Authentication Transmission Overhead Between Entities in Mobile Networks

Ja'afer AL-Saraireh and Sufian Yousef

Faculty of Science and Technology, Anglia Ruskin University, UK

Abstract
This paper analyses the authentication and key agreement (*AKA*) protocol for UMTS mobile networks, where a new authentication protocol which is able to reduce the network traffic and signaling message between entities, and consequently the bottleneck at authentication centre is avoided, this is achieved by reducing the number of messages between mobile and authentication centre, and then reducing the authentication times and setup time as well as improveing authentication efficiency as shown in numerical analysis and simulation results. In this paper we propose dynamic length (*L*) for an array for authentication vector (*AV*). This required designing new technique to predict the numbers of records in *AV* in each authentication data request depending on the to arrival rate of authentication events and residence time of *MS* in *VLR/SGSN*. The proposed ***AKA*** with dynamic ***L*** for ***AV*** is compared with the current ***AKA*** with fixed length for ***AV***.

Keywords:
AuC, Authentication, UMTS, Authentication Vector.

Introduction

In order to provide security services in wireless networks, authentication is used as an initial process to authorize a mobile terminal for communication through secret credentials [4]. Authentication procedure is executed when the MS moves from one registration area (*RA*) to another one (location update), call origination and call termination. The MS is continuously listening to the broadcast message from VLR/SGSN to identify the location area by using location area identity (*LAI*), and the MS comparing the LAI which is received with the *LAI* stored in the USIM. When the *LAI* is different then the MS execute authentication procedure.
Recently [1] discussed reducing authentication signalling in 3G mobile networks, and proposed an automatic selection mechanism that dynamically selects the length (*L*) of the array to reduce the network cost [1].

2. UMTS AKA Authentication Protocol

Figure 1 describes authentication procedure in 3G. The following steps describe the procedure [7]:

1. When the ***MS*** moves to new ***VLR/SGSN*** area then MS sends (***IMSI***) authentication request to ***VLR/SGSN*** (Visitor Location Register/Serving GPRS Support Node).
2. ***VLR*** passes this authentication request to ***HLR***.
3. ***HLR*** Generates authentication vectors ***AV(1..n)*** and sends authentication data response ***AV(1..n)*** to ***VLR/SGSN***.
4. ***VLR*** stores authentication vectors. In the i^{th} authentication and key agreement procedure, ***VLR/SGSN*** selects the i^{th} authentication vector ***AV(i)***, and sends (***RAND (i), AUTN(i)***) to ***MS***. In the ***VLR*** one authentication vector is needed for each authentication instance. This means that the signaling between ***VLR*** and ***HLR/AuC*** is not needed for every authentication events.
5. ***MS*** computes the response $RES = f_2(K, RAND)$, and $CK = f_3(K, Rand)$, and sends ***RES to VLR/SGSN***.
6. ***VLR*** compares the received ***RES*** with ***XRES***. If they match, then authentication is successfully completed.

The transmission between the ***HLR/AuC*** and ***VLR/SGSN*** is usually expensive, if increasing the number ***L*** of ***AVs*** in then reduces the number of transmissions. But, if ***L*** is too large, the ***AVs*** will consume network bandwidth. In the 3G standard, ***L*** is fixed at 5 records. In our analysis we assume that the link between ***VLR/SGSN*** is secure when it is belonging to the same network and insecure when it belongs to different networks. When the ***MS*** moves from one ***VLR/SGSN*** to another in the same network, then the new ***VLR/SGSN*** requests the unused ***AVs*** from the old ***VLR/SGSN***. If the unused ***AVs*** has formed 25% from the ***AV***, the old ***VLR/SGSN*** deletes all ***AVs*** relating to this ***MS***. But when unused ***AVs*** formed less than 25%, the new ***VLR/SGSN*** requests new ***ADRs***.
When ***MS*** moves to new ***VLR/SGSN*** that belongs to other networks, then the new ***VLR/SGSN*** sends and receives authentication data request and response (***ADR***) message to get new ***AV*** to/from ***HLR/AuC***.

The following procedure process of authentication event with data time diagram is shown in Fig. 2.

*There are two counter **i** and **j**, set the initial value for them is 0.*
MS generates events (Location update, Call origination and Call termination).
VLR/SGSN check the event
If event is Location Update then
*Increment the two counter **i** and **j** by 1*
At time $T_{i,j}$ execute ADR_i, and UAR_j

Else if event is call originator or termination then
*If there AVs available in VLR/SGSN (i.e. j less than or equal **L**)*
*Increment counter **j** by 1*
At time $T_{i,j}$ execute UAR_j
Else
*Set initial value for counter **j** (i.e. **j**=1)*
*Increment counter **i** by 1*
At time $T_{i,j}$ execute ADR_i,and UAR_j
End if
End if

From above algorithm, when the MS moves to new VLR/SGSN at time T_{N+1} and the last authentication event occurs at $T_{N,i}$ $(where\, 1 \le i \le L)$ then during the period $T_{N,i} - T_{1,1}$ there are L-i records in VLR/SGSN that are unused, N ADRs and (N – 1)*L + I UARs are performed.

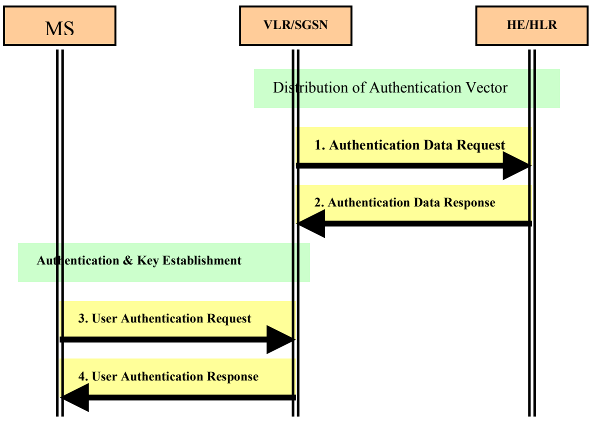

Figure 1 Authentications and Key Agreement Protocol

3. Analytical Model for the Current AKA with Fixed Length (L) for AVs

The Poisson distribution formula can be used to determine the probability of authentication events arriving such as location update (registration), call origination and call termination. Let λ be the constant that represents the average rate of arrivals event. According to Poisson probability in an interval of length ***T***, the probability of mass function (***pmf***) is

$$P\{X = k\} = P(k) = \frac{e^{-\lambda T}(\lambda T)^k}{k!} \quad \text{Where k=0,1,2...} \quad \textbf{(1)}$$

And the cumulative distribution function (***cdf***) is

$$P\{X \le k\} = G(x) = \sum_{K=1}^{x} \frac{e^{-\lambda T}(\lambda T)^k}{k!} \quad \textbf{(2)}$$

We evaluate the performance of 3G authentication protocol. The evaluation methodology is drawn from [1]. Assume that a ***MS*** makes a number of ***ADRs*** which satisfy a Poisson distribution with mean λ. According to the equation (2) for period ***T***, there is ***(N-1)*L + i UARs***, then the probability that there are ***N ADRs*** to the ***HLR/AuC*** is

$$\Theta(N,L,T) = \sum_{i=1}^{L} \left\{ \frac{(\lambda \tau)^{(N-1)*L+i}}{[(N-1)L+i]!} \right\} e^{-\lambda t} \quad \textbf{(3)}$$

Where $\Theta(N,L,T)$ is the probability that there are n transmissions between the ***MS*** and ***VLR/SGSN*** during the period ***T***. Let the ***MS*** resides for a period ***t*** in ***VLR/SGSN***, $t = T_{N+1} - T_{1,1}$ and ***t*** has exponential distribution with the density function ***f(t)*** and with mean ***1/µ***. The probability that there are ***n ADRs*** during the ***MS*** residence in the ***VLR/SGSN*** is

$$P(N,K) = \int_{t=0}^{\infty} \Theta(N,L,t)\ ?t)\ dt \quad \textbf{(4)}$$

By using Laplace transform function, for a function f(t) defined on $0 \le t \le \infty$, its Laplace transform function is denoted as:

$$\ell\{f(t)\} = F(S) = \int_{t=0}^{\infty} e^{-st} f(t)\,dt \quad \text{Where s is a real number} \quad \textbf{(5)}$$

$$P(N,K) = \sum_{i=1}^{L} \int_{t=0}^{\infty} \left\{ \frac{(\lambda t)^{(N-1)*L+i}}{[(n-1)*L+i]\,!} \right\} e^{-\lambda t}\ ?t)\ dt$$

$$P(N,K) = \sum_{i=1}^{L} \left\{ \frac{(\lambda \lambda t^{(N-1)*L+i}}{[(n-1)*L+i]\,!} \right\} \int_{t=0}^{\infty} t^{(N-1)L+i}\ ?t)\ e^{-\lambda t}\,dt \quad \textbf{(6)}$$

$$P(N,K) = \sum_{i=1}^{L} \left\{ \frac{(\lambda t)^{(N-1)*L+i}}{[(n-1)*L+i]\,!} \right\} (-1)^{(N-1)*L+i} \left[\frac{d^{(N-1)L+i} F(s)}{ds^{(N-1)L+i}} \right] \Bigg|_{s=\lambda} \quad \textbf{(7)}$$

Thus ***N*** is the number of ***ADRs*** that has a Poisson distribution, the average number of ***ADRs*** when the ***MS*** resides in the ***VLR/SGSN*** is

$$E[N] = \sum_{N=1}^{\infty} N * P(N,L) \quad \textbf{(8)}$$

And the total cost for transmission one *AV* is

$$C[L] = E[N].(L + 2.\alpha) \quad \textbf{(9)}$$

Where ***2α*** is the cost of transmission from the ***VLR/SGSN*** to ***HLR/AuC*** to back to the ***VLR/SGSN***. In our paper we assumed that the residence time ***t*** of ***MS*** in ***VLR/SGSN*** is exponential distribution. The general formula for the probability density function (***pdf***) of the exponential distribution is

$$f(x) = \mu . e^{-\mu . t}$$

By using equation (7) and (8) to derive the ***P(n,K)*** and ***E[N]*** for exponential distribution [1], is

$$P(N,K) = \left(\frac{\lambda}{\lambda+\mu}\right)^{(N-1)*L} \left[1 - \left(\frac{\lambda}{\lambda+\mu}\right)^{L}\right] \quad \textbf{(10)}$$

$$E[N] = \frac{1}{1 - \left(\frac{\lambda}{\lambda + \mu}\right)^L} \quad (11)$$

By using equation (9), the total cost of transmission one ***AV*** is

$$C[L] = \frac{L + 2 * \alpha}{1 - \left(\frac{\lambda}{\lambda + \mu}\right)^L} \quad (12)$$

Fig 3, 4 represent our analysis and simulation results. These figures show how the expected ***ADRs*** number ***E[N]*** and the cost of total ***ADRs*** transmission ***C(K)*** are effected by the authentication vector size ***(L)*** and arrival rate ***λ***. When the number of records increased in ***AV*** then the expected number of ***ADRs*** will be decreased. Fig. 3 shows that the relationship between the ***L*** and ***E[N]*** is indirectly proportional, and the relationship between arrival rate ***λ*** and ***E[N]*** is directly proportional. Fig. 4 shows that the relationship between arrival rate ***λ*** and ***C[L]*** is directly proportional. But Fig. 3, 4 and 5 shown that there is optimal value for ***L*** that depends on the arrival rate ***λ***, and if ***L*** is increased more than optimal value for ***L***, then it does not improve the ***E[N]*** performance.

4. Analytical Model for the Proposed AKA with Dynamic length (L) for AVs

Here, we discuss how to select optimal value of ***L*** for ***AV***. These values are affected by the following factors:

1. The residence time of ***MS*** in ***VLR/SGSN***.
2. Number of user authentication requests and response ***UARs*** and Data authentication request and response ***ADRs***.
3. Average rate of arrivals event.

We assumed that there is field in ***HLR/AuC*** that we can store in it the optimal value for ***L*** of ***AV*** for each ***MS***, this value depends on the history of ***UARs*** and ***DARs*** for the ***MS***. For new ***MS*** the initial value for ***L = 5*** as recommended by 3GPP. Here will discuss two cases; one of them is the ***MS*** which stays in the same ***VLR/SGSN*** while ***AV*** is turned out i.e. a new ***ADRs*** is requested, and another case is ***MS*** moving to new ***VLR/SGSN***.

Case 1: *MS* staying in the same *VLR/SGSN*

The ***HLR/AuC*** is responsible for store the issue time T_i for the i[th] authentication data request and response ***ADR***, when ***AV*** is turned out and new ***ADRs*** is requested at time T_{i+1}, then ***HLR/AuC*** compute arrival rate which is equal to the number of UARs are used divided by (T_{i+1} - T_i), and execute the following algorithm to find the optimal value of ***L***. Depending on the arrival rate ***λ*** for the previous ***UARs***, the following procedure is executed to compute ***L***. For example if there are 5 events per 2 minutes then arrival rate = 2.5 events/minutes.

Procedure to find optimal value for the Length of AV

```
        Minimum cost = ∞
        Counter J = 1
        Found = True
While found = True do
        Compute cost for L = J by using equation 12
        If cost [L] Less than minimum cost then
                Optimal value = L
                Minimum cost = cost[L]
                Increment counter J
        Else
                Found = False and stop execution
        End if
End while
```

Fig. 4 illustrate the result of our simulation to get the optimal value ***L*** for $1 \le \lambda \le 40$ and Fig. 6 illustrates the cost for optimal value *L*. In Fig. 4, we have classified the optimal value for each arrival rate ***λ***, But if you take the average of arrival rate then we get most optimal value with optimal cost. The ***HLR/AuC*** compute arrival rate which is equal to the number of UARs used divided by (T_{i+1} - T_i), let the computed arrival rate is λ_{i+1}. Then calculate the average arrival rate $\lambda_{av} = (\lambda_i + \lambda_{i+1})/2$ and then execute the above algorithm to find optimal value of L as shown in Fig. 6.

Case 2: *MS* moving to new *VLR/SGSN*

In this case, they will find the optimal value of ***L***, when ***MS*** moves from ***VLR/SGSN*** to new ***VLR/SGSN***. The ***VLR/SGSN*** is responsible to count the number of ***UAR***s which are executed during the time ***MS*** stayed in it. When the ***MS*** moves to new ***VLR/SGSN*** or detaches from the network, then the old ***VLR/SGSN*** must provide the number of ***UARs*** to the ***HLR/AuC***. Also the ***HLR/AuC*** is responsible for storing the last optimal value of ***L*** that is assigned to ***MS***. However, the initial optimal value assigned to ***MS*** when the first time is **5** as suggested by 3GPP. Let ***MS*** is staying in j[th] ***VLR/SGSN*** and ***L(j)*** is the optimal value that is selected to ***MS*** and there are ***N*** of ***UARs*** are counted by j[th] ***VLR/SGSN***. When the ***MS*** leaves the j[th] ***VLR/SGSN*** area, then the optimal value of ***L*** must be computed by ***HLR/AuC*** and generate ***AV*** with optimal size ***L***. The new value of ***L*** is computed as following

$$L(j+1) = \begin{cases} L_1 = L(j) \quad or \\ L_2 = L(j) - 1 \quad or \\ L3 = L(j) + 1 \end{cases}$$

This depends to the average of cost for L_1, L_2 and L_3, where the cost of L_i, where $1 \le i \le 3$ is computed according the following formula:

$$C_i = \frac{N}{L_i} * (L_i + 2\alpha) \qquad for\ i = 1,2,3$$

Then

$$L(j+1) = L_s \ where \ 1 \le s \le 3, \quad and \ C_s \ is \ neareast \ to \ \underset{1 \le i \le 3}{Average} \ C_i$$

As shown in Fig. 7, the costs of L_i (c_i), where $1 \le i \le 3$, are close to each other. From our simulation the best performance is achieved when we select L whose is cost close to average, rather than whose cost is minimum. The optimal L is stored in HLR/AuC to be used in next time for initial ADRs.

5. Conclusion

The proposed dynamic length for ***AV*** when compared to the currently used fixed length for ***AV***, found to be reducing the authentication traffic overhead between ***MS*** and authentication centre, and the authentication latency from end user's point of view, and the energy consumption of a mobile terminal. The transmission of ***ADRs*** between ***HLR/AuC*** and ***VLR/SGSN*** is usually expensive; increasing the ***L*** for ***AV*** is reducing the number of ***ADRs*** request. But, if ***L*** is too large, the ***AVs*** may consume network bandwidth for each ***ADRs*** request. From our simulation and analysis, we have shown that increasing the number of records in ***AV*** will decrease the number of ***ADRs,*** but there are limits to increasing ***L***. Also the cost is decreased when ***L*** is increased, but the critical point happens when ***L*** is increased, when cost will be increased as well. Hence we need to stick to choosing an optimal value of ***L*** in ***AV***. The analysis of the model analytically and by simulation has produced an optimal ***L*** in this dynamic ***AV***.

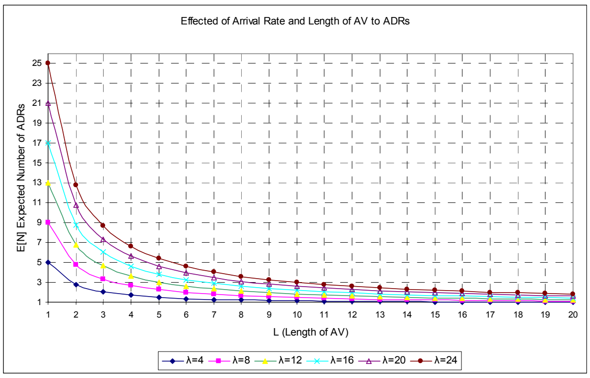

Figure 3 Expected numbers of ADRs during MS resides in VLR/SGSN

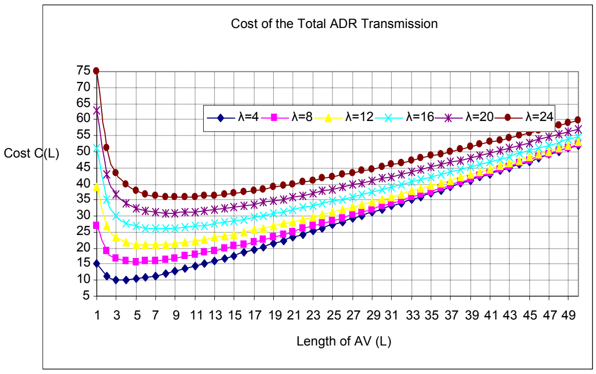

Figure 4 Cost of the Total ADR Transmission

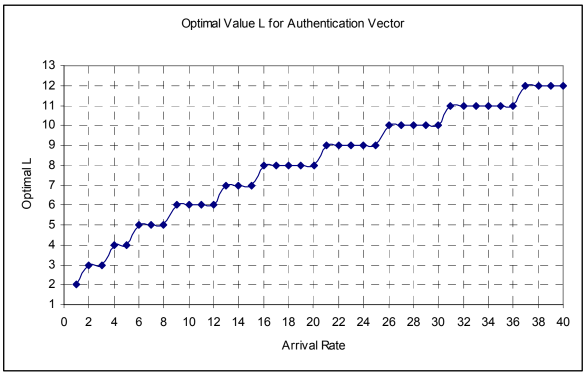

Figure 5 Optimal Values L for Authentication Vector

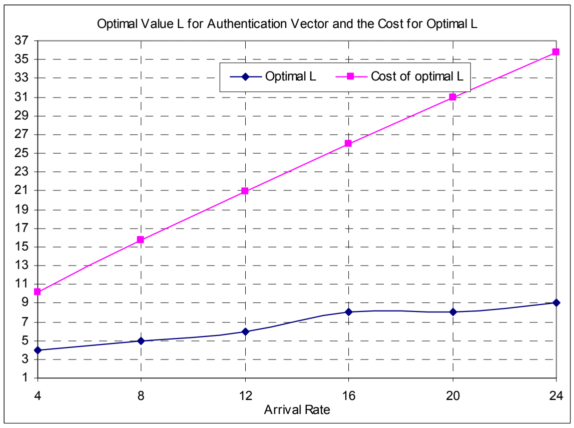

Figure 6 Optimal Values L for Authentication Vector and Cost

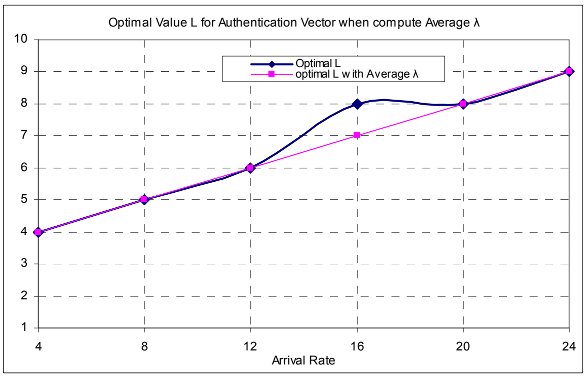

Figure 7 Optimal Values L for Authentication Vector when compute Average λ

References

[1]. Yi-Bing Lin, Yuan-Kai Chen, "Reducing authentication signaling traffic in third-generation mobile network", *IEEE Transactions on Wireless Communications*, vol. 2, no. 3, May 2003 pp. 493-501

[2]. Mark Johnson, "Revenue Assurance, Fraud and Security in 3G Telecom Services", VP Business Development Visual Wireless AB, *Journal of Economic Management*, Fall 2002, Volume 1, Issue 2, www.jecm.org

[3]. L. Salgarelli, M. Buddhikot, J. Garay, S. Patel, and S. Miller. "The Evaluation of wireless LANs and PANs – Efficient Authentication and Key Distribution in Wireless IP Networks". *IEEE Personal Communication on Wireless* Communication 10(6):52-61, December 2003.

[4]. 3GPP TS 21.133. 3GPP Security; Security Architecture.

[5]. Muxiang Zhang and Yuguang Fang "Security Analysis and Enhancements of 3GPP Authentication and Key Agreement Protocol", *IEEE.Transacions on wireless communications*, Vol, 4, NO. 2, March 2005.

[6]. Watson, E.J. "Laplace Transforms and Applications," Birkhauserk, 1981.

Ja'afer AL-Saraireh received the BSc degree in computer science from Mu'tah University, Karak, Jordan, in 1994. He received the MSc degree in computer scinec form University of Jordan, Amman, Jordan, in 2002. He is currentlt a PhD student in the Faculty of Science and Technology at Anglia Ruskin University, UK. His research interests include mobile and wireless network security.