SECURITY V/S QOS FOR LTE AUTHENTICATION AND KEY AGREEMENT PROTOCOL

Jacques Bou Abdo[1], Jacques Demerjian[2] and Hakima Chaouchi[3]

[1]Nokia Siemens Networks, Beirut, Lebanon
jacques.bou-abdo@nsn.com
[2]Faculty of Engineering, Antonine University, Baabda, Lebanon
jacques.demerjian@upa.edu.lb
[3]Telecom Sud Paris, Institut Telecom, CNRS SAMOVAR, UMR 5751, Paris, France
hakima.chaouchi@it-sudparis.eu

ABSTRACT

Protocol and technology convergence, the core of near future communication, will soon be forming the interoperating heterogeneous networks. Attaining a strict secure authentication without risking the QoS performance and call success rates is a major concern when it comes to wireless heterogeneous networks. In order to achieve this, a generic, fast and secure, Authentication and Key Agreement protocol is to be used; a version of which is to be implemented between each two technologies. In this research, different existing EPS-EPS AKA protocols will be compared with our proposed protocol EC-AKA (Ensure Confidentiality Authentication and Key Agreement) based on security, cost effectiveness, signaling overhead, delay and performance. It is proven that EC-AKA is the exclusive protocol satisfying the New Generation Network's KPIs and it will be promoted as the target generic AKA protocol in heterogeneous networks.

KEYWORDS

Authentication, LTE Security, EPS, Mobile Security, AKA, EC-AKA, NGN

1. INTRODUCTION

Since we consider EPS (Evolved Packet System) as the umbrella technology in heterogeneous networks [1], we are working on creating a converged [2] AKA (Authentication and Key Agreement) protocol, to be shared among different technologies or at least create converged versions of AKA. We are taking advantage of EPS's built-in compatibility with 3GPP and non-3GPP technologies, used to propose minimum modifications on the current systems [17]. These converged versions will each be used by a technology, to transform identification and authorization in heterogeneous networks, into a homogeneous process.

The three requirements for AKA, we are interested in, are converged AKA mechanism, with highest possible security and best QoS performance, in heterogeneous networks. Convergence is needed for adapting AKA mechanisms in different technologies. More security is needed to satisfy the privacy requirements, which EPS, UMTS (Universal Mobile Telecommunications System) and GSM (Global Systems for Mobile Communications) has failed to ensure [3] [4]. QoS performance is critical in the success of inter-technology handovers, which will be offered by heterogeneous networks [18]. During inter-technology handover, as the delay during identification and authentication at the destination technology increases, the call drop rate increases also. Operators are very sensitive to call drop rate, and very tough KPIs are used to ensure optimized network performance.

DOI : 10.5121/ijnsa.2012.4506

In this work we are interested in converging EPS AKA mechanism as a first step of creating unified AKA across the different technologies, participating in a heterogeneous network. The rest of this work will discuss the security and QoS of different EPS AKA mechanisms, from which we'll be able to evaluate the protocols satisfying the three requirements mentioned above.

Since the Authentication and Key Agreement protocol in EPS has a known vulnerability that can be exploited to breach the privacy of the user's identity and even his location [3] [5] [6], many attempts have tried to solve this problem by proposing alternative protocols. The vulnerability (i.e. sending the International Mobile Subscriber Identity in plaintext when no temporary identifier is valid) which was inherited from UMTS, can be used in tracking the user and/or in detecting the user's presence. One of the latest proposed alternative protocols noted as SE-AKA (Security Enhanced Authentication and Key Agreement) [7] was Crypt-analyzed in our previous work [8] and it was found vulnerable to two attacks (brute force and intelligent brute force) if no padding is used. In this work we'll compare the standard AKA [6], SE-AKA [7] and our protocol EC-AKA (Ensured Confidentiality Authentication and Key Agreement) [8] to allow architects to choose the protocol best suiting their needs (KPIs, Cost, etc.).

EC-AKA's design and the cryptanalysis scenarios can be found in our previous work [8], We'll be proving now, that EC-AKA is not just outperforming on security aspects, but achieving excellent QoS rates when compared to other proposed AKA mechanisms.

Security and performance aren't necessarily opposites. But more tightened security usually requires more processing and additional overheads. A protocol's performance is positioned based on its characteristics in comparison with the application's need. Usually there is no best protocol, since decision making is biased by the application's need, policy design and signed agreement.

We are going to define in this work, five parameters to evaluate an AKA protocol. The parameters are:

- Security/Risk: The protocol's resiliency and resistance to attacks, and the attack's probability. It is known that for the same estimated revenue, with the increase in cost and effort to exploit a certain vulnerability the probability of attacking decreases.
- Cost: Deployment cost (CAPEX) and running/operation cost (OPEX).
- Overhead: Additional overhead (added traffic on transmission interface).
- Delay: Overall resulting delay. Higher delay will lead to lower call completion rate when used in a heterogeneous network.
- Performance: CPU processing directly proportional to battery consumption.

The rest of this work is organized as follows. In section 2, the "Risk" parameter will be evaluated in all the studied protocols, and ordered based on the results. In section 3, the studied protocols will be compared based on the "Cost" parameter. In section 4, the comparison will be based on "overhead". In section 5, the studied protocols will be compared based on "Delay". In section 6, the "Performance" parameter will be studied. In section 7, the results will be analyzed, and the optimal protocol for use in heterogeneous networks will be selected. Finally, the conclusion will be given in section 8.

2. RISK

This section will compare protocols based on "Security/Risk" parameter, which is defined in Table 1.

Table 1. Risk definition

Risk = Asset value * Perceived Threat * Vulnerability

The asset value and perceived threat parameters are the same for the three studied protocols, thus we are interested in evaluating the vulnerability parameter, i.e. the ease to exploit a vulnerability. We have modelled EPS's AKA in HLPSL (High-Level Protocol Specification Language) to be able to verify its security using AVISPA [16], and it turned out to be unsafe if MME-HSS (Mobility Management Entity – Home Subscriber Server) interface was not considered secure. In case of roaming the HSS and MME belong to different networks, thus we consider it open to attacks if no closed network is used.

The attack on EPS AKA can be ran on two depth levels:

1. Capturing IMSI in plaintext (attack against the user's identity and location privacy).

2. Running an active fake BTS (Base Transceiver Station) attack (breaches the user's call and data privacy, with having some control over the mobile device).

Level 1 attack requires minimum resources and knowledge, and has less risk levels. Level 2 attack requires exploiting the transport security (between Home Network's HSS and Serving Network's MME), or maliciously using a trusted operator's infrastructure (private key) [14] [15] to gain the HN's HSS trust.

Table 2 represents the level 2 attack scenario in SPAN's (Security Protocol ANimator) trace model, and the figure 1 illustrates a SPAN representation of the attack.

Table 2. Level 2 attack scenario

Step 1	(role_U, 5) -> (role_M, 4) : *x(IMSI,IMSI)*
Step 2	(role_M, 4) -> (Intruder_, 0) : *x(pair(IMSI,SNID),Listen_i)*
Step 3	(Intruder_, 0) -> (role_H, 3) : *x(pair(imsi-1,snid),pair(IMSI,SNID))*
Step 4	(role_H, 3) -> (Intruder_, 0) : *x(pair(RAND_new,pair(apply(F2, pair(K,RAND_new)),pair(apply(F3,pair(K,RAND_new)),pair(apply(F4,pair(K,RAND_new)),pair(xor(SQN_new,apply(F5,pair(K,RAND_new))),pair(AMF,apply(F1,pair(K,pair(SQN_new,pair(RAND_new,AMF))))))))),Listen_i)*
Step 5	(Intruder_, 0) -> (role_M, 4) : *x(pair(nonce-2,pair(apply(f2, pair(k,nonce-2)),pair(apply(f3,pair(k,nonce-2)), pair(apply(f4,pair(k,nonce-2)), pair(xor(nonce-3,apply(f5,pair(k,nonce-2))), pair(amf,apply(f1,pair(k,pair(nonce-3,pair(nonce-2,amf))))))))),pair(RAND,pair(apply(Test_F2,pair(K,RAND)),pair(apply(Test_F3,pair(K,RAND)),pair(apply(Test_F4,pair(K,RAND)),pair(xor(SQN,apply(Test_F5,pair(K,RAND))), pair(AMF,apply(Test_F1,pair(K,pair(SQN,pair(RAND,AMF))))))))))*
Step 6	(role_M, 4) -> (role_U, 5) : *x(pair(RAND,pair(xor(SQN,Vf5_new), pair(AMF,Vf1_new))),pair(RAND,pair(xor(SQN,Vf5),pair(Test_AMF,Vf1))))*

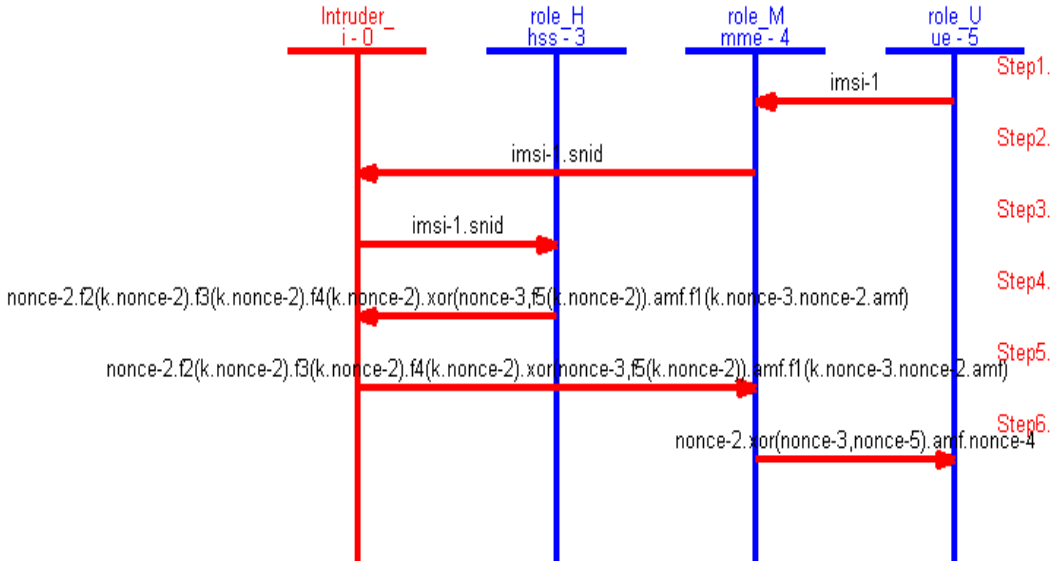

Figure 1. SPAN representation of the attack

SE-AKA has been crypt-analyzed in our previous work [8], and it was proven to be unsafe, but the effort to exploit it exceeds that of EPS's AKA. EC-AKA has been verified using AVISPA and turned to be SAFE, thus when comparing the three protocols, EC-AKA is considered the most secure. The protocols are ordered in decreasing order of security and increasing order of Risk as shown in Table 3:

Table 3. List of protocols ordered by security/risk

1	EC-AKA
2	SE-AKA
3	EPS's AKA

3. COST

This section will compare protocols based on the "Cost" parameter. 3GPP's AKA is considered the cost reference, and the additional cost of protocols SE-AKA and EC-AKA is evaluated in the sub-sections below.

3.1 SE-AKA

Of the messages exchanged between the UE and MME or MME and HSS in the SE-AKA protocol, the 4th message is the most demanding for cost. This message is encrypted by the message sender (MME) using the public key (PK_u) of the message receiver (UE). Thus the sender should have the X.509 identity certificate of the receiver. This certificate must be delivered by a trusted CA (Certificate Authority) of a PKI (Public Key Infrastructure) [19].

Table 4. The fourth message in SE-AKA

MME → UE: D= { RAND (i), SNID , KSI_{ASME}(i), S –TMSI } $_{PKU}$

The message sender (MME) must have access to the message receiver's X.509 Identity certificate. In our work we assume that the MME can access the certificate using three possible scenarios:

1. The user's certificate is stored in the HN's HSS [9].
2. Each network has its own database containing all its users' certificates. Since the user is authorized to access the SN (according to an inter-operator agreement in roaming scenario), then the SN's MME can securely access the user's certificate in his HN's database.
3. The user's certificate is available in a specific database ex: VeriSign.

Scenario 1 is the most suitable choice because of low investment cost (CAPEX) needed. The connection between foreign networks is usually slow (small bandwidth) and costly [10], when compared to local networks. Then option 1 will be suitable for authentication requests from the same network, while underperforming for roaming users. The certificate's size is 11 times larger than the AV (Authentication Vector) which is also sent from the HSS.

Scenario 2 is cheaper than scenario 3, but both are much expensive when compared to scenario 1. In performance, this option is efficient for local connections but also underperform for roaming connections.

Scenario 3 is the most expensive, and underperforming for local connections, but has better results for roaming users when compared to the first 2 scenario.

3.2. EC-AKA

The first message in EC-AKA uses asymmetric encryption, thus it has a fixed length. The free spaces are used to send a temporary ciphering key, which will be used later (message four and beyond) in symmetric encryption. In symmetric encryption, there is no need for user certificates, thus no extra investment is needed in EC-AKA.

As a conclusion of this section, EC-AKA outperforms SE-AKA in cost. When comparing the three protocols, it can be ordered in increasing order of cost:

1. EC-AKA and EPS's AKA
2. SE-AKA

4. OVERHEAD

This section will compare the extra-traffic generated from EPS's AKA, SE-AKA and EC-AKA protocols. The following table present the overhead of each protocol listed above using the asymmetric algorithm RSA (Rivest Shamir Adleman) instead of elliptic curve used in [7].

Table 5. Protocols' overheads categorized in interfaces

	Upload Radio & Backhaul (bit)	Download Radio & Backhaul (bit)	Core traffic (bit)
3GPP's AKA	118	304	80 +n*688
SE-AKA	1152	1024	1024 +ceiling((n*688+8060)/1024)*1024
ECAKA	1172	515	2068+ ceiling ((n*688+396)/1024)*1024

We note that "n" is the number of authentication vectors sent to MME in each Authentication data response. MME uses a new AV every time it needs to authenticate the user, so HSS generate more than one AV for each authentication request, to be saved in MME for instant user authentication (when needed) instead of calling key sharing algorithm (part of AKA) each time a user has to be authenticated. This will decrease latency and load on HSS.

As "n" decreases, MME builds a smaller backup list of AVs, thus AKA mechanism is requested more, then more latency and load on HSS. As "n" increases, the risk of over generating AVs increase, thus we risk overloading the HSS and the expensive connection between HSS and MME with unused Keys.

Figure 2 and 3 illustrate respectively the signalling overhead between EC-AKA and EPS's AKA, and EC-AKA and SE-AKA.

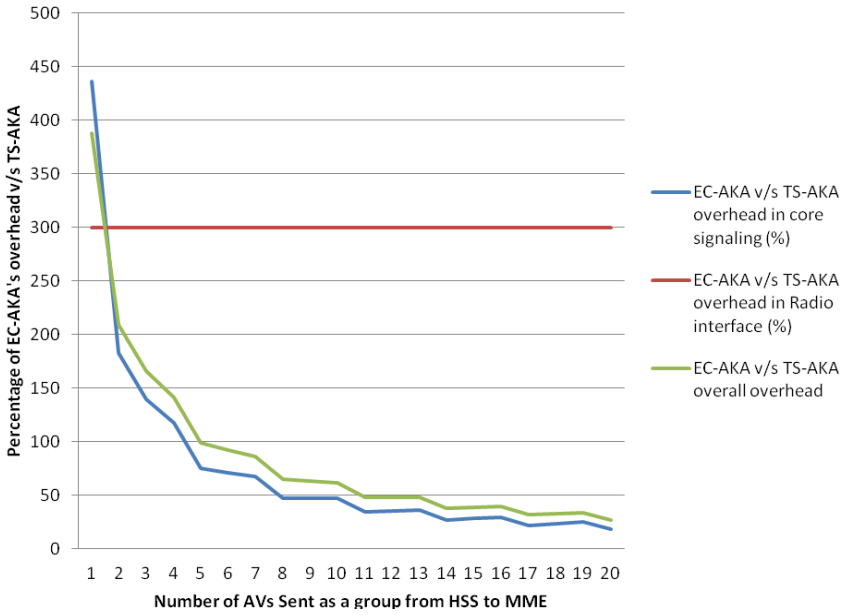

Figure 2. Signalling Overhead EC-AKA v/s EPS's AKA

We deduce from Figure 2 that EC-AKA generate more signalling on both Radio and Core levels than the standard AKA. This difference in signalling decreases as "n" increases. Network architects interested in dimensioning the signalling traffic will use the curve best suiting their interest, i.e. in networks overloaded with signalling traffic on core level, architects' selection of mechanism is influenced primary with the generated rates in core more than that on radio.

Below in Figure 3, the red line represents the percentage of extra-signalling generated by EC-AKA in comparison with SE-AKA. We observed that EC-AKA has a constant 22% less signalling traffic on the air channel, while the additional signalling on the core level, varies with the number of sent AVs, represented in blue. The extra traffic generated by EC-AKA on network level is shown in green. All the values are in comparison with SE-AKA.

We conclude that EC-AKA has a superior performance over SE-AKA, ranging between 28 and 56% for the overall traffic.

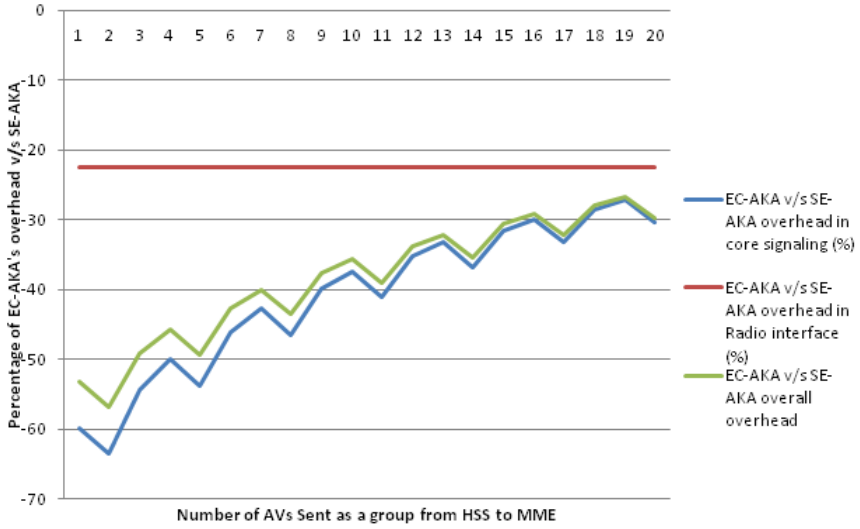

Figure 3. Signalling Overhead EC-AKA v/s SE-AKA

As a compromise, "n" is usually configured as 10. So the resulting table will be:

Table 6. Protocols' overheads for n=10

Signalling overhead	Percentage
Radio traffic Overhead of EC-AKA v/s SE-AKA	-22.4724%
Radio traffic Overhead of EC-AKA v/s 3GPP's AKA	299.763%
Core traffic Overhead of EC-AKA v/s SE-AKA	-37.3779%
Core traffic Overhead of EC-AKA v/s 3GPP's AKA	47.41379%
Overall Overhead ECAKA v/s SEAKA	**-35.6304%**
Overall Overhead ECAKA v/s 3GPP's AKA	**61.83961%**

In usual implementations, EC-AKA will result in 299% more traffic on Radio channel and 47.4% more traffic in Core network, so an overall 61.3% more traffic on network level over 3GPP's AKA. When compared to SE-AKA, EC-AKA will result in 22.4% less traffic on Radio channel and 37.3% less traffic in Core network, so an overall 35.6% less traffic on network level.

5. DELAY

This section will compare protocols based on the "Delay" parameter, which is decomposed into two sources: Transmission and processing. Each source will be studied separately since transmission delay depends on the effective bandwidth (Network congestion, radio conditions, distance from base station, network dimensioning, etc.), while processing delay depends on the UE's resources (CPU speed, Operating System, load on the OS, etc.).

We note that the calculated values are used with RSA, if elliptic curve is used, the difference between the protocols will decrease, thus the results converge. If the delay converge then EC-AKA will become the optimal solution because it offers higher security with similar cost to 3GPP's AKA while lower cost to SE-AKA.

5.1 Transmission Delay

In this subsection, we consider that the:

- Minimum of the "Upload effective Radio bandwidth and upload backhaul bandwidth" for the studied user is noted as EBU.
- Minimum of the "Downlink effective Radio bandwidth and downlink backhaul bandwidth" for the studied user is noted as EBD.
- Bandwidth between the HN's HSS and SN's MME is noted as CoreBD.

To study the Delay performance, we'll categorize the available bandwidth into:

- Roaming user (Low core bandwidth): Core [100K, 10Mbps]
- Local user (High core bandwidth): Core [20M, 200M]
- In applicable core BD: Core [1K, 10K]
- Condensed cell: EBU [100K, 900K] and EBD [200K, 1.8M]
- Semi-condensed cell: EBU [1M, 9M] and EBD [2M, 18M]
- Non condensed cell: EBU [10M, 50M] and EBD [20M, 100M]
- In applicable rate in a cell: EBU [1K, 2K] and EBD [2K, 10K]

Considering digits are transmitted in hexadecimal format, so binary length = 4 * decimal length.

SE-AKA's Overall estimated transmission delay is equal to: 1152/EBU + 1024/EBD + (1024 + ceiling((n*688+8060)/1024)*1024)/CoreBD

EC-AKA's Overall estimated transmission delay is equal to: 1172/EBU + 515/EBD + (2068+ ceiling ((n*688+396)/1024)*1024)/CoreBD

Relational Delay difference between EC-AKA and SE-AKA (%) is : (Delay ECAKA – Delay SEAKA)*100/(Delay SE-AKA) = ((20)/EBU + (-509)/EBD + (1044 + ceiling ((n*688+396)/1024)*1024 - ceiling((n*688+8060)/1024)*1024))/CoreBD)*100/ (1152/EBU + 1024/EBD + (1024 +ceiling((n*688+8060)/1024)*1024)/CoreBD)

In Table 7, the delay difference between EC-AKA and SE-AKA is illustrated.

Table 7. Delay difference between EC-AKA and SE-AKA

	Inapplicable	Roaming user	Local user
Inapplicable	-29.89%	-4.27%	-0.011639202
Condensed cell	-39.86%	-39.87%	-39.87%
Semi-condensed cell	-39.86%	-39.87%	-39.87%
Non condensed cell	-39.86%	-39.86%	-39.86%

We deduce that, EC-AKA has a superior performance in transmission delay with an average of 39.8% less delay when compared to SE-AKA for all the possible network conditions.

AKA's Overall estimated transmission delay is equal to: 188/EBU + 304/EBD + (80+n*688)/CoreDB

EC-AKA's Overall estimated transmission delay is equal to: 1172/EBU + 515/EBD + (2068+ ceiling ((n*688+396)/1024)*1024)/CoreBD

Relational Delay difference between EC-AKA and 3GPP's AKA (%) is : (Delay ECAKA – Delay SEAKA)*100/(Delay SE-AKA) = ((20)/EBU + (-509)/EBD + (1044 + ceiling ((n*688+396)/1024)*1024 - ceiling((n*688+8060)/1024)*1024))/CoreBD)*100/ (1152/EBU + 1024/EBD + (1024 +ceiling((n*688+8060)/1024)*1024)/CoreBD)

Table 8. Delay difference between EC-AKA and 3GPP's AKA

	Inapplicable	Roaming user	Local user
Inapplicable	76.28%	465.27%	539.37%
Condensed cell	47.76%	146.93%	433.11%
Semi-condensed cell	47.47%	63.95%	222.15%
Non condensed cell	47.44%	49.60%	86.79%

We deduce that EC-AKA has higher transmission delay when compared to 3GPP's AKA, and this extra delay varies between 49.6% and 433.11% depending on the network's situation (Radio conditions, congestion,...).

As deduced from the graph above, as cell density decreases (higher radio bandwidth), the difference between the two studied protocols decreases, so EC-AKA's performance increases. EC-AKA is most suitable in non condensed cells with low Core rates.

5.2 Processing Delay

Since the mobile's computational resources are much less than that of the network, we will only consider the delay resulting from the processing on the mobile's side.

MME and HSS are considered capable of handling high processing. The core network's performance is mainly effected by traffic, which is studied here under overhead.

Table 9. Processing Delay on the mobile's side

	Number of CPU Cycles
3GPP's AKA	1026
EC-AKA	142717
SE-AKA	2821026

We deduce that EC-AKA has 94.95 % less processing delay when compared to SE-AKA.

6. PERFORMANCE

A protocol's performance and battery consumption in a mobile equipment is directly proportional to the processing and transmission overhead. Based on the above results, it can be shown that EC-AKA has lower transmission overhead and processing overhead at the same time, thus we can deduce that EC-AKA has better CPU performance and battery consumption, which are the main factors affecting the performance indicator.

7. ANALYSING RESULTS

In this section, we are going to consolidate the results of our study shown above into the technical sheet that can support Architects in choosing the AKA mechanism, best suiting their requirements.

We present in Table 10, the technical sheet comparing EC-AKA, SE-AKA and EPS's AKA. This table can be read in decreasing order of each parameter (Security, Cost, Overhead, Delay, Performance), where "1" represents best performance and "3" represents the worst.

Table 10. Technical sheet of EC-AKA, SE-AKA, and 3GPP's AKA

	EC-AKA	SE-AKA	Standard AKA
Security	1	2	3
Cost	1	3	1
Overhead	2	3	1
Delay	2	3	1
Performance	2	3	1

It can be shown that EC-AKA has the best security and cost level, with very acceptable performance in the remaining parameters. Standard AKA has the best performance since no additional security is implemented, but its security level is poor.

In our design, security is a very important factor especially that the ability to decrease the risk requires acceptable increase in resources, as what was shown from the result of EC-AKA. SE-AKA has poor performance on all the parameters, so it considered not adequate for future implementations.

Since EC-AKA is the only protocol satisfying the security requirements for NGN and achieving excellent QoS performance, it will be adopted as the protocol of choice for EPS-EPS Authentication and key agreement mechanisms. The generic AKA protocol in heterogeneous networks will be inspired from EC-AKA with minimum modifications.

8. CONCLUSIONS

It was proven that EC-AKA is the only proposed AKA mechanism satisfying the strict security requirements of NGNs. Nevertheless, it succeeded to perform very well on all the studied parameters (cost, signalling overhead, delay and performance), and outperform SE-AKA. EC-AKA is considered the protocol of choice for EPS-EPS connection in heterogeneous networks. The generic AKA to be developed for heterogeneous networks will be very close to EC-AKA, which is the protocol that eventually fulfilled all our requirements (Malleable protocol thus ensuring minimum adaption of AVs, Highly secure, and having good QoS performance).

REFERENCES

[1] T. Yahya and H. Chaouchi, "On the Integration of LTE and Mobile WiMAX Networks", 2010 Proceedings of 19th International Conference on Computer Communications and Networks (ICCCN), 2-5 Aug. 2010, pp. 1-5.

[2] J. Rohrer, J. Sterbenz, and W. Weicho, "Homogeneous Security in Heterogeneous Networks: Towards A Generic Security Management Protocol", Military Communications Conference, 2007. MILCOM 2007. IEEE, 29-31 Oct. 2007, pp.1-6.

[3] 3rd Generation Partnership Project, 3GPP TR 33.821 V9.0.0 (2009-06), Rationale and track of security decisions in Long Term Evolved (LTE) RAN / 3GPP System Architecture Evolution (SAE) (Release 9).

[4] D. Forsberg, G. Horn, W. Moeller andV. Niemi, LTE Security. John Wiley & Sons Ltd, 2010.

[5] 3rd Generation Partnership Project, 3GPP TS 33.401 V11.2.0 (2011-12), 3GPP System Architecture Evolution (SAE); Security architecture (Release 11).

[6] 3rd Generation Partnership Project, 3GPP TS 33.401 V8.8.0 (2011-06), 3GPP System Architecture Evolution (SAE); Security architecture (Release 8).

[7] L. Xiehua and W. Yongjun, "Security Enhanced Authentication and Key Agreement Protocol for LTE/SAE Network," 7th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM), 23-25 Sept. 2011, pp.1-4.

[8] J. Bou Abdo, H. Chaouchi and M. Aoude, "Ensured Confidentiality Authentication and Key Agreement Protocol for EPS". 3rd Symposium on Broadband Networks and Fast Internet, 28-29 May 2012.

[9] 3rd Generation Partnership Project, 3GPP TS 33.220 V11.2.0 (2012-03), Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA) (Release 11).

[10] J. AL-Saraireh, and S. Yousef, "Extension of Authentication and Key Agreement Protocol (AKA) for Universal Mobile Telecommunication System (UMTS)", International Journal of Theoretical and Applied Computer Sciences, Volume 1 Number 1 (2006) pp. 109–118.

[11] H. Dake, W. Jianbo and Z. Yu, "User authentication scheme based on self-certified public-key for next generation wireless network", . International Symposium on Biometrics and Security Technologies, ISBAST 2008, 23-24 April 2008, pp.1-8.

[12] L. Xiehua, Y. Shutang and L. Jianhua, "Security protocol analysis with improved authentication tests," ISPEC 2006, IEEE Press, 2006, pp.123-133.

[13] A. Herzberg, H. Krawczyk and G. Tsudik," Travelling Incognito", WMCSA '94 Proceedings of the 1994 First Workshop on Mobile Computing Systems and Applications, pp.205-211.

[14] G. Sawma and J. Demerjian. "A Distributed Trust and Reputation Model for Capacity Enhancement in Wireless Networks", IFIP Wireless Days Conference 2008, 24-27 Nov. 2008.

[15] R. Tawil, J. Demerjian and G. Pujolle. "A Trusted Handoff Decision Scheme for the Next Generation Wireless Networks", International Journal of Computer Science and Network Security, IJCSNS, Vol. 8, no. 6, PP. 174-182, Jun. 2008.

[16] AVISPA Project: http://www.avispa-project.org/

[17] AS Ali. "Authentication and key management in heterogeneous wireless networks", PhD Thesis in Electrical and Computer Engineering, The University of British Columbia, 2010.

[18] M. Aiash, G. Mapp and A. Lasebae. "A Survey on Authentication and Key Agreement Protocols in Heterogeneous Networks", International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.4, July 2012.

[19] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley and W. Polk. "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", IETF RFC 5280, May 2008.

Authors

Jacques Bou Abdo: received his BE in Electrical and Computer Engineering from the Lebanese University in 2009 and DEA in Telecommunication Networks from the Lebanese University and Saint Joseph University in 2012. He is working with Nokia Siemens Networks since 2010.

Jacques Demerjian: received his PhD degree in Network & Computer Science from TELECOM ParisTech (ENST-Paris) in 2004. Dr. Demerjian is an Associate Professor in the Faculty of Engineering at the Antonine University in Lebanon. His main research activities concern wired and wireless network security. He is an IEEE senior member.

Hakima Chaouchi: received her PhD degree from Université Pierre et Marie CURIE (Paris6) in 2004. Pr. Chaouchi is a Professor at Telecom Sud Paris in France. Her main research activities concern heterogeneous networks, handover management, and authentication and AAA in self organized networks.