WLAN to UMTS. Thus,

$$\pi_{(0,i,j,z)} = \frac{\mu_w}{\mu_w+\lambda_w}\pi_{(1,i-1,j+1,z)} \tag{6}$$

CASE I.2.B) For all other values of i, with $i < 0$: It is similar to ***I.1.C.1*** and thus,

$$\pi_{(0,i,j,z)} = \frac{\mu_w}{\mu_w+\lambda_w}\pi_{(1,i-1,j+1,z)} + \frac{\lambda_u}{\mu_u+\lambda_u}\pi_{(0,i-1,j+1,z)} \tag{7}$$

SET II) $\delta = 1$: The equations of the second set are similar to those of the first and thus, are not analyzed in details.

II.1) $i < 0$,

CASE II.1.A) $i = -(a+1)$,

II.1.A.1) *If* $i - j \equiv -z(modL)$,

$$\pi_{(1,i,j,z)} = \frac{\lambda_w}{\mu_w+\lambda_w}\pi_{(1,i,j,z+1)} + \frac{\lambda_w}{\mu_w+\lambda_w}\pi_{(1,i-1,j,z+1)} \tag{8}$$

II.1.A.2) Otherwise,

$$\pi_{(1,i,j,z)} = \frac{\lambda_w}{\mu_w+\lambda_w}\pi_{(1,i,j,z+1)} \tag{9}$$

CASE II.1.B) $i = -(j+1)$ and $z = L-1$,

$$\pi_{(1,i,j,z)} = \frac{\mu_u}{\mu_u+\lambda_u}\pi_{(0,a+1,j,z*)} \tag{10}$$

CASE II.1.C) For all other values of i with $i < 0$:

II.1.C.1) If $j \neq L-1$,

$$\pi_{(1,i,j,z)} = \frac{\mu_u}{\mu_u+\lambda_u}\pi_{(0,i-1,j,z+1)} + \frac{\lambda_w}{\mu_w+\lambda_w}\pi_{(1,i-1,j,z+1)} \tag{11}$$

II.1.C.2) If $j = L-1$,

$$\pi_{(1,i,j,z)} = \frac{\lambda_w}{\mu_w+\lambda_w}\pi_{(1,i-1,j,z+1)} \tag{12}$$

II.2) If $i > 0$,

CASE II.2.A) $i = a-1$ or $z = L-2$,

$$\pi_{(1,i,j,z)} = \frac{\mu_u}{\mu_u+\lambda_u}\pi_{(0,i-1,j,z+1)} \tag{13}$$

CASE II.2.B) For all other values of i, with $i > 0$:

$$\pi_{(1,i,j,z)} = \frac{\mu_u}{\mu_u+\lambda_u}\pi_{(0,i-1,j,z+1)} + \frac{\lambda_w}{\mu_w+\lambda_w}\pi_{(1,i-1,j,z+1)} \tag{14}$$

Finally, the sum of the steady state probabilities is equal to 1

$$\sum\sum\sum\sum \pi_{(\delta,i,j,z)} = 1 \tag{15}$$

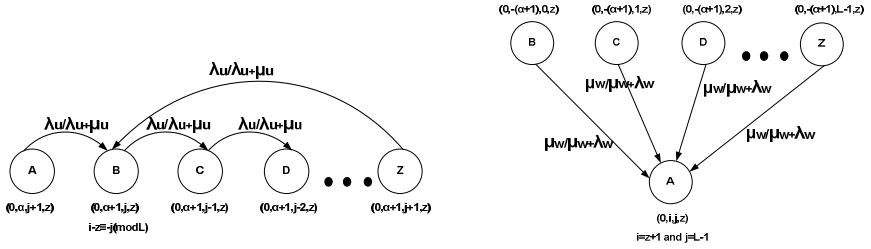

Fig. 5. Transitions examples for: (a) CASE I.1.A and (b) CASE I.1.B

4.4 Solution of Linear System and Derivation of P_{sync}

Equations (1)-(15) comprise a system of linear equations that has a unique solution (i.e., the steady state probabilities), which can be easily calculated using numerical methods. Having obtained the steady state probabilities of the truncated Markov chain, the probability of false synchronization P_{sync} can be calculated as follows. Let $P_{sync,W}$ be the probability of a false synchronization in WLAN, and $P_{sync,U}$ the probability of a false synchronization in UMTS. Considering the false synchronization conditions from UMTS to WLAN (see section 4.1), $P_{sync,W}$ can be derived as, $P_{sync,W} = \Pr[D_k = \alpha + 1$ and the WLAN has at least one AV stored for MS$] \cdot \Pr$ [MS handover from UMTS to WLAN], which is equivalent to:

$$P_{sync,W} = \sum_{z>0,j=0}^{j=L-1} \pi\{N_k = 0, D_k = \alpha + 1, U_k = j, W_k = z\} \cdot \frac{\mu_u}{\mu_u + \lambda_u}$$

Similarly, $P_{sync,U}$ can be derived as $P_{sync,U} = \Pr[D = -(\alpha + 1)$ and UMTS has at least one AV stored for the MS$] \cdot \Pr$ [MS handover from WLAN to UMTS], which is equivalent to:

$$P_{sync,U} = \sum_{j>0,z=0}^{z=L-1} \pi\{N_k = 1, D_k = -(\alpha + 1), U_k = j, W_k = z\} \cdot \frac{\mu_w}{\mu_w + \lambda_w}$$

Finally, we can derive v as $P_{sync} = P_{sync,U} + P_{sync,W}$

To validate the accuracy of the analytical model, a discrete event-driven simulator written in C/C++ was developed. The statistical results collected from the simulation system, after attained the equilibrium state, were averaged to eliminate the randomness effect. It was observed that the maximum related error between the analytical and simulation results was 1%, which verifies the accuracy of the analytical model. The simulation methodology that we followed is analyzed in [4].

5 Conclusions

In this paper we used a generic modeling procedure to solve analytically the problem of false synchronization in 3G-WLAN integrated networks. First, we elaborated on false synchronizations using a numerical example. Using the generic modeling procedure, we developed an analytical solution based on a four dimensional Markov chain. We truncated the state space of the Markov chain in order to derive the steady state equations. Finally, we solved the linear system of equations to derive the probability of a false synchronization. As a future work, we could apply probabilistic model checking to verify the correctness of the analytical model and improve the modeling effectiveness [9].

References

1. 3GPP TS 33.102 (v11.0.0), 3G security; Security Architecture, Release 11 (2011)
2. 3GPP TS 33.234 (v11.2.0), 3G security; WLAN interworking security, Release 11 (2011)
3. Arkko, J., Haverinen, H.: EAP-AKA Authentication. RFC 4187 (January 2006)
4. Ntantogian, C., Xenakis, C., Stavrakakis, I.: Reducing False Synchronizations in 3G-WLAN Integrated Networks. IEEE Transactions on Wireless Communications 10(11), 3765–3773 (2011)
5. Lin, Y.-B., Chen, Y.-K.: Reducing Authentication Signalling Traffic in Third-Generation Mobile Network. IEEE Transactions on Wireless Communications 2(3), 493–501 (2003)
6. Zhang, Y., Fujise, M.: An Improvement for Authentication Protocol in Third Generation Wireless Networks. IEEE Transactions on Wireless Communications 5(9), 2348–2352 (2006)
7. Liang, W., Wang, W.: On Performance Analysis of Challenge/Response Based Authentication in Wireless Networks. Computer Networks, Elsevier Science 48(2), 267–288 (2005)
8. Lin, P., Cheng, S.-M., Liao, W.: Modeling Key Caching for Mobile IP Authentication, Authorization, and Accounting (AAA) Services. IEEE Transactions on Vehicular Technology 58(7), 3596–3608 (2009)
9. Alexiou, N., Deshpande, T., Basagiannis, S., Smolka, S., Katsaros, P.: Formal Analysis of the Kaminsky DNS Cache-Poisoning Attack Using Probabilistic Model Checking. In: IEEE 12th International Symposium on High-Assurance Systems Engineering (HASE), San Jose, CA (November 2010)