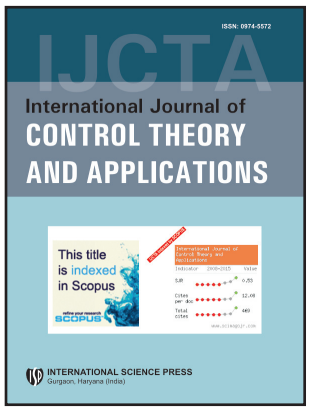

International Journal of Control Theory and Applications

ISSN : 0974-5572

Volume 10 • Number 12 • 2017

Trust based Authentication Latency Reduction Scheme for Internetwork Handover

R. Narmadha[a]

[a] ?

Abstract: In our paper to provide security to 4G networks, authentication protocol is provided in which authentication messages are exchanged among User Equipment, Mobility Management Equipment and Home Subscriber Server. In order to provide a fast authentication, we use a trust aware handoff algorithm to select the handoff access point (AP). The nodes which are already present in the network authenticate the joining node using this algorithm. Based on the trust level of the nodes, the nodes perform the handoff to BS. Completing authentication, a local authentication agent perform re authentication on request by mobile user to check whether the identity is legal or not. The re-authentication is carried in the form of iterative fast re-authentication process.

1. INTRODUCTION

1.1. 4G networks

4G is the extreme network providing higher data rates (100mb/sec), expanded multimedia services and about 2.8GHz frequency. 4G is not a defined technology or standard, but rather a collection of technologies and protocols which generate fully packet-switched networks optimized for data [1][3]. It has wide area of applications in extensive wireless multimedia services, full-motion video applications and wireless teleconferencing [3]. The fourth generations (4G) wireless networks possess specific characteristics like high usability at anytime, anywhere and with any technology, assist intelligent services at low transmission cost [2]. The multiple standards of voice traffic in 3G harden the task of roaming and interoperating whereas 4G provides global mobility and service portability by its digital packet network. The disabilities and drawbacks of 3g motivate deploying 4G [3]. The network architecture has a core component of system integration [2]. The existing wireless technologies are seamlessly integrated in 4G and which provides fast and pervasive access and service for mobile user. The mobility and networking are combined and to develop a new class of interesting applications [4].

Security is a challenging problem due to mobile networking. User mobility increases the risk of illegal users masquerading as legal users and radio channels have become more vulnerable to eavesdroppers [4]. Security is essential in wireless networks due to increasing demands for applications like as text messaging (SMS), eb and

WAP access, Multimedia Messaging (MMS) and content downloads and these require higher bandwidth video applications such as video sharing, mobile video and IPTV is quickly growing [13].

1.2. Authentication 4G networks

Authentication is a primary security mechanism to verify the source of what they claim to be [1]. The increasing security threats and attacks in mobile communications impose the need of authentication of mobile subscriber and network. The authentication technique can identify correct mobile subscribers as well as the mobile network. This can be implemented by collecting three entities like SIM, Password and Biometric property like caller's fingerprint, image, voice print, retinal scan, clapping and flipping sound etc. and cross interchanging between MS (mobile station/subscriber), SIM (Subscriber Identity Module) and the network [4]. There are various authentication schemes like

- public key-based authentication scheme
- symmetric key based authentication scheme
- mutual authentication mechanism
- user authentication
- handoff authentication
- Extensible Authentication Protocol [10] [11][12]

Generally some extra messages are added to the original message in flow authentication procedure and which leads to throughput reduction or increase in processing time. Hence, mobile nodes face long authentication delays, affecting the goodput. Most of the existing authentication protocols have been designed for scenario in which client device directly connects to a trusted device (e.g., an access point). On applying to the multihop scenario, the duration of the authentication process increases significantly. The reduction of the processing time on authentication procedure is required for a smooth and seamless hand over [5] [14] [15].

1.3. Problem Identification

There are only a limited number of works done in reducing authentication delay in 4G networks. Moreover the existing works on reducing authentication delay in 4G networks shows a performance decrease in efficiency [5], increased delay [6] etc.

Hence our objective is to propose a mechanism for reducing delay in authentication in 4G networks with high performance, throughput, delivery ratio, and with reduced overhead.

2. LITERATURE REVIEW

Kevin Lee et. al., [5] proposed two techniques to minimize the initial authentication delay without compromising the authentication process and overall security. One is fast authentication which admits data traffic temporarily by the network to the gateway and the immediate parent node of the joining node presents network-side authentication. The next is prefetch-assisted authentication, which enable the authenticated wireless nodes prefetching and storing the authentication vectors of the potential mobile clients. However efficiency of protocol is decreasing.

F. Hadiji et. al., [6] presented an authentication protocol in handoff for overlapping wireless networks security which determined the optimum solution providing best performance in terms of network parameters such as handoff latency and signaling overhead. The proposed protocol decreases the latency delay and the overhead of the network. However the latency delay is not much reduced.

Kamal Ali Alezabi et. al., [7] proposed an Efficient EPS-AKA protocol (EEPS-AKA) based on the Simple Password Exponential Key Exchange (SPEKE) protocol. This is a faster method as it uses a secret key method which is faster than certificate-based methods. Also, the size of messages exchanged between User Equipment (UE) and Home Subscriber Server (HSS) was reduced, which in turn reduced authentication delay and storage overhead effectively.

Yu-Lun Huang et. al., [8] proposed a Secure Authentication Key Agreement Protocol (S-AKA) to enhance the security to resist the attacks. The efficiency and redundancy of UMTS AKA was enhanced by S-AKA reducing both the authentication messages and bandwidth consumption of UMTS AKA. The formal proof of S-AKA was also given to ensure the security strength of S-AKA.

Masoumeh Purkhiabani and Ahmad Salahi [9] presented a protocol increasing authentication performance. The protocol share serving network with Home Subscription Server (HSS) for execution of authentication procedure and increasing a little computation in Mobility Management Entity (MME) and generated joined authentication vectors in both MME and HSS can remove aforementioned problems during authentication process.

Shen-Ho Lin et. al., [16] proposed a protocol fast iterative localized reauthentication (FIL re-authentication) which replaced the fast re-authentication of EAP-AKA protocol. The protocol impose some modifications to attain the same security level as EAP-AKA and made use of both localized re-authentication process and iterative process within the AP to manage the fast re-authentication locally and iteratively for speeding up the re-authentication. However it has an increased authentication delay.

Ali al Shidhani and Victor C. M. Leung [17] proposed LFR protocol to minimize re-authentication delays by slightly modifying the key management hierarchy in the EAP-AKA protocol to improve performance and security during re-authentication. LFR underwent localized authentication within the WLAN domain to reduce the authentication delay occurred between the WLAN domain and the 3GHN.

Ali al Shidhani and Victor C. M. Leung [18] proposed a pair of re-authentication protocols to reduce re-authentication delays on UMTS-WLAN VHs (Universal Mobile Telecommunication Systems- IEEE 802.11 wireless local area networks Vertical Handover). The protocol substantially reduced message signaling. In addition, the scheme attained secured key management and mutual authentication between the UE and authentication servers in the 3G Home Networks. However it had an increasing much authentication time.

Jahan Hassan et. al., [19] proposed trust-based fast authentication mechanism. In addition two handoff algorithms were developed to support the trust cloud model. Then the scheme developed analytical model using Markov chains, followed by the model validation using simulation studies and analytical results.

3. PROPOSED SOLUTION

3.1. Overview

In our paper authentication messages are exchanged among User Equipment, Mobility Management Equipment and Home Subscriber Server [7]. Here the MME computes its key V, so that the protocol starts to send the identity request message to the UE.

While MME sends registration request to UE, we use a trust aware handoff algorithm to select the handoff access point (AP) which in turn offers a fast authentication. This algorithm is based on BS to BS trust.

In this trust model, the serving base station (BS) of the mobile node (MN) shares the currently attached key of MN with trust cloud. Based on the number of BSs in the serving BS's trust cloud, some of the BS contains the keys to be utilized for fast authentication. When MN hands off to one of these BSs, MN shares the key among BSs of the trust cloud.

Completing authentication, a local authentication agent perform re authentication on request by mobile user to check whether the identity is legal or not [16]. The re authentication is carried in the form of iterative fast re-authentication process. This is made by generating fast re authentication identity by authentication vectors and the identities are delivered to access point databases via AVD (authentication vectors distributor). Figure 1 shows the block diagram of the proposed authentication protocol.

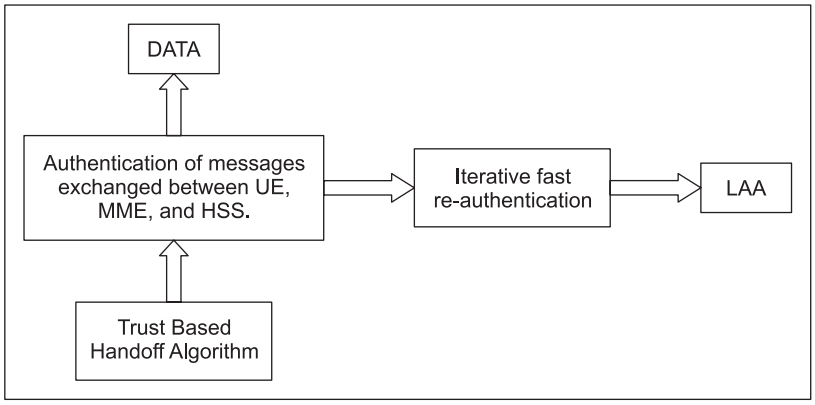

Figure 1: Block Diagram

3.2. Authentication Protocol

3.2.1. Exchanging Messages

The authentication protocol consists of the following components [7]:

1. User Equipment (UE) and International Subscriber Identity Module (ISIM).
2. Enhanced Node Base station (eNB), and Mobility Management Equipment (MME). The Access Security Management Entity (ASME) is hosted in the MME to provide access security and it is chosen as a key distributor in the EPS-AKA protocol.
3. Home Subscriber Server (HSS).

The protocol uses two random values s and t which is chosen by the UE to generate the key U. initially MME computes the value V and send it to the UE along with the user identity message. After that, UE computes its value U with s and t along with the shared secret key K_{um} using f function, this key is used to protect the IMSI. MME after receiving the protected IMSI (PIMSI) calculates the K_{um} key and forwards it to HSS with other values. Figure 2 shows the pictorial representation of the authentication protocol.

3.2.2. Algorithm

1. Initially the MME computes its value $V = g^m \bmod p$, and attaches V to the user identity request message and send it to UE via eNB.
2. UE computes the value $U = g^s t \bmod p$, and by using the received V it computes the symmetric shared key $K_{um} = V^u \bmod p$. This key is computed between UE and MME. UE chooses a random nonce R_u and uses the key K_{um} with function f to compute protected IMSI (PIMSI) which is given by,

$$PIMSI = f_{Kum}(IMSI, R_u) \tag{1}$$

3. The UE sends the message U, PIMSI, R_u to the MME.

4. MME after receiving the identity response message, computes the shared key $K_{um} = U^m \bmod p$ and forwards K_{um}, PIMSI, R_u to the HSS server. The MME computes the shared key which is computed in UE and HSS,

$$K_{uh} = K_{um} \oplus K \tag{2}$$

where K is a pre-shared key between UE and HSS

5. The HSS checks the IMSI and recovers the corresponding key for the UE. It checks the received value R_u with the value retrieved from PIMSI, and then it computes key K_{uh}, which is computed in UE and HSS. After that it chooses random value R_h, uses K_{uh} and R_h to generate HSS Verification value (HSSV) and Expected Response (XRES) and sends it to MME, where

$$HSSV = f1_{Kuh}(R_u, R_h) \tag{3}$$

$$XRES = f2_{Kuh}(R_h) \tag{4}$$

6. Next to this MME generates a random value R_m and computes MME Verification value (MMEV) and sends the message (MMEV, R_m, R_h) to UE.

$$MMEV = f1_{Kum}(HSSV, R_m) \tag{5}$$

7. UE then verifies the HSSV and MMEV to authenticate HSS server and MME, if matches it generates the RES value and sends it to MME.

$$XRES = f2_{Kuh}(R_h) \tag{6}$$

8. MME checks the received RES with the XRES, if matches it sends a success message to UE, otherwise it sends a failure message.

3.3. Trust Based Handoff Algorithm - Fast Authentication

While MME sends registration request to UE, we use a trust aware handoff algorithm to select the handoff access point (AP) which in turn offers a fast authentication. This algorithm is based on BS to BS trust.

In this trust model, the serving base station (BS) of the mobile node (MN) shares the currently attached key of MN with trust cloud. Based on the number of BSs in the serving BS's trust cloud, some of the BS contains the keys to be utilized for fast authentication. When MN hands off to one of these BSs, MN shares the key among BSs of the trust cloud.

Let TBS_L and UBS_L be the list of lightly loaded trusted and untrusted BSs.

Let MN be the mobile nodes

The steps involved in this algorithm are as follows:

1. If TBS_L = non-empty

   Then

   MNs perform the handoffs from TBS_L to first BS.

   This results in fast authentication.

   Else if TBS_L = empty and UBS_L = non-empty

   Then

   MN performs the handoffs from UBS_L to first BS.

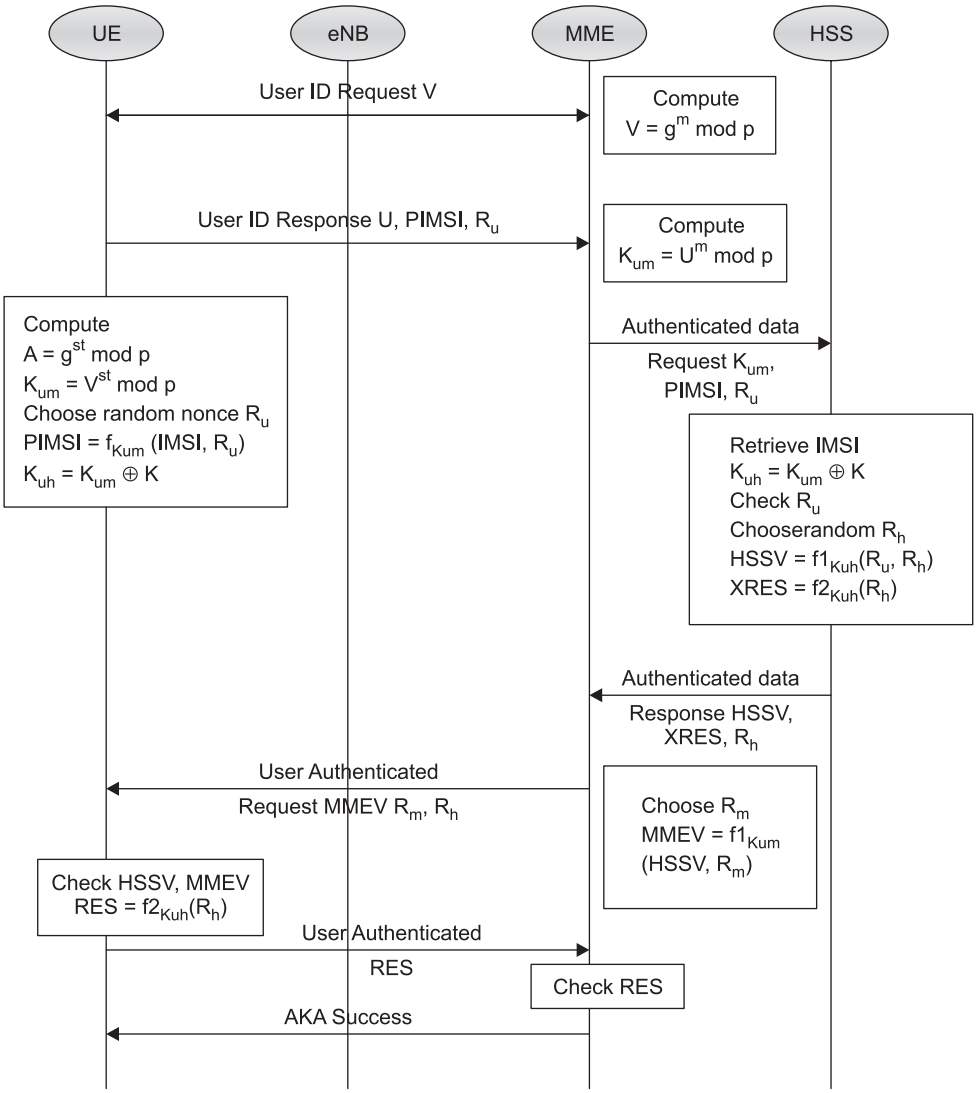

Figure 2: Authentication Protocol

This results in full authentication.

End if

2. If UBS_L = empty

Then

Handoff session is stopped.

End if

3.4. Iterative Localized Re-authentication Process

As an initial round of the iterative process the MS provides its temporal Fast_ID to request a re-authentication access, so that the fast iterative localized (FIL) re-authentication is launched to trigger the localized re-authentication process. Upon receiving the temporal Fast_ID, the Local Authentication Agent (LAA) is used in order to run the identity authentication. This checks whether the identity is authorized or not. If it is authorized

both the LAA and the UE runs the initial round iterative AVs generation for re-deriving new AVs, which are also stored back to its database, correspondingly.

When the MS responses the Fast_ID ($i-1$) to request a re-authentication access again, FIL re-authentication is invoked again for activating new round iterative process as an first round iterative process. Here the index 'i' denotes the i-th iterative process. The LAA after receiving the identity authentication function check s the identity and agrees running iterative localized re-authentication with the MS. As completing the identity authentication of this round iterative localized re-authentication, iterative AVs generation function from this round is subsequently invoked for deriving new AVs. When the MS requires a re-authentication access again, a new round iterative process is triggered for invoking a new round iterative localized re-authentication. This results in the generation of a new round iterative AVs generation again. As a result, if any error has been occurred during any round iterative localized re-authentication, the iterative process is terminated immediately. Meanwhile, while the MS requests a re-connection again, the full authentication will be activated. Figure 3 shows the flow diagram of the re-authentication process.

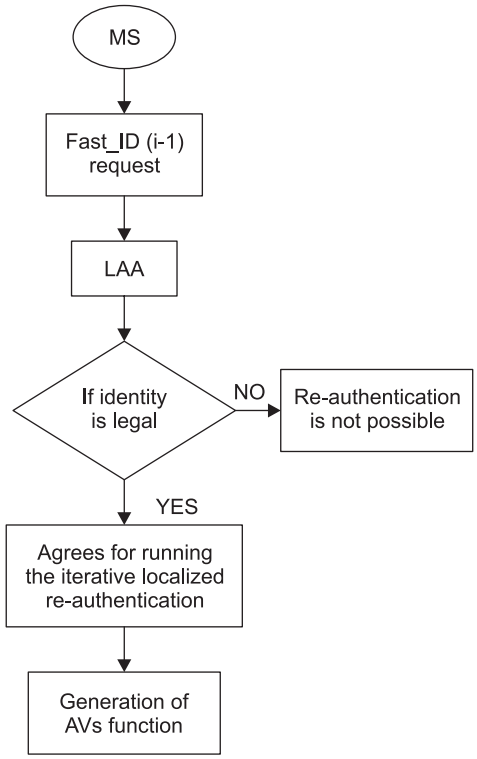

Figure 3: Flow Diagram

3.4.1. Overall Algorithm

1. Initially UE computes key U and MME compute key V and exchange among themselves.
2. UE chooses R_u and uses the key K_{um} with function f to compute protected IMSI (PIMSI) and forwards to MME along with the message U.
3. MME computes the shared key and forwards K_{um}, PIMSI, R_u to the HSS server.
4. HSS checks the IMSI checks the received value R_u with the value retrieved from PIMSI and computes key K_{uh}.
5. HSS chooses random value R_h, uses K_{uh} and R_h to generate HSSV and XRES and sends it to MME.
6. Next MME generates R_m and MMEV and sends the message (MMEV, R_m, R_h) to UE.

7. UE then verifies the HSSV and MMEV to authenticate HSS server and MME, if matches it generates the RES value and sends it to MME.
8. MME checks the received RES with the XRES, if matches it sends a success message to UE, otherwise it sends a failure message.
9. In the second stage for providing fast authentication, nodes which are already present in the network authenticate the joining node using trust aware handoff algorithm.
10. Based on the trust level of the nodes, the nodes perform the handoff to BS.
11. In the third stage, for re-authentication the MS send a Fast_ID (*i*-1) to request a re-authentication access.
12. The LAA after receiving the request identity checks whether it is legal or not.
13. If it is legal the iterative AVs generation is done.
14. If any error has been occurred during any round of the iterative localized re-authentication, the iterative process is terminated immediately.

4. SIMULATION RESULTS

4.1. Simulation Model and Parameters

To simulate the proposed scheme, NS-2 [20] is used. In the simulation, a WLAN- LTE heterogeneous network is considered. It consists of 4 base stations among which, 2 are based on LTE and remaining 2 are based on WLAN. The base stations BS1 and BS2 marked with orange circle belongs to 802.11 WLAN and base stations eNB1 and eNB2 marked with blue circle belongs to LTE network. Each network contains 5 clients (refer Figure 4). All nodes have the same transmission range of 250 meters. In our simulation, Mobile node 3 and 13 perform vertical handoff.

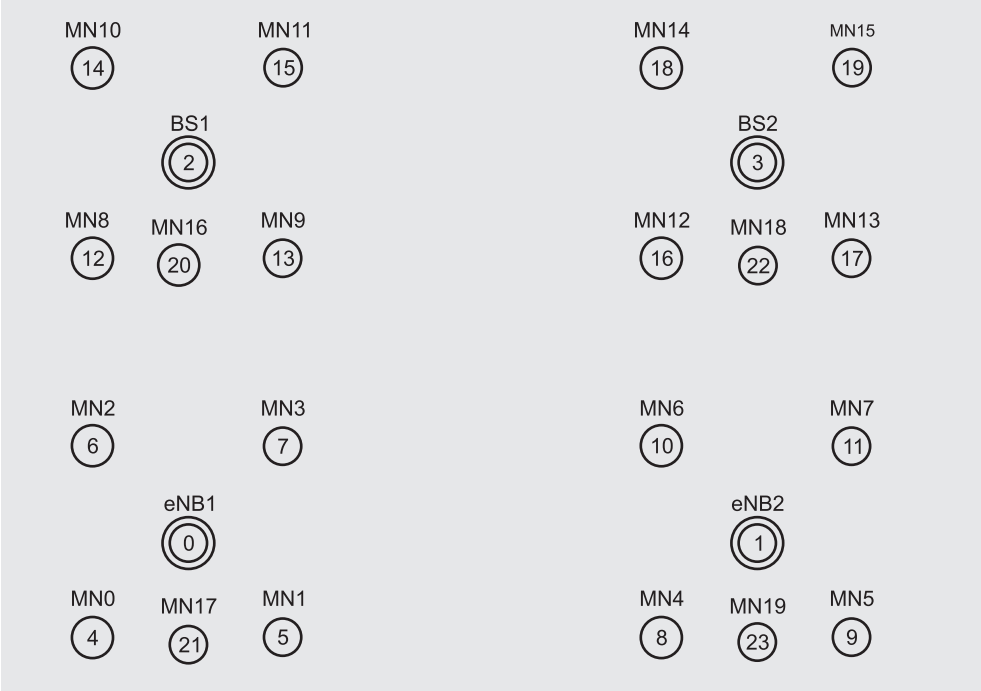

Figure 5: Simulation Topology

The simulation settings and parameters are summarized in table.

No. of Mobile Nodes	20
Area Size	500 × 500
MAC	E-UTRAN and 802.11
Transmission Range	250 m
Simulation Time	50 sec
Traffic Source	CBR
Packet Size	512
Rate	50, 100, 150, 200 and 250 kb
Number of eNB	2
Number of BS	2
Speed of Mobile node	10 m/s

4.2. Results

The proposed Enhanced Authentication for Delay Reduction in 4G networks (EADR) is compared with the Evolved Packet System AKA (EPS-AKA) technique [7].

4.2.1. Performance Metrics

(i) **Authentication Delay:** The total authentication delay (D_{auth}) is composed of three delay elements: the processing, transmission, and propagation delays:

$$D_{auth} = D_{proc} + D_{trans} + D_{prop} \tag{7}$$

The transmission delay, D_{trans}, is the delay experienced while transmitting an EAP message.

The processing delay D_{proc} is the delay experienced by each node while processing a message. Cryptographic operations and key generation accounts for most of the processing delay.

D_{prop} is a one-direction propagation delay between the UE and the AP.

(ii) **Bandwidth Cost:** To evaluate the bandwidth consumption of the re-authentication, all transaction message size between different network entity sections in one round authentication session are calculated.

(iii) **Packet Delivery Ratio:** In order to evaluate the packet drops due to attacks and network disconnections, the packet delivery ratio (PDR) is estimated. The PDR is given by

$$PDR = pkt\_rec/pkt\_snt \tag{8}$$

where pkt_rec and pkt_snt are the total number of data packets received and sent, respectively.

4.2.2. Varying Handoff Attempts

In handoff scenario-1, the number of handoff attempts is increased from 1 to 5 in which node MN8, MN9 from BS1 of WLAN network is handoff to eNB1 of LTE network. Similarly MN7 and MN4 from eNB2 of LTE network is handoff to BS2 of WLAN network. Then MN15 from BS2 of WLAN network is handoff to eNB2 of LTE network.

Figure 6, 7 and 8 show the results of authentication delay, bandwidth cost and delivery ratio for both the approaches.

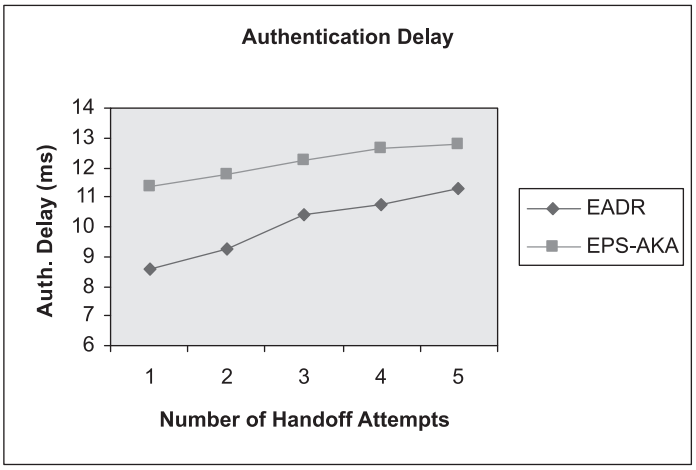

Figure 6: Authentication Delay for varying Handoff Attempts

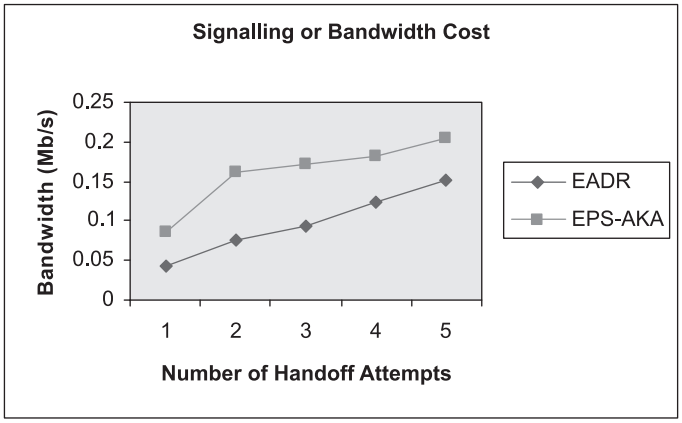

Figure 7: Bandwidth Cost for varying Handoff Attempts

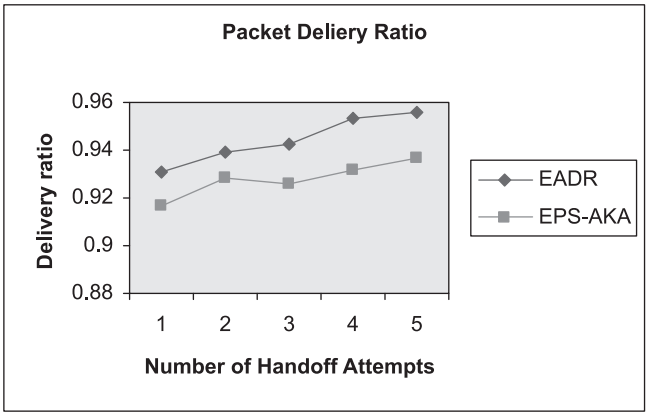

Figure 8: Packet Delivery Ratio for varying Handoff Attempts

The authentication delay is increased when the handoff attempts are more. From figure 5, we can see that EADR has 8% lesser authentication delay than EPSAKA because of the fast re-authentication process.

Similar to the authentication delay, the bandwidth cost is also increased when the handoff attempts are more. But EADR has exactly 50% reduced cost when compared to EPSAKA because of the load aware handoff technique, as seen from Figure 7.

Figure 8 shows the delivery ratio of EADR and EPSAKA techniques. We can see that delivery ratio of EADR is 3% of higher than EPSAKA, because of the trust aware handoff technique.

4.2.3. Varying Mobile Speed

In handoff scenario-2, the speed of the mobile nodes MN9 and MN4 during handoff are varied from 5 m/s to 25 m/s.

Figure 9, 10 and 11 show the results of authentication delay, bandwidth cost and delivery ratio for both the approaches, when the speed is increased.

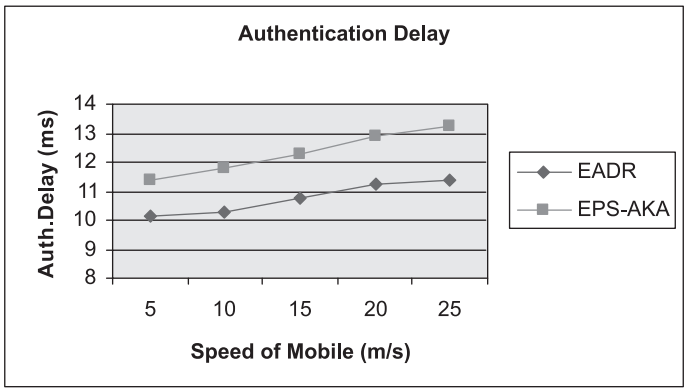

Figure 9: Authentication Delay for varying Speed

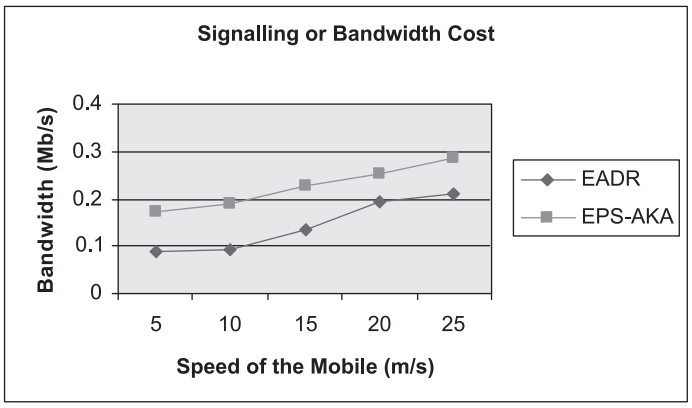

Figure 10: Bandwidth Cost for varying Speed

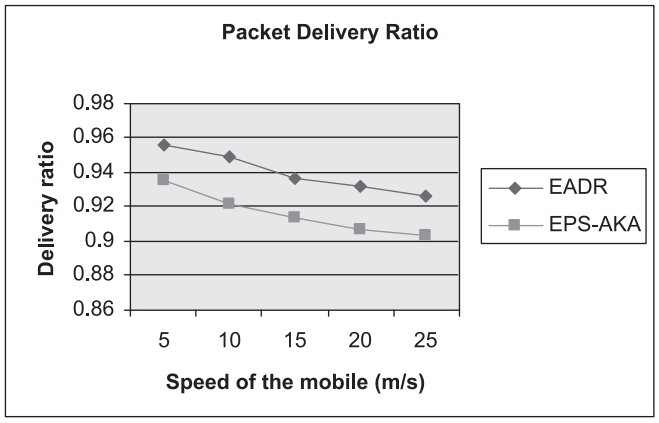

Figure 11: Delivery Ratio for varying Speed

Both the delay and bandwidth cost increases when the mobile speed increases. However EADR has 8% lesser delay and 40% lesser bandwidth cost, when compared to EPSAKA.

Figure 11 shows the delivery ratio of EADR and EPSAKA techniques. Due to increased disconnections, the delivery ratio begins to degrade beyond 5 m/s speed. But delivery ratio of EADR is 2% of higher than EPSAKA, because of the trust and load aware handoff technique.

5. CONCLUSION

In this paper we have provided security to 4G networks, by which the authentication messages are exchanged among User Equipment, Mobility Management Equipment and Home Subscriber Server. Next a fast authentication is provided using a trust aware handoff algorithm to select the handoff access point (AP). This algorithm is based on BS to BS trust. Completing authentication, a local authentication agent performs a re-authentication on request by mobile user to check whether the identity is legal or not. The re-authentication is carried in the form of iterative fast re-authentication process.

REFERENCES

[1] S. Arunkumar and P. Rajkumar, "Fast Re-Authentication for Efficient and Seamless Handover in 4g Networks", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), Volume 3 Issue 4, April 2014.

[2] Minsoo Lee and Sehyun Park, "A Secure Context Management for QoS-Aware Vertical Handovers in 4G Networks", Communications and Multimedia Security, Vol. 3677, 2005, pp. 220-229.

[3] Tamal Dhar and Chandan Koner, "Password and Biometric Based Mutual Authentication Technique for 4-G Mobile Communications", IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS), Vol. 3, No. 2, April 2013.

[4] Pijush Kanti Bhattacharjee and Rajat Kumar Pal, "Mutual Authentication Technique Applying Three Entities in 4-G Mobile Communications", International Journal of Computer Theory and Engineering, Vol. 3, No. 6, December 2011.

[5] Kevin Lee, Jing Deng and Raghuram Sudhaakar, "Fast Authentication in Multi-Hop Infrastructure-based Communication", in Proc. of IEEE International Conference on Communications - Communication and Information Systems Security Symposium (ICC), Sydney, Australia, June 10-14, 2014.

[6] F. Hadiji, F. Zarai and L. Kamoun, "Authentication Protocol in Fourth Generation Wireless Networks", IFIP International Conference on Wireless and Optical Communications Networks, WOCN, 2009.

[7] Kamal Ali Alezabi, Fazirulhisyam Hashim, Shaiful Jahari Hashim and Borhanuddin M. Ali, "An Efficient Authentication and Key Agreement Protocol for 4G (LTE) Networks", IEEE Region 10 Symposium, 2014.

[8] Yu-Lun Huang, C.Y. Shen, Shiuhpyng Shieh, Hung-Jui Wang and Cheng-Chun Lin, "Provable Secure AKA Scheme with Reliable Key Delegation in UMTS", Third IEEE International Conference on Secure Software Integration and Reliability Improvement, 2009.

[9] Masoumeh Purkhiabani and Ahmad Salahi, "Enhanced Authentication and Key Agreement Procedure of next Generation 3GPP Mobile Networks", International Journal of Information and Electronics Engineering, Vol. 2, No. 1, January 2012.

[10] Yu Zheng, Dake He, Xiaohu Tang and Hongxia Wang, "AKA and Authorization Scheme for 4G Mobile Networks Based on Trusted Mobile Platform", Fifth International Conference on Information, Communications and Signal Processing, 2005.

[11] Mohanaprasanth.P, B. Sridevi and Dr. S. Rajaram, "Secured Cost Effective Group Handover Authentication Scheme for WiMAX Networks", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), Volume 2, Issue 3, March 2013.

[12] Dake He, Jianbo Wang and Yu Zheng, "User Authentication Scheme Based on Self-Certified Public-Key for Next Generation Wireless Network", International Symposium on Biometrics and Security Technologies, ISBAST 2008.

[13] R. Narmadha, Dr. S. Malarkkan "Small cell security implementation and authentication deliberation" , International Journal of Applied Engineering Research, Volume 9, Number 22 (2014), pp. 13637-13644.

[14] R. Narmadha, Dr. S. Malarkkan and Dr. C. Ramesh, "Performance Analysis of Signaling Cost on EAP-TLS Authentication Protocol based on Cryptography", International Journal of Computer Applications (0975-8887), Vol. 33-No. 7, November 2011.

[15] R. Narmadha and Dr. S. Malarkkan, "Authentication Key Management Analysis For Heterogeneous Networks", i-manager's Journal on Wireless Communication Networks, Vol. 2, No. 1, 2013.

[16] Shen-Ho Lin, Jung-Hui Chiu and Sung-Shiou Shen, "A fast iterative localized re-authentication protocol for UMTS-WLAN heterogeneous mobile communication networks", EURASIP Journal on Wireless Communications and Networking 2011.

[17] Spectrum Holes Sensing: (Another type of "White Spaces" Challenges in Cognitive Radio network, is Presented in Springer International conference on Communication, Cloud and Big Data (CCB2016),Organized by Department of Information Technology, Sikkim Manipal Institute of Technology on November 2016, Sikkim manipal Institute, and Proceedings will be Published in Springer Lecture Notes on Networks & Systems. (Indexed by EI and SCOPUS).

[18] E-Agricultural Market, Published in IJCTA. [Scopus Indexed].

[19] Jahan Hassan, Harsha Sirisena and Bjorn Landfeldt, "Trust-Based Fast Authentication for Multiowner Wireless Networks", IEEE Transactions On Mobile Computing, Vol. 7, No. 2, February 2008.

[20] Network Simulator: http:///www.isi.edu/nsnam/ns