IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received June 4, 2021, accepted June 18, 2021, date of publication July 1, 2021, date of current version July 15, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3094045

Reducing the Overhead Messages Cost of the SAK-AKA Authentication Scheme for 4G/5G Mobile Networks

SHADI NASHWAN[1] **AND IMAD. I. H. NASHWAN**[2]
[1]Computer Science Department, Jouf University, Sakaka 42421, Saudi Arabia
[2]Faculty of Technology and Applied Science, Al Quds Open University, Gaza 860, State of Palestine

Corresponding author: Shadi Nashwan (shadi_nashwan@ju.edu.sa)

ABSTRACT One of the recently proposed authentication schemes for 4G/5G mobile networks is a secure anonymity key of authentication and key agreement scheme (SAK-AKA), wherein the home subscriber server (HSS), mobility management entity (MME), and user equipment (UE) represent authentication entities. In the SAK-AKA scheme, UE authentication is performed through an initial authentication processes session (IAPS) and subsequent authentication processes session (SAPS) phases to ensure that the UE is authorized to use the network services. In IAPS, the MME accesses the HSS to obtain the authentication parameters and takes the delegation from the HSS to execute the authentication process with the UE mutually. Since accessing the HSS is expensive, the HSS generates a number (k) of authentication vectors (AVs) and then sends them back to the MME as one unit at a time. SAPS is then executed (k) times to authenticate the UE without going back to the HSS. Therefore, it is useful to choose a specific value of (k) that would reduce the traffic cost. In this paper, we proposed an analytical cost function model to examine the effect of the (k) value on the transmission cost of authentication processes. The proposed model assumes that the signaling traffic of the SAK-AKA scheme is represented by a Poisson process where the authentication request time has an exponential distribution. This model was analyzed numerically to identify appropriate values of the (k-AVs) that can minimize the overhead messages cost of the SAK-AKA scheme.

INDEX TERMS 3GPP, 4G/5G mobile communication, LTE networks, SAK-AKA scheme, mutual authentication, Poisson process.

I. INTRODUCTION

The long-term evolution (LTE) network was developed by the 3rd generation Partnership Project (3GPP) to achieve interworking between heterogeneous communication systems, higher bandwidths, and wider coverage technology for the fourth generation (4G) and fifth generation (5G) mobile networks [1], [2]. One of the promising authentication schemes proposed to enhance the security features of the LTE network is a secure anonymity key of authentication and key agreement (SAK-AKA) scheme [3]. The SAK-AKA scheme can support attractive security services such as full mutual authentication, perfect forward secrecy, and anonymity services [3]–[7]. Furthermore, the SAK-AKA scheme can resist numerous types of related attacks such as the denial of service (DOS), replay, desynchronization, and man-in-the-middle attacks [8], [10], [11]. The main authentication entities of the SAK-AKA scheme are the home subscriber server (HSS), mobility management entity (MME), and user equipment (UE) [3]. When the UE requests a particular network service such as a location update, call origination, call termination, or multimedia streaming, an authentication process with the network (i.e., MME and HSS) should be performed to validate the service request type and to ensure that the UE is authorized to use such services [9], [12]–[15]. Additionally, the authentication process with the UE in the opposite direction should also be performed. In general, these authentication processes can be executed mutually in the SAK-AKA scheme through the initial authentication processes session (IAPS) and subsequent authentication processes session (SAPS) phases, as shown in Fig. 1.

The associate editor coordinating the review of this manuscript and approving it for publication was Prakasam Periasamy.

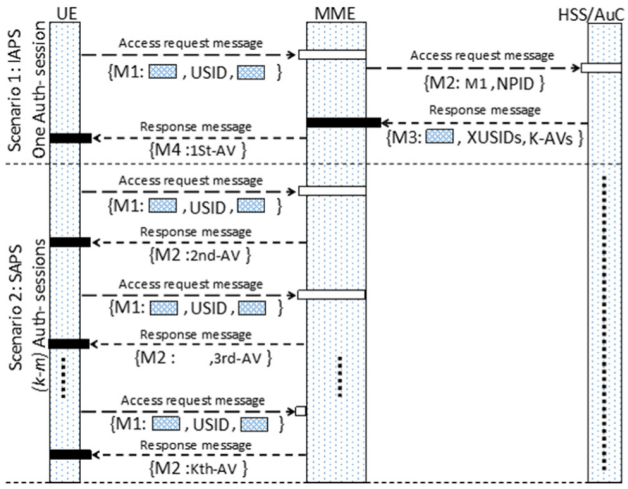

FIGURE 1. Signaling traffic flows of the authentication scenarios.

In the IAPS phase, the MME accesses the authentication center (AuC) in the HSS to obtain the authentication parameters and signals the HSS to execute mutual authentication with the UE. The HSS authenticates the UE and MME using the access request messages that have been sent by the UE (M1) and MME (M2). In the same context, the UE authenticates the network using the content of (M4) as a response authentication message. On the other hand, in the SAPS phase, both the UE and MME authenticate each other directly through the authentication messages (M1) and (M2) as request and response authentication messages. The signaling traffic flows of the authentication procedures can be summarized according to the following authentication scenarios:

Scenario 1: When the MME does not include the authentication data and authentication vectors (AVs) to authenticate the UE as shown in Fig. 1.

1) The UE sends an access request message (M1) to the MME that includes the unique session identifier (USID) that is updated for each authentication session.
2) Upon receiving (M1), the MME computes the network path unique identifier (NPID) and forwards the access request message (M2) to the HSS after adding (NPID) and (M1) to invoke a new burst of the (k-AVs).
3) When the HSS receives (M2), the HSS uses both the (USID) and (NPID) to authenticate the UE and the MME. Then, it generates a burst of (k-AVs) based on the UE's record and the attached authentication parameters in (M1). The HSS then sends the authentication response message (M3), which includes the generated (k-AVs), to the MME. It should be noted that each AV contains the response message (RES), key derivation (KASME), and the authentication token (AUTN). One AV is adequate to execute one authentication session between the UE and MME directly during the SAPS phase without going back to the HSS.
4) Upon receiving the (M3) message, the MME stores the ordered array of (k-AVs) and then forwards (M4) back as a response message, which includes the first AV, to the UE.
5) When the UE receives (M4), the UE checks the freshness of the AV and authenticates the MME.

Scenario 2: When the MME includes the authentication data with $(k-m)$-AVs) to authenticate the UE, where (m) is the used AV's and $(0 \leq m \leq k-1)$, as shown in Fig. 1.

1) The UE sends an access request message (M1), which includes the unique session identifier (USID), to the MME.
2) Upon receiving (M1), the MME authenticates the UE and forwards (M2), which includes the $(k-m)$-AV, back to the UE (start from the end in the previous session).
3) When the UE receives (M2), the UE checks the freshness of the AV and authenticates the MME.

Since accessing the HSS is expensive, the HSS generates a number of (k-AVs) and sends them to the MME one at a time to execute SAPS and authenticate the UE directly $(k-1)$ times. This mechanism reduces the signaling traffic between the HSS and the MME. On the other hand, this method may also be expensive if the size of the (k-AVs) is large. Therefore, it is useful to choose a specific value of (k) to effectively reduce the traffic cost.

This paper proposes an analytical model to examine the effects of the (k) value on the transmission cost of authentication. In this model, the authentication events are represented by a Poisson process [16]–[18]. Then, the cost function of the signaling traffic, whether between MME/HSS or UE/MME, is derived to calculate the optimal (k) value that minimizes the messages overhead according to the expected number of the authentication events.

The remaining parts of this paper are arranged as follows: Section II introduces the cost function of the proposed analytic model for the SKA-AKA scheme where the model is represented by a Poisson process. Section III shows the effects of the (k -AV's) on the authentication events' signaling traffic cost. The optimal values of the (k-AV's) that minimize signaling traffic cost are determined in section IV. Finally, the conclusion is given in section V.

II. THE PROPOSED ANALYTIC MODEL

Consider Fig. 2 to illustrate the timeline diagram of the authentication phases in the SAK-AKA scheme. According to scenario 1, the UE sends an authentication request message to MME at the time $(\tau_{1,0})$. Since the MME does not have the AVs, the 1st IAPS phase is executed to obtain the first burst of (k-AV's). After the MME has obtained the (k-AV's), the 0th SAPS phase is executed to perform the mutual authentication between the MME and UE using the first AV.

After $(\tau_{1,0})$, the second authentication request takes place at the time $(\tau_{1,1})$; the UE initiates the 1st SAPS phase, wherein the MME uses the second AV to achieve mutual authentication without referring back to the HSS.

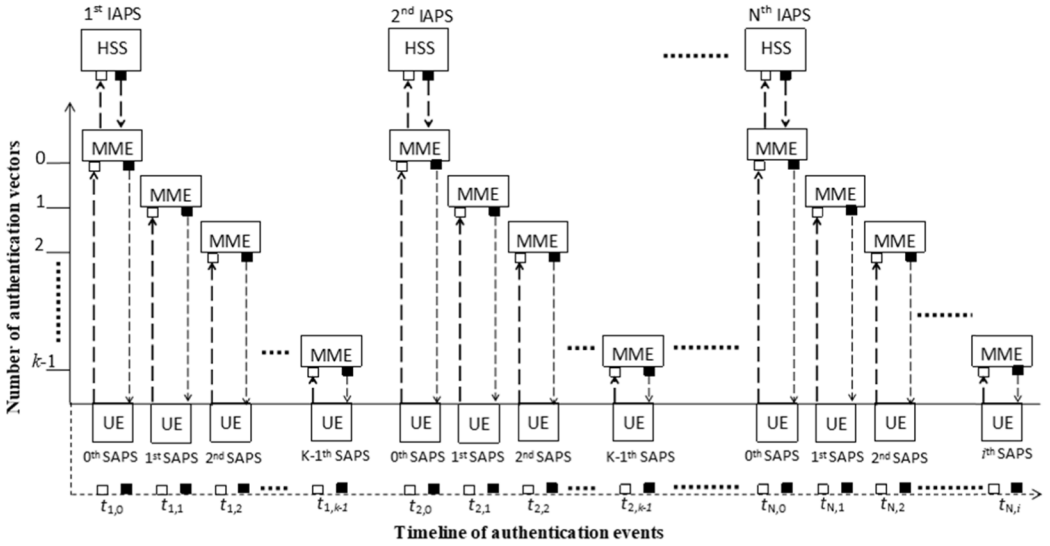

FIGURE 2. Timeline of the authentication events in the SAK-AKA scheme.

At the time $(\tau_{1,k-1})$, the last AV is used to execute the k-1$^{\text{th}}$SAPS phase (i.e., the k^{th} authentication events have been performed). The next authentication event will occur at the time $(\tau_{2,0})$, where the MME recognizes that no AV is available. This leads the MME to execute the 2$^{\text{nd}}$ IAPS phase to obtain the next burst of the (k-AV's), after which the SAPS phase is executed. The next authentication events through the IAPS and SAPS phases are performed as mentioned above.

Suppose that at the time $(\tau_{N,i+1})$, the UE is leaving the area of MME coverage. The last execution of the SAPS phase is performed at the time $(\tau_{N,i})$, where $(0 \leq i \leq k-1)$. This means the SAPS phase has utilized (i-AV's) during the N^{th} IAPS phase. Therefore, from (i-AV's) during the N^{th} IAPS phase. Therefore, from $(\tau_{1,0}$ to $\tau_{N,i+1}))$, the authentication scheme has performed $(k \times (N-1)+i)$ of SAPS and (N) of IAPS phases.

According to scenario 2, the 1$^{\text{st}}$ SAPS starts from time $(\tau_{1,m})$, where $(0 \leq m \leq k-1)$. Scenario 1 is considered a special case of scenario 2 when $(m = 0)$. Suppose that the cumulative of authentication requests and response messages is represented by a Poisson process with rate (λ), $\{N(t) : t \geq 0\}$, where (t) is the time that the UE requests the authentication services.

Let $\Psi(n, k, m, t)$ be the probability that there are n-IAPS for a specific request period (t), since the 1$^{\text{st}}$ SAPS starts at time $(\tau_{1,m})$, where $(0 \leq m \leq k-1)$.

The authentication processes that have been performed through the n-IAPS are $(k-m)$-SAPS in the 1$^{\text{st}}$ IAPS, and $(n-2) \times k$-SAPS + (i)-SAPS in the last IAPS. Then,

$$\Psi(n, k, m, t) = \sum_{i=0}^{k-1} \frac{(\lambda t)^{(k-m)+(n-2)k+i}}{[(k-m)+(n-2)k+i]!} e^{-\lambda t} \quad (1)$$

Let $\Psi(n, k, m)$ be a probability function to represent that there are n-IAPS throughout the execution of the authentication processes between the UE, MME, and HSS. Therefore,

$$\Psi(n, k, m) = \int_0^{\infty} \Psi(n, k, m, t) f(t)\, dt \quad (2)$$

When the time (T) has an exponential distribution with mean (μ^{-1}), $\gamma = \frac{\lambda}{\lambda+\mu}$. Therefore,

$$\begin{aligned}\Psi(n, k, m) &= \sum_{i=0}^{k-1} (1-\gamma)\, \gamma^{(k-m)+(n-2)k+i} \\ &\quad \times \int_0^{\infty} \frac{y^{(k-m)+(n-2)k+i}}{((k-m)+(n-2)k+i)!} e^{-y} dy \\ &= \gamma^{(k-m)+(n-2)k} \left[1-\gamma^k\right] \quad (3)\end{aligned}$$

If $p = 1-\gamma^k$, then

$$\Psi(n, k, m) = p(1-p)^{(n-1)} \gamma^{-m} \quad (4)$$

In scenario 1, $\Psi(n, k, 0)$ has a geometric probability distribution function with parameter (p) as:

$$\Psi(n, k, m) = p(1-p)^{(n-1)} \quad (5)$$

Therefore, the expected number of authentication events is

$$E(N) = \sum_{n=1}^{\infty} n \times \Psi(n, k, 0) = \frac{1}{p} = \frac{1}{1-\gamma^k} \quad (6)$$

Let $C(k, 0)$ be the total overhead messages cost of the SAK-AKA scheme in scenario 1, where the number of authentication messages is (2) between the serving network entities (MME and HSS) and (2) between the UE and MME. Then,

$$C(k, 0) = E(N) \times [2\alpha k + 2\beta] \quad (7)$$

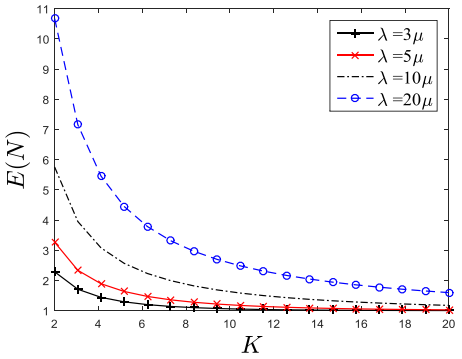

FIGURE 3. The effect of SAPS on IAPS according to the request rate (λ).

where (α) and (β) represent the overhead messages normalized by the cost of the authentication vectors between the UE/MME and MME/HSS, respectively. Finally, from (6) and (7), the cost function will be

$$C(k,0) = \frac{2\alpha k + 2\beta}{1-\gamma^k} : \quad \alpha \lll \beta \tag{8}$$

In scenario 2, the cost function $C(k,m)$ when the authentication event starts at the m-SAPS is the cost function $C(k,0)$ minus the authentication cost of the first m-SAPS at the 1st IAPS, i.e., the signaling traffic of the authentication events costs in SAK-AKA scheme can be represented according to the following formula:

$$C(k,m) = \begin{Bmatrix} \frac{2\alpha k+2\beta}{1-\gamma^k} & m=0 \\ \frac{2\alpha k+2\beta}{1-\gamma^k} - 2[\alpha m+\beta] & 1 \le m \le k-1 \end{Bmatrix} \tag{9}$$

III. ANALYSIS OF PROPOSED MODEL

This section describes the impacts of the (k) value (number of SAPS for each IAPS) on the total execution number of IAPS and the cost function $C(k,m)$ according to equations (5), (6), and (9).

Fig. 3 plots the $E(N)$, or the expected number of IAPS, function against k-SAPS with different request rates (λ), where the time is exponentially distributed with mean (μ^{-1}). It is obvious that $E(N)$ is a decreasing function of (k). The figure indicates that for $3\mu \le \lambda \le 20\mu$, the plotted points are close to each other after ($k \ge 9$), and that $E(N)$ is insignificantly reduced as the (k) value increases and with respect to (λ). In contrast, $\Psi(n,k,m)$ behaves differently with respect to (n) when the ratio (γ) is a constant value.

Fig. 4 (a), Fig. 4 (b) and Fig 4. (c) plot the probability function $\Psi(n,k,m)$ for ($m = 0, 3, 4$), where ($\lambda = 20\mu$) and ($5 \le k \le 20$), respectively. The behavior of the probability functions has varied for different values of (m) but is a decreasing function of (n). Contrarily, the behavior of the probability function increases with respect to (k) until a specific value of (n), after which it decreases with respect to (k).

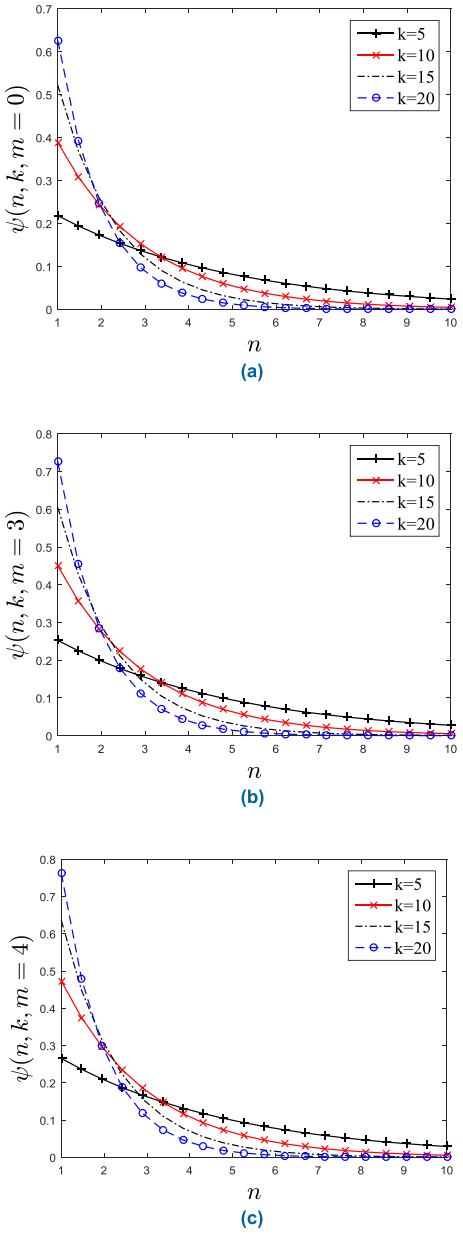

FIGURE 4. (a) The probability function of IAPS when $m = 0$ and $\lambda = 20\mu$. (b) The probability function of IAPS when $m = 3$ and $\lambda = 20\mu$. (c) The probability function of IAPS when $m = 4$ and $\lambda = 20\mu$.

Notably, when ($n \ge 4$), the plotted points are close to each other. These observations are consistent with Fig. 3, i.e., the $E(N)$ value is roughly the same for large (k) values, and increasing (k) when ($k \ge 5$) does not improve the $E(N)$ value.

Fig. 5 (a) and Fig. 5 (b) illustrate the relation of $C(k,0)$ versus different values of (k) to show the effect of the authentication requests on the cost function for ($5\mu \le \lambda \le 20\mu$). These figures indicate that $C(k,0)$ is significantly increased with the increase of (λ). In the same context, for a fixed (λ) and after a specific value of (k) (i.e., $k \ge 5$), $C(k,0)$ is significantly increased. Notably, $C(k,0)$ has the same behavior regardless of the values of (α) and (β).

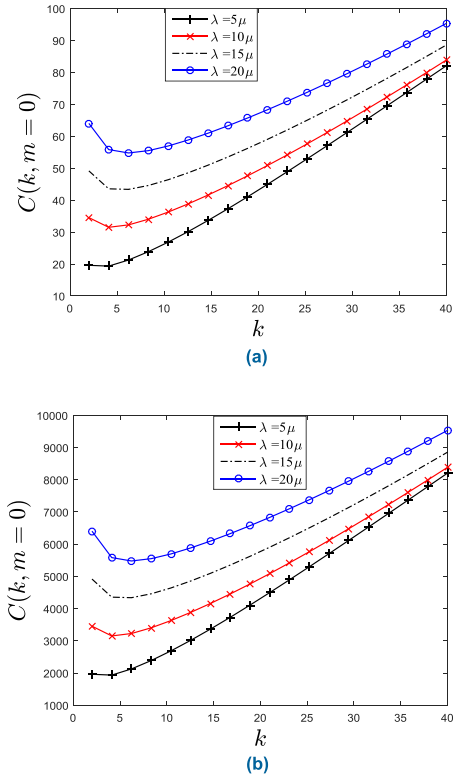

FIGURE 5. (a) The cost function when $\alpha = 1$ and $\beta = 1$. (b) The cost function when $\alpha = 100$ and $\beta = 100$.

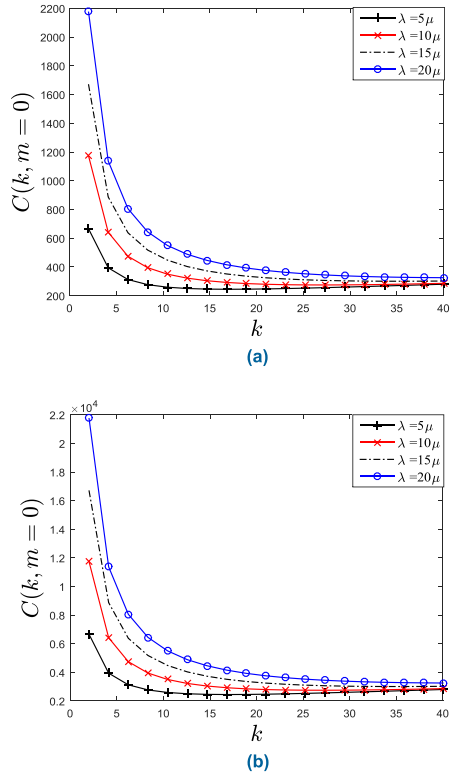

FIGURE 6. (a) The cost function when $\alpha = 1$ and $\beta = 100$. (b) The cost function when $\alpha = 10$ and $\beta = 1000$.

Comparing the plots of Fig. 7 (a) and Fig. 7 (b) shows that there is a critical value of k that minimizes the cost

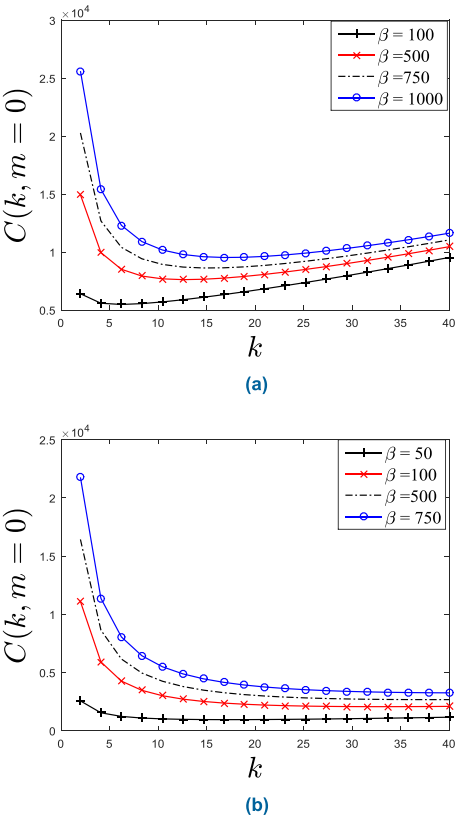

FIGURE 7. (a). The cost function when $\beta > \alpha = 100$. (b) The cost function when $\beta > \alpha = 10$.

function, $C\,(k, 0)$, but that after this value, an increasing (α) will increase the cost function $C\,(k, 0)$.

IV. THE OPTIMAL k-VALUE SELECTION

This section provides a numerical analysis that confirms the results deduced from Fig. 5, Fig. 6, and Fig. 7. There is an optimal value $X^* = \lceil X \rceil$ that minimizes the cost function $C\,(k, m)$ after which the behavior of $C\,(k, m)$ will increase sharply. The value of X can be obtained by differentiating $C\,(k, m)$ in equation (9). Note that, the derivatives of equation (9) for all $m \geq 0$ with respect to k are equal. Therefore, X can be approximated for scenario 1 and 2 as shown in equation (10).

$$\gamma^{-X} = 1 - \frac{(\alpha X + \beta)}{\alpha} ln\gamma \tag{10}$$

It is worth mentioning that it is not easy to find the optimal value $X^* = \lceil X \rceil$ from the differentiation of equation (9). Thus, numerical methods are good alternative tools. The Newton-Raphson method is considered the best and fastest method to approximate $X^* = \lceil X \rceil$ [19], [20]. The recursive Newton-Raphson equation for equation (8) can be represented as:

$$X_{r+1} = X_r - \frac{\alpha + \gamma^{X_r}\,(ln\gamma\,[\alpha X_r + \beta] - \alpha)}{\gamma^{X_r}\,(ln\gamma)^2\,[\alpha X_r + \beta]} \tag{11}$$

TABLE 1. The optimized X^* of the cost function $C(k, m)$ for different values of (α) and (β) with respect to a fixed ratio (γ) when $\lambda = Z\,\mu$, and z = {1, 2, 3, 5, 10,20}.

$\lambda =$		μ	2μ	3μ	5μ	10μ	20μ
α	β	$\gamma =$ 0.5	$\gamma =$ 0.667	$\gamma =$ 0.75	$\gamma =$ 0.833	$\gamma =$ 0.909	$\gamma =$ 0.952
1	50	6	8	11	14	22	34
	100	7	10	13	18	27	43
	500	9	14	18	27	42	69
	750	10	15	19	28	45	76
	900	10	15	20	29	48	80
	10^3	10	15	20	29	49	82
	10^4	13	21	28	42	72	127
	10^5	17	27	36	54	97	173
2	50	5	7	9	12	17	26
	100	6	8	11	14	22	34
	500	8	12	16	22	35	57
	750	9	13	17	24	39	64
	900	9	13	18	25	41	67
	10^3	9	14	18	26	42	69
	10^4	12	19	26	38	65	113
	10^5	16	25	34	51	89	159
3	50	4	6	8	10	15	22
	100	5	7	9	13	19	29
	500	7	11	14	20	32	50
	750	8	12	16	22	35	57
	900	8	12	16	23	37	60
	10^3	8	13	17	23	38	62
	10^4	12	18	24	36	61	105
	10^5	15	24	32	48	85	151
5	50	4	5	6	8	12	18
	100	5	7	7	11	16	24
	500	7	10	13	18	27	43
	750	7	11	14	19	31	49
	900	8	11	15	20	33	52
	10^3	8	12	15	21	33	53
	10^4	11	17	23	33	56	95
	10^5	14	23	31	50	80	141
10	50	3	4	5	7	9	13
	100	4	5	6	8	12	18
	500	6	8	11	14	22	34
	750	6	9	12	16	25	39
	900	7	10	12	17	27	41
	10^3	7	10	13	18	27	43
	10^4	10	15	20	29	49	82
	10^5	13	21	28	42	72	127

where $X_0 = 1$ and $r = 0, 1, 2, \ldots$, and the optimal values of the cost function correspond to different values of (α) , (β), and (γ).

Table 1 shows the computed results of the numerical analysis and confirms the previous deduced results as the following:

1) The value of X^* increases when the value of (γ) is increased (i.e., (λ) is increased).
2) The value of X^* slightly increases when (β) is sharply increased, for any specific fixed value of the request ratio (γ).
3) The value of X^* decreases when the value of (α) is increased, for any specific fixed value of the request ratio (γ).

The abovementioned results confirmed the consistency of the relation between the optimal values of the cost function and the values of (α), (β) and (γ) that was previously deduced. Therefore, these results indicate that the MME should maintain a dynamic mechanism to choose an optimal value of (k) according to the authentication requests rate of (λ) the UE when it executes the SAK-AKA scheme.

V. CONCLUSION

In the SAK-AKA scheme, it is desirable to choose an appropriate (k) value to determine how many times the SAPS phase will be executed when the IAPS phase is executed to maintain a specific level of security and reduce the authentication signaling traffic cost.

In this paper, we propose an analytic model based on the Poisson process for the SAK-AKA scheme to investigate the cost function of authentication processes and compute the optimal values of (k) that minimize the overhead messages cost of the authentication processes.

We observed from the analysis of the proposed model that the optimal value (k) will be increased when the value of the authentication request rate (λ) is increased. Specifically, for any fixed value of (λ), the optimal value of (k) will slightly increase when the overhead cost of the authentication messages transmitted between the MME and HSS are increased. In contrast, the overhead cost of the authentication messages that are transmitted between the UE and MME are decreased. Consequently, the MME should maintain a dynamic mechanism to determine the best value of (k) according to the authentication request rate of each UE to reduce the network signaling traffic cost.

ACKNOWLEDGMENT

The authors are very grateful to the reviewers for their valuable comments that helped to improve the article. They express their gratitude to all members of our colleges, Jouf University, and Al Quds Open University, for their support.

REFERENCES

[1] M. A. Ferrag, L. Maglars, A. Argyriou, D. Kosmanos, and H. Janicke, "Security for 4G and 5G cellular networks: A survey of existing authentication and privacy-preserving schemes," *J. Netw. Comput. Appl.*, vol. 101, pp. 55–82, Jan. 2018.
[2] K. A. Alezabi, F. Hashim, S. J. Hashim, B. M. Ali, and A. Jamalipour, "Efficient authentication and re-authentication protocols for 4G/5G heterogeneous networks," *EURASIP J. Wireless Commun. Netw.*, vol. 2020, no. 1, pp. 1–4, Dec. 2020.
[3] S. Nashwan, "SAK-AKA: A secure anonymity key of authentication and key agreement protocol for LTE network," *Int. Arab J. Inf. Technol.*, vol. 14, no. 5, pp. 790–801, 2017.
[4] S. Nashwan, "Secure authentication protocol for NFC mobile payment systems," *Int. J. Comput. Sci. Netw. Secur.*, vol. 17, no. 8, pp. 256–263, 2017.
[5] S. Nashwan, "Synchronous authentication key management scheme for inter-eNB handover over LTE networks," *Int. J. Adv. Comput. Sci. Appl.*, vol. 8, no. 8, pp. 100–107, 2017.
[6] M. Al-Fayoumi and S. Nashwan, "Performance analysis of SAP-NFC protocol," *Int. J. Commun. Netw. Inf. Secur.*, vol. 10, no. 1, pp. 125–130, 2018.
[7] S. Nashwan, "SE-H: Secure and efficient hash protocol for RFID system," *Int. J. Commun. Netw. Inf. Secur.*, vol. 9, no. 3, pp. 358–366, 2017.

[8] A. Al-Qerem, F. Kharbat, S. Nashwan, S. Ashraf, and K. Blaou, "General model for best feature extraction of EEG using discrete wavelet transform wavelet family and differential evolution," *Int. J. Distrib. Sensor Netw.*, vol. 16, no. 3, pp. 1–21, 2020.
[9] S. Nashwan, "AAA-WSN: Anonymous access authentication scheme for wireless sensor networks in big data environment," *Egyptian Informat. J.*, vol. 22, no. 1, pp. 15–26, Mar. 2021.
[10] S. Nashwan, "An end-to-end authentication scheme for healthcare IoT systems using WMSN," *Comput., Mater. Continua*, vol. 68, no. 1, pp. 607–642, 2021.
[11] N. Almrezeq, L. T. Almadhoor, T. Alrasheed, A. A. A. El-Aziz, and S. Nashwan, "Design a secure IoT architecture using smart wireless networks," *Int. J. Commun. Netw. Inf. Secur.*, vol. 12, no. 3, pp. 401–410, 2020.
[12] A. Hamarsheh, Y. Abdalaziz, and S. Nashwan, "Recent impediments in deploying IPv6," *Adv. Sci., Technol. Eng. Syst. J.*, vol. 6, no. 1, pp. 336–341, Jan. 2021.
[13] A. Damnjanovic, J. Montojo, Y. Wei, T. Ji, T. Luo, M. Vajapeyam, T. Yoo, O. Song, and D. Malladi, "A survey on 3GPP heterogeneous networks," *IEEE Wireless Commun.*, vol. 18, no. 3, pp. 10–21, Jun. 2011.
[14] M. Abu-Lebdeh, J. Sahoo, R. Glitho, and C. W. Tchouati, "Cloudifying the 3GPP IP multimedia subsystem for 4G and beyond: A survey," *IEEE Commun. Mag.*, vol. 54, no. 1, pp. 91–97, Jan. 2016.
[15] J. Cao, M. Ma, and H. Li, "An uniform handover authentication between E-UTRAN and non-3GPP access networks," *IEEE Trans. Wireless Commun.*, vol. 11, no. 10, pp. 3644–3650, Oct. 2012.
[16] Y.-B. Lin and Y.-K. Chen, "Reducing authentication signaling traffic in third-generation mobile network," *IEEE Trans. Wireless Commun.*, vol. 2, no. 3, pp. 493–501, May 2003.
[17] J. Al-Saraireh and S. Yousef, "Authentication transmission overhead between entities in mobile networks," *Int. J. Comput. Sci. Netw. Secur.*, vol. 6, no. 3, pp. 150–154, 2006.
[18] C. K. Han, H. K. Choi, J. W. Baek, and H. W. Lee, "Evaluation of authentication signaling loads in 3GPP LTE/SAE networks," in *Proc. LCN*, Zürich, Switzerland, 2009, pp. 37–44.
[19] B. Sereeter, C. Vuik, and C. Witteveen, "On a comparison of Newton–Raphson solvers for power flow problems," *J. Comput. Appl. Math.*, vol. 360, pp. 157–169, Nov. 2019.
[20] A. Adu-Sackey, F. Oduro, and G. Fosu, "Inequalities approach in determination of convergence of recurrence sequences," *Open J. Math. Sci.*, vol. 5, no. 1, pp. 65–72, Dec. 2021.

SHADI NASHWAN was born in Amman, Jordan, in 1978. He received the B.Sc. degree in computer science from Al-Azhar University, Palestine, in 2001, the M.Sc. degree in computer science from The University of Jordan, Jordan, in 2003, and the Ph.D. degree in computer and network security from Anglia Ruskin University, U.K., in 2009. From 2009 to 2010, he was an Assistant Professor with the Department of Computer Science, Al-Zaytoonah University, Jordan. At the end of 2010, he became an Assistant Professor with the Computer Science Department, Jouf University, Saudi Arabia. In 2018, he was promoted to the position of associate professor in cybersecurity. He has published several articles in the area of authentication protocol, recovery techniques, analytic model, and mobility management. His research interests include authentication protocol for mobile networks, mobility management, and security of the wireless networks, such as NFC, RFID, WSNs, and WMSNs.

IMAD. I. H. NASHWAN was born in Amman, Jordan, in 1974. He received the B.Sc. degree in mathematics from the University of Sana'a, in 1995, the M.S. degree from the Islamic University of Gaza, in 2006, and the Ph.D. degree in mathematical statistics from Ain-Shams University, Egypt, in 2012. He is currently an Associate Professor in mathematical statistics with the Faculty of Technology and Applied Science, Al Quds Open University, State of Palestine. He has authored two books in statistics. He has published several articles in the area of the mathematical and applied statistics, reliability analysis, consecutive systems, and systems modeling.