Performance Analysis and Analytical Modeling for the Optimization of the Users' Authentication Procedure in 4G Mobile Networks

Christoforos Ntantogian[1]

National and Kapodistrian University of Athens
Department of Informatics and Telecommunications
ntantogian@di.uoa.gr

Abstract. This thesis deals with the optimization of the users' authentication procedure in 4th generation mobile networks. Overall, two different problems are studied. The first problem copes with the false synchronizations issue which is occurred in the users' authentication procedure. An analytical model based on a four-dimensional markov chain is developed to investigate the impact of various network parameters on the system performance. The mathematical model facilitates the dynamic adaptation of the network parameters achieving an optimal tradeoff between security and performance. The second problem deals with the authentication latency and the associated burden of multi-pass authentications. A novel mechanism called security binding is proposed that reduces the authentication delay of multi-pass authentications in a simple yet effective and secure manner. The focal point of the proposed mechanism is its generic application in multi-pass authentications regardless of the underlying network or protocol. The performance improvement of the proposed mechanism is evaluated through extensive simulations and mathematical modeling.

Keywords: 4G mobile networks, user authentication, multi-pass authentication, security binding, markov chain.

1 4G Network Architecture

4G mobile networks are materialized from the gradual integration of heterogeneous wireless and wired networks to a common core network platform, which provides users' and networks' autonomy and supports a wide range of multimedia services in a seamless manner. A 4G network architecture generally consists of three different Network Domains (NDs) (see fig. 1): (i) ND1 that includes the different Radio Access Networks (RANs) technologies (e.g., GSM EDGE Radio Access Network (GERAN), UMTS Terrestrial Radio Access Network (UTRAN), Wireless LAN (WLAN) and Worldwide Inter-operability for Microwave Access (WiMAX)); (ii) ND2 that comprises the core network and performs administrative tasks such as mobility

[1] Dissertation Advisor: Lazaros Merakos, Professor

management, accounting, billing, etc.; and (iii) ND3 that contains the provided network services (e.g., IP Multimedia Subsystem (IMS), Multimedia Messaging Service (MMS), Location Based Services (LBS), etc.).

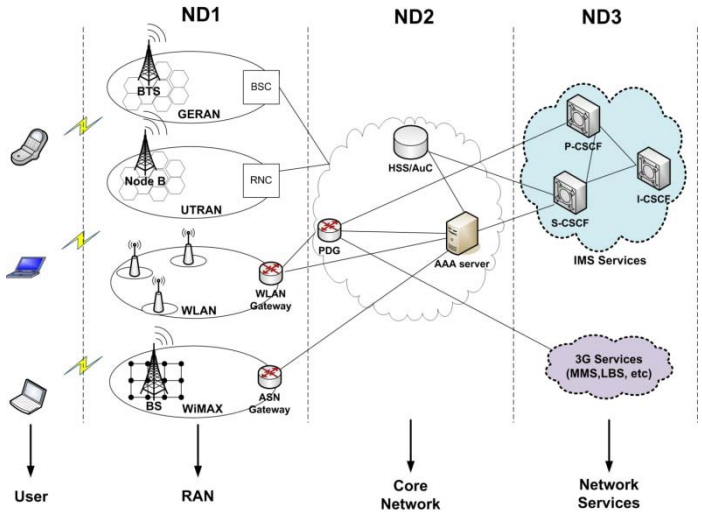

Fig. 1. 4G Network Architecture

2 First Problem - False Synchronizations in 3G-WLAN Integrated Networks

In 3G-WLAN integrated networks a Mobile Station (MS) can handoff from UMTS to WLAN and vice versa according to its connection requirements. When MS resides in UMTS, then it executes the UMTS-AKA protocol, while when it resides in WLAN, it executes the EAP-AKA protocol. The authentication mechanism in these two protocols is exactly the same and it is based on a challenge-response procedure in which the USIM card of MS requests from HSS/AuC (which is located in MS's home network) to generate and send authentication credentials, called 3G authentication vectors. To avoid relay attacks, 3GPP has adopted a mechanism, which ensures that each authentication vector can be used only once. To achieve this, HSS/AuC maintains a counter SQN_{HE} that generates an increasing sequence number SEQ, which is unique for each authentication vector. The sequence number SEQ is conveyed along with the authentication vector to MS. On the other hand, MS keeps track of the greatest sequence number received from the HSS/AuC.

When MS receives an authentication vector through the authentication procedure, it checks if the received SEQ is greatest from the corresponding one stored in USIM. If it is greatest, then the authentication vector has never been used in the past. In this case, USIM accepts the authentication vector and stores the received sequence number SEQ. Otherwise, USIM denies the authentication vector and initiates a re-synchronization procedure. In this procedure, HSS/AuC checks if the values of the

counters are correct and then generates new authentication vectors. It is evident that the re-synchronization procedure increases the authentication latency in the authentication procedure of MS. Especially in case MS has a real time session (VoIP, video conference), then the execution of the re-synchronization procedure could result in session drop [12].

Although this mechanism provides security from replay attacks, 3GPP has recognized cases [3], which the authentication vector received by HSS/AuC may contain a sequence number SEQ, which is smaller than the stored sequence number in the USIM card of MS, without however the specific authentication vector been used in the past. This case is called false synchronization and unfortunately the USIM card rejects the authentication vector and executes the time consuming re-synchronization procedure. In order to resolve the problem of false synchronizations, 3GPP recommends USIM to maintain a matrix SEQ_{ms} for the storage of α values of SEQ which have been accepted from previous authentications. The parameter α is called offset. The symbol $SEQ_{ms}(i)$, denotes the value of the matrix SEQ_{ms} in place i ($0 \leq i \leq \alpha$ -1). In addition, HSS/AuC maintains the counther IND_{HE}, which is increased by one value for each new generated authentication vector and takes values from 0 to α-1.
The procedure that HSS/AuC follows to generate an authentication vector is: initially, HSS/AuC increments by one value the counters SEQ_{HE} and IND_{HE}. Assume SEQ and IND be the new values of the counters SEQ_{HE} and IND_{HE}. Next, HSS/AuC calculates the parameter SQN as follows:

$$SQN = SEQ \;||\; IND$$

HSS/AuC derives also the expected response XRES, the integrity key IK, the cipher key CK, an authentication token AUTN, and a random number RAND. The above procedure is repeated L times for the derivation of L authentication vectors. The parameter L is defined as size of authentication vectors. Next, HSS/AuC forwards to SGSN L ordered authentication based on the sequence number SEQ that contain. SGSN upon receiving the L authentication vectors, chooses the first vector and conveys the parameters RAND and AUTN to MS, and stores the remaining $L - 1$ for future use.

MS upon receiving (RAND, AUTN), derives SQN from AUTN and from SQN derives sequence number SEQ as well as the IND parameter. USIM using IND checks if SEQ_{MS} (IND) < SEQ. If yes, then SIM accepts the authentication vector, since it considers to be fresh and stores the received SEQ in place i=IND of the matrix SEQ_{MS} (i.e., $SEQ_{MS}(i)$=SEQ). Otherwise (i.e., SEQ_{MS} (i) > SEQ), USIM rejects the authentication vector and initiates the re-synchronization procedure. In this procedure, SGSN deletes the stored authentication vectors for the specific MS (if it has any) and executes and requests from the HSS/AuC new authentication vectors.

Although this mechanism reduces false synchronizations, the use of a constant value of offset α is not the optimum strategy to reduce false synchronizations in 3G-WLAN integrated networks. This observation stems from the fact that in 3G-WLAN networks, MS can handoff frequently between 3G and WLAN and as a result, the sequence numbers SEQ deviate from the correct order, increasing false synchronizations.

In order to reduce false synchronizations in 3G-WLAN integrated networks, one possible solution is to choose a big value of offset α. However, by increasing the value of offset α, the level of security in UMTS and WLAN is decreased [12]. Thus, a

mechanism is required that will dynamically adapt the value of offset α in 3G-WLAN integrated networks to achieve an optimal tradeoff between security and performance. In the next section, we summarize the developed analytical model and we outline the most important numerical results.

2.1 Analytical Model and Numerical Results

The aim of the analytical model is to derive the false synchronization probability P_{sync} and the mean number of false synchronization $E[X_\tau]$ during time period τ. For the system modeling, we assume that the MS residence time in UMTS and WLAN follows an exponential distribution with mean $1/\mu_u$ and $1/\mu_w$ respectively and the authentication request rate in the UMTS and WLAN is a poisson process with rate λ_u and λ_w respectively. Under these assumptions, the system behavior can be modeled as a discrete time four-dimensional markov chain $E = \{N, D, U, W: N \in [0,1],\ D \in (-\alpha - 1, \alpha + 1),\ U \in [0, L),\ W \in [0, L)\}$ where N is a variable that denotes if the user is in UMTS or in the WLAN network, D denotes the difference between the sequence numbers of the UMTS and WLAN networks, U denotes the number of the stored authentication vectors in UMTS and, finally, W denotes the number of the stored authentication vectors in the WLAN. Since the markov chain is ergodic, we can first derive the steady state probabilities, and next, the false synchronization probability as follows:

$$P_{sync} = \sum_{D=a+1, W\neq 0} \pi_{(0,D,U,W)} \cdot \frac{\mu_u}{\mu_u + \lambda_u} + \sum_{D=-(a+1), U\neq 0} \pi_{(1,D,U,W)} \cdot \frac{\mu_w}{\mu_w + \lambda_w} \quad (1)$$

The mean number of false synchronization $E[X_\tau]$ during a specific time period t can be calculated as follows:

$$E[X_\tau] = n \cdot P_{sync} \quad (2)$$

where n is the number of authentications during t. In order to ensure the validity of the analytical model, we have carried out simulations using a simulation model implemented in C/C++ programming language. Numerical results showed that the maximum error between the results of the analytical and the simulation model is 1%. Therefore, the analytical and simulation models are consistent.

Based on equation 2, fig. 2 plots the mean number of false synchronizations $E[X_\tau]$ as a function of offset α for different values of λ_u. It is evident that the mean number of false synchronizations is a decreasing function of α. We also observe that if λ_u is increased, then $E[X_\tau]$ is also increased. Finally we can pinpoint that there is a value of α with which $E[X_\tau]$ becomes a constant function of α. We define this value of α as $\alpha_{optimum}$. The value of $\alpha_{optimum}$ is dynamic and depends on the traffic patterns of the MS (i.e., $\lambda_u, \lambda_w, \mu_u, \mu_w$.). For example, if $\lambda_u = 5\mu_u$, then $\alpha_{optimum} = 35$, while when $\lambda_u = 20\mu_u$ then $\alpha_{optimum} = 80$ (see fig. 2). Similar results are observed for other values of $\lambda_u, \lambda_w, \mu_u, \mu_w$.

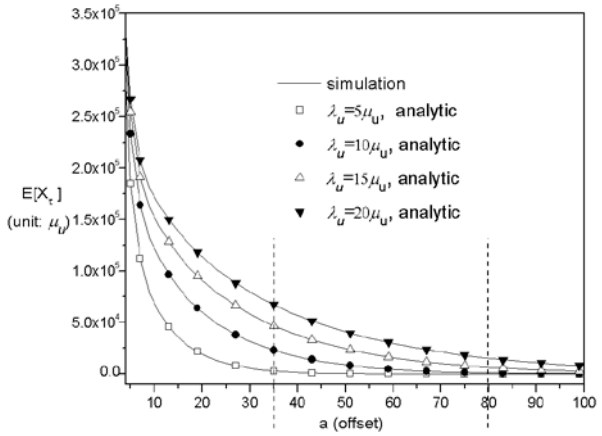

Fig. 2. Mean number of false synchronization $E[X_\tau]$ as a function of offset $\boldsymbol{\alpha}$ for different values of λ_u ($L = 5$ and $\lambda_w = \mu_u = \mu_w$)

Fig. 3 plots the mean number of false synchronizations as a function of the offset α for different values of the size L of authentication vectors. It is assumed that $\lambda_u = 5\lambda_w$. It is observed that when α is smaller than L, then the mean number of false synchronizations has its maximum value. For instance, when $L = 40$ and $\alpha < 40$, then the mean is equal to $E[X_\tau] = 5.5 \cdot 10^5 \mu_u$ (see fig. 3). This result is a direct consequence of the fact that when the value of α is too small, then any execution of an AVR procedure either in UMTS or WLAN, leads to the execution of the re-synchronization procedure. Moreover, similarly to fig. 2, for all values of L, there is value of a, in which the mean number of false synchronizations becomes a constant function of α. For example, when $L = 10$, then $\alpha_{optimum} = 20$, while when $L = 40$ τότε $\alpha_{optimum} = 38$(see fig. 2). Finally, it is observed that when L is increased, then the mean number of false synchronizations is also increased. This happens because an increase of the value of L entails an increase of the counter SEQ_{HE} maintained by HSS/AuC resulting in more frequent false synchronizations.

From the previous results, we can deduce that the mean number of false synchronizations is a decreasing function of α. Thus, the optimum strategy of MS is to tune dynamically the value of α based on the parameters $\lambda_u, \lambda_w, \mu_u, \mu_w$ and L, in order to $a = \alpha_{optimum}$. The value of α must never be greater than $\alpha_{optimum}$, since increasing α beyond $\alpha_{optimum}$ does not reduce significantly the mean number of false synchronizations but reduces considerably the security level in 3G-WLAN integrated networks and the storage overhead in the USIM card. The mechanism that will adapt the value of a can be implemented either in the MS's device or in the 3G-WLAN integrated network. In the latter case, the 3G-WLAN network must keep track of the $\lambda_u, \lambda_w, \mu_u, \mu_w$ values, while it will convey the value $\alpha_{optimum}$ in the AMF payload of the authentication vectors.

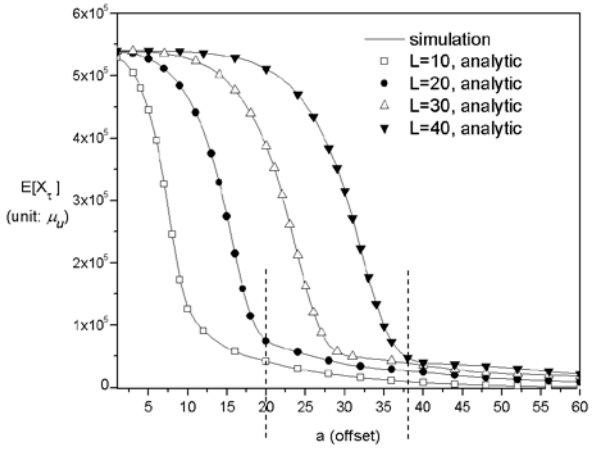

Fig. 3. Mean number of false synchronizations $E[X_\tau]$ as a function of offset $\boldsymbol{\alpha}$ for different values of L ($\lambda_u = 5\lambda_w$ and $\lambda_w = \mu_u = \mu_w$)

3 Second Problem – Multi Pass Authentications

Although 4G networks offer great prospects in network evolution, they also present some serious operational drawbacks, driven mainly by the integration of different technologies. One of these drawbacks is related to the users' authentication through the multiple network domains. More specifically, a user, in order to get access to the network services, has to perform one authentication step for each domain, called as multi-pass authentication.

In a generic form, the user multi-pass authentication includes three discrete authentication steps: (i) an initial authentication step that establishes a wireless connection between the user and ND1 (i.e., the RANs); (ii) a second authentication step that registers the user to ND2 (i.e., the core network); and (iii) a third authentication step that provides the user access to the network services. These steps include a redundant repetition of the same or similar authentication functions, which imposes an unnecessary overhead that is related to: (i) the computation and verification of authentication values (e.g., signatures, Hash Message Authentication Codes (HMAC), etc.); (ii) the generation of security keys; (iii) the exchange of authentication messages; and, (iv) the encryption and decryption of authentication messages. This overhead causes pointless delays in users' authentication, especially in cases that users reside far away from their home network [25]. Moreover, it increases the energy consumption and depletes the available computational resources at the level of mobile devices, which are usually characterized by low processing capabilities and limited energy power. Finally, the redundant exchange of authentication messages entails a needless consumption of the available radio

resources. Thus, the multi-pass authentication has detrimental effects on the quality of service offered to end users.

The user multi-pass authentication occurs in many 4G scenarios. For example, a WLAN user that wants to get access to IMS services (3G-WLAN scenario) should perform a multi-pass authentication that includes three authentication steps (see section 6.1.5 of [4] and section 6.1 of [7]). In the initial step, the user executes the EAP-AKA or EAP-SIM protocol that registers it to the WLAN domain. In the second step, it executes the Internet Key Exchange version 2 (IKEv2) protocol that encapsulates EAP-AKA or EAP-SIM, which registers it to the 3G Public Land Mobile Network (PLMN) domain. Finally, in the third step, it executes IMS-AKA using the Session Initiation Protocol (SIP) for registration within the IMS domain. In the 3G-WLAN scenario, the second authentication step includes a duplicated execution of EAP-AKA (or EAP-AKA), while the third step includes a redundant execution of IMS-AKA. A multi-pass authentication (i.e., two step authentication) also occurs in WiMAX (see section 7.8.2 of [1]). In the initial step of this scenario, the user executes an RSA-based authentication for its device authentication within the WiMAX Base Station (BS). In the second step, it executes an Extensible Authentication Protocol (EAP) method for the user's authentication within the WiMAX core network. Moreover, a multi-pass authentication also occurs in the Unlicensed Mobile Access (UMA) networks, where a user wants to have access to the GPRS or UMTS services using the UMA technology (see section 7.5 of [5]). In this scenario, the user first performs an initial authentication step to be registered in RAN (i.e., IP access network). Then, it performs a second step with the Generic Access Network Controller (GANC) in order to use the UMA technology. Finally, it performs a third step to get access to the core network. Another scenario, where multi-pass authentication is employed, is when a WLAN user wants to get access to 3G services, e.g., MMS, LBS, etc (see section 6.1.5 of [4]). In this scenario, the user performs an initial authentication step to be registered within WLAN and then it performs a second step to be registered within the 3G PLMN domain. Finally, a multi-pass authentication also takes place in cases that a UMTS user wants to get access to IMS services (see section 6.1 of [6]). In this scenario, the user performs an initial authentication step to be registered within the UMTS network and then, it performs a second step with the IMS network to gain access to the IMS services [10].

3.1 Proposed Mechanism

To limit the execution of the redundant authentication functions of multi-pass authentications, a security binding mechanism is proposed. The proposed mechanism authenticates a user in the second and third step of a multi-pass authentication procedure by using the user's authentication credentials of the initial step, in a simple yet effective and secure manner. In this way, it reduces the overall authentication signaling traffic of multi-pass authentications and mitigates the associated burden. The proposed mechanism is deployed through two different forms: (i) the security identity binding and (ii) the security key binding. Both of them can be applied either in the second or third step of multi-pass authentications. The security identity binding enables ND2 or ND3 (of a 4G network architecture) to authenticate a user using the

identity of the user (ID_1user) employed in the initial authentication step. The security key binding enables ND2 or ND3 to authenticate a user using the key (K_1auth) generated in the initial step. The focal point of the proposed mechanism is its generic application in multi-pass authentications, regardless of the underlying network architecture or protocols.

To prove this, we have applied the proposed mechanism in the legacy 3G-WLAN authentication resulting in the improved 3G-WLAN authentication. We have performed a security analysis to identify and elaborate on possible attacks that threaten the operation of the improved procedures, the users and the underlying network. We examined the feasibility of these attacks and, if required, we proposed security measures to defeat them. We concluded that the proposed procedures retain the same security level with the legacy procedures. In addition, we have performed simulations to estimate and compare the performance of the improved 3G-WLAN authentication to that of the legacy 3G-WLAN authentication. The simulation results indicated that the improved procedure achieves reduced authentication delays compared to the legacy procedure, as a direct consequence of the reduced number of authentication messages exchanged. In the next section we analyze the most important results of the carried simulations.

3.2 Results and Discussion

In the first set of experiments, the authentication delay was estimated as a function of the rate of authentication requests λ_{auth} (see fig. 4). It can be deduced that for small values of the rate of authentication requests (i.e., $\lambda_{auth} < 2$), the authentication delay values are constant (see fig. 4) for both procedures (i.e., about 0.4 seconds for the improved 3G-WLAN authentication and 1.4 seconds for the legacy). The decreased delay of the improved procedure is a direct consequence of the reduced number of authentication messages exchanged and the associated computational overhead. Moreover, it is observed that in the interval of $2 < \lambda_{auth} < 5$, the authentication delay of the legacy procedure increases exponentially, leading to excessive delay values and, eventually, to a system saturation. On the other hand, for the same values of the rate of authentication requests, the authentication delay of the improved 3G-WLAN procedure remains constant. Only under a sufficiently high rate of authentication requests (i.e., $\lambda_{auth} > 5$), the authentication delay of the improved 3G-WLAN authentication procedure increases exponentially, indicating that the system has exceeded its maximum capacity. Therefore, it can be figured out that because of the reduced authentication delay, the improved procedure is capable of fulfilling a greater demand of authentication requests, compared to the legacy. Another benefit of the proposed procedure is that it mitigates bottlenecks in PDG [13]. Recall that PDG is a gateway that connects RAN with the core network (see fig. 1). Thus all the WLAN traffic is aggregated to PDG, causing bottlenecks that (i) slow down the data flow, (ii) reduce the network capacity and (iii) impede the system scalability. The proposed procedure copes with bottlenecks in PDG, since it significantly reduces the total amount of authentication messages that are conveyed and processed by it. Moreover, the reduced number of messages exchanged for users' authentication in the improved procedure, optimizes the bandwidth utilization over the wireless and core network

segments. This also entails a reduced computational and energy cost at the level of mobile devices, which avoid the execution of authentication functions and the associated security algorithms (i.e., encryption/decryption, computation/verification of hash values, etc.).

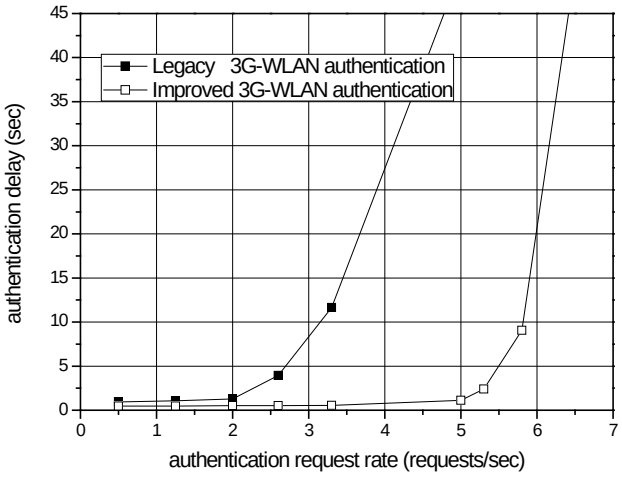

Fig. 4. Authentication delay as a function of the rate of authentication requests

The aim of the second set of experiments was to compute the ratio R_{AVR} of the *AVR* procedures in the improved 3G-WLAN authentication to those in the legacy procedure, as a function of *L*. In the carried experiments, the rate of authentication requests is constant (i.e., λ_{auth}=1 req./sec), since the ratio of *AVR* procedures is independent of λ_{auth}. The outcome of this experiment was that the ratio R_{AVR} of *AVR* procedures is constant (i.e., its value is about $R_{AVR}\approx 0.33$) and independent of *L*. This outcome is directly linked to the fact that for each user's authentication, the legacy 3G-WLAN authentication consumes three 3G AV (one for each authentication step), while the improved consumes only one. Thus, it can be figured out that the improved 3G-WLAN authentication reduces the executions of the *AVR* procedure by 66%, compared to the legacy. It is evident that the reduced number of execution of *AVR* entails reduced authentication delays, since the AAA server and P-CSCF communicate less frequently with HSS/AuC. Moreover, the proposed procedure reduces the authentication latency of roaming users, which reside far away (in terms of number of hops) from their HSS/AuC. Note that when an AVR procedure is performed, the AAA server or S-CSCF communicates with HSS/AuC. The latter is always located in the users' home network, since it stores the users' authentication credentials. Therefore, roaming users experience long authentication delays during an AVR procedure. Thus, the proposed procedure is especially beneficial for roaming users, since it reduces the execution of AVR procedures and, consequently, the authentication latency. In addition, it mitigates the communication and processing overhead in HSS/AuC. This enables HSS/AuC to reserve resources in order to fulfill *AVR*s generated by other types of networks (e.g., UMTS, GSM, GPRS, etc.), which

are also connected to the 4G network and served by the same HSS/AuC. Therefore, the improved authentication procedure optimizes the performance of the entire 4G network architecture as well as the individual networks that the latter comprises.

4 Conclusions

In this thesis two different problems were studied, aiming at optimizing the users' authentication procedure in 4G mobile networks. In the first problem, we studied false synchronizations that occur during handovers from UMTS to WLAN and vice versa. We argued that a constant value of the offset a does not reduce efficiently the number of false synchronizations. Thus, a mechanism is required to adapt dynamically the value of a based on the traffic patterns of the MS. To this end, an analytical model was developed using a four dimensional markov chain. The analytical model facilitates the dynamic adaptation of the value of offset a, to achieve an optimal tradeoff between security and performance. This mechanism can be implemented either in the MS's device or in the 3G-WLAN network infrastructure.

In the second problem, the security binding mechanism was proposed to mitigate the redundant authentication functions of multi-pass authentications. The focal point of the proposed mechanism is that it does not require modifications in the 4G network architecture or in the existing security protocols. The proposed mechanism was applied in the legacy 3G-WLAN authentication resulting in the improved 3G-WLAN authentication. A security analysis was conducted to pinpoint possible attacks that target the users and the underlying network. This analysis showed that the improved procedure that does not undermine the provided security level. A performance analysis was carried out simulations to estimate and compare the performance of the improved 3G-WLAN authentication to that of the legacy 3G-WLAN authentication. The simulation results indicated that the improved procedure achieves reduced authentication delays compared to the legacy procedure, as a direct consequence of the reduced number of authentication messages exchanged and associated computational overhead.

References

1. IEEE 802.16-2004, "IEEE Std 802.16-2004; IEEE Standard for Local and Metropolitan Area Networks Part 16: Air Interface for Fixed Broadband Wireless Access Systems," 2004.
2. 3GPP TS 23.234 (v8.0.0), "3GPP System to WLAN Interworking; System description", Release 8, 2008.
3. 3GPP TS 22.100 (v3.7.0), "UMTS Phase 1 Release '99", Oct. 2001.
4. 3GPP TS 33.234 (v8.1.0), "3G security; WLAN interworking security; System description", Release 8, Mar. 2008.
5. 3GPP TS 43.318 (v8.3.0), "Generic Access Network (GAN); Stage 2", Release 8, 2008.
6. 3GPP TS 23.228 (v8.7.0), "IP Multimedia Subsystem; Stage 2", Release 8, 2008.

7. 3GPP TS 33.203 (v8.5.0), “3G security; Access security for IP based services”, Release 8, 2008.
8. 3GPP TS 33.102 (v.8.1.0), “3G Security; Security architecture”, Release 8, 2008.
9. 3GPP TS 29.002 (v. 8.8.1), “Mobile Application Part (MAP) specification”, Release 8, 2008.
10. Y.B. Lin, M.F. Chang, M.T. Hsu, L.Y. Wu, “One-pass GPRS and IMS Authentication Procedure for UMTS”, IEEE Journal on Selected Areas in Communications, Vol. 23, No. 6, pp 1233-1239, Jun. 2005.
11. Y.B. Lin, Y.K. Chen, “Reducing Authentication Signalling Traffic in Third-Generation Mobile Network”, IEEE Transactions on Wireless Communications”, Vol.2, No. 3, pp 493-501, May 2003.
12. M. Zhang and Y. Fang, “Security analysis and enhancements of 3GPP authentication and key agreement protocol”, IEEE Transactions on Wireless Communication, Vol.4, No.2, 734-742, March 2005.
13. Sung-Min Oh, Jae-Hyun Kim, You-Sun Hwang, Hye-Yeon Kwon, and Ae-Soon Park, “End-to-End QoS Guaranteed Service in WLAN and 3GPP Interworking Network”, 9th Asia-Pacific Network Operations and Management Symposium (APNOMS 2006), Busan, Korea, Sept. 2006.
14. Christoforos Ntantogian, Christos Xenakis, “Reducing Authentication Traffic in 3G-WLAN Integrated Networks”, IEEE 18th International Symposium on Personal, Indoor and Mobile Radio Communications, (PIMRC), Athens, Greece, Sep 2007.
15. Christoforos Ntantogian, Christos Xenakis, Ioannis Stavrakakis, "Reducing the User Authentication Cost in Next Generation Networks", 5th Annual Conference on Wireless On demand Network Systems and Services (WONS 2008), Garmisch-Partenkirchen, Germany, Jan 2008.
16. Christoforos Ntantogian, Christos Xenakis, Lazaros Merakos, “An Enhanced EAP-SIM Authentication Scheme for Securing WLAN”, 15th IST Mobile & Wireless Communications, Mykonos, Greece, June 2006.
17. Christoforos Ntantogian, Christos Xenakis, "A Security Binding for Efficient Authentication in 3G-WLAN Heterogeneous Networks", PhD poster presented in the 6th Annual Mediterranean Ad Hoc Networking Workshop (Med-Hoc-Net 2007), Corfu, Greece, June 2007.
18. Christoforos Ntantogian, Christos Xenakis, "A Security Protocol for Mutual Authentication and Mobile VPN Deployment in B3G Networks", In Proc. 18th Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, (PIMRC 2007), Athens, Greece, Sept 2007.
19. Christoforos Ntantogian, Christos Xenakis, Ioannis Stavrakakis, "Efficient Authentication for Users Autonomy in Next Generation All-IP Networks", In Proc. In Proc. 2nd International Conference on Bio-Inspired Models of Network, Information, and Computing Systems (BIONETICS 2007), Budapest, Hungary, Dec 2007.
20. Christoforos Ntantogian, Christos Xenakis, “One pass EAP-AKA Authentication in 3G-WLAN Integrated Networks", Wireless Personal Communications, Springer, Vol. 48, Issue 4, pp: 569-584, March 2009.
21. Christos Xenakis, Christoforos Ntantogian, Ioannis Stavrakakis,“A Network Assisted Mobile VPN deployment for UMTS", Computer Communications, Elsevier, vol. 31, No. 14, pp. 3315-3327, September 2008.
22. Christoforos Ntantogian, Christos Xenakis, “Security Architectures for B3G Mobile Networks,” book chapter in “Handbook of Research on Wireless Security,” Information Science Reference (2008), editor: Yan Zhang, Jun Zheng, Miao Ma, ISBN: 978-1-59904-899-4.

23. Christoforos Ntantogian, Christos Xenakis, “A Generic Mechanism for Efficient Authentication in B3G Networks”, Computer and Security, Elsevier, (accepted for publication).
24. Χριστόφορος Νταντογιάν, Χρήστος Ξενάκης, «Μηχανισμοί Προστασιας της Ιδιωτικοτητας των Χρηστών στα Δικτυα $4^{ης}$ Γενιας», κεφάλαιο στο βιβλίο: « Προστασία της Ιδιωτικότητας στις Τεχνολογίες Πληροφορικής και Επικοινωνιών: Τεχνικά και Νομικά Θέματα», Εκδόσεις Παπασωτηρίου, συντάκτες: Κωνσταντίνος Λαμπρινουδάκης, Λίλιαν Μήτρου, Στέφανος Γκρίτζαλης και Σωκράτης Κάτσικας. (υπό έκδοση).
25. Christos Xenakis, Christoforos Ntantogian, “Security Architectures for B3G Mobile Networks”, Telecommunication Systems, Springer, Vol.35, pp: 123-139, Aug. 2007.