International Journal of Computer Theory and Engineering, Vol. 2, No. 2 April, 2010
1793-8201

Artificial Intelligence Based Mutual Authentication Technique with Biometric Entities in 3-G Mobile Communications

Pijush Kanti Bhattacharjee, *Member, IACSIT,* Chandan Koner , *Member, IACSIT* , Chandan Tilak Bhunia, Sr. *Member, IEEE* and Ujjwal Maulik, Sr. *Member, IEEE*

***Abstract*—An artificial intelligence based mutual authentication system with four entities is developed keeping any eye to enhancing threat and hacking in mobile network. Since voice frequency lies between 0 ~ 3.5 KHz, a person talking some specific word in different times is always consisting of a very narrow range of frequencies which are varying person to person. Voice frequency of the salutation or selective words used by a subscriber at the beginning of conversation like Hello, Good Morning, Namaskar etc is taken as first entity for authentication purpose. Second entity is chosen as frequency of flipping or clapping sound of the subscriber at the time of initializing a call. Then third entity is taken as face image of the calling subscriber. We propose fourth entity as probability of salutation or greeting word from subscriber's talking habit (set of salutation words) whiles the subscriber starts a call. These four entities such as probability of particular range of frequencies for the salutation word, frequency of flipping sound, face image matching of the subscriber, particular salutation or greeting word at the time of starting a call are used with most frequently, more frequently and less frequently by the subscriber like uncertainty in Artificial Intelligence (AI). Now different relative grades are assigned for most frequently, more frequently and less frequently used parameters and the grades are modified according to weightage. We invent a Fuzzy Rule (condition) by Fuzzy operation. If the results obtained from fuzzy operations are satisfied by the invented fuzzy rule, the subscriber (MS) and the network (MSC or PDSN) are mutually authenticated in 3-G mobile communications.**

Pijush Kanti Bhattacharjee is an Assistant Professor in the Department of Electronics and Communication Engineering, Bengal Institute of Technology and Management, Santiniketan, P.O. Doranda, West Bengal, Pin-731236, India. He was an Ex Asssitant Director in the Department of Telecommunications (DoT), Government of India, India. He has possessed vast working experience in the field of Telecommunications including Mobile Communications, Image Processing, Network Security, VLSI etc. He is a member of IACSIT, IAENG, CSTA, IE, ISTE, IAPQR.
(phone: +91-33-25954148; email: pijushbhatta_6@hotmail.com).

Chandan Koner is an Assistant Professor in the Department of Computer Science and Engineering, Bengal Institute of Technology and Management, Santiniketan, P.O. Doranda, West Bengal, Pin-731236, India. He is pursuing PhD course. He is member of IACSIT and IAENG.
(phone: +91-9434535556; email: chandan_durgapur@yahoo.com).

Chandan Tilak Bhunia is a Director, Bengal Institute of Technology and Management, Santiniketan, P.O. Doranda, West Bengal, Pin-731236, India. He is a FIE(I), FIETE and Senior Member of IEEE. (phone: +91-9434033157; email: ctbhunia@vsnl.com).

Ujjwal Maulik is currently a Professor in the Department of Computer Science and Technology, Jadavpur University, Kolkata, India. He is a FIE(I) and Senior Member of IEEE. (phone: +91-33-24131766; email: ujjwal_maulik@yahoo.com).

***Index Terms*—Flipping sound, Fuzzy operation Mutual authentication, Salutation word, USIM.**

I. INTRODUCTION

Artificial Intelligence (AI) is a theory based on uncertainty. Fuzzy operations [6] can be performed for taking decision in AI based application. AI can be applied in such applications which are based on uncertainties like vagueness, ambiguity and imprecision. Subscriber's talking habit is also based on uncertainties.

This provides a research challenge for application of AI on subscriber authentication. We propose to use parameter of subscriber's talking habit. It means which particular range of frequency of the salutation (greeting) word, frequency of flipping sound, face image matching, salutation word are used with most frequently, more frequently, less frequently by a subscriber while initializing the call. By applying theory of AI, different relative grades can be assigned for most frequently, more frequently, less frequently used parameters considering talking pattern of the subscriber. Fuzzy sets are derived from the modified relative grades which are obtained by assigning weightage. Then fuzzy operations are performed on fuzzy sets, results of fuzzy operations are analyzed by setting an invented fuzzy rule or condition. If the results are satisfying the fuzzy rule, the subscriber (MS) as well as the network (MSC or PDSN) is authenticated, otherwise not.

Thus we propose an AI based subscriber authentication scheme that will check the authenticity of a subscriber by fuzzy operations on fuzzy sets which are derived from talking habit of the subscriber especially salutation word, its frequency, flipping sound frequency and face image matching of the subscriber at the time of starting a call.

II. AUTHENTICATION TECHNIQUE IN 3-G MOBILE COMMUNICATIONS NETWORK

In 3-G mobile communication, voice communication is held by MSC (Main Switching Center) and its accessories. In packet switching, authentication is done separately by PDSN (Packet Data Serving Node) servers [1], [4], [5]. The existing authentication technique is described below.

In circuit switching, the authentication for establishing voice path is done by the following procedure,

1) Mutual authentication where MS and MSC are

IACSIT
International Association of Computer Science and Information Technology
WWW.IACSIT.ORG

confirmed identity individually.

2) Assure that the authentication information and keys are not being re-used (key freshness).

Additional parameters and cryptographic checks are introduced in 3-G network to provide mutual entity authentication between the USIM (Universal Subscriber Identity Module) at the user side and the AUC (Authentication Center) at the network side. This technique uses symmetric key or code using a secret subscriber authentication key K which is shared between and available only to the USIM and the AUC in the user's HE (Home Environment). In addition, the AUC entrusts with track of a counter SQN_{HE} and at the same time USIM controls track of a counter SQN_{MS}. It also stores additional data to support network authentication providing the user with assurance by key freshness. This scheme is assembled of a challenge/response protocol identical to the 2-G mobile subscriber authentication with an additional feature of network authentication. The HE, which manages both the AUC and the USIM, possesses some technique in the management of sequence numbers.

A. Authentication for Circuit Switching in 3-G Mobile Communications Network

Authentication in the 3G network utilizes following Challenge/Response mechanism [1],

1) The VLR (Visitor Location Register) sends a request to the user's AUC.
2) After receiving the request the AUC generates an ordered array of n quintets which are being sent to the VLR. Each quintet consists of the following components, such as Challenge (RAND), Expected response (XRES), Cipher key (CK), Integrity key (IK), Authentication token ⊕ (AUTN = SQN [⊕ AK] || AMF || MAC-A). [where is bit wise EX-OR operation] The AUC generates each quintet by the following procedure:
   - Generates a fresh sequence number SQN from a counter SQN_{HE}.
   - Generates an unpredictable challenge RAND.
   - Computes a message authentication code for authentication MAC-A = $f1_K$ (SQN || RAND || AMF) where f1 is a message authentication function;
   - Computes an expected response XRES = $f2_K$ (RAND), where f2 is a (possibly modified) message authentication function;
   - Computes a cipher key CK = $f3_K$ (RAND), integrity key IK = $f4_K$ (RAND) and anonymity key AK = $f5_K$ (RAND), where f3, f4, f5 are key generating functions.
   - Computes the concealed sequence number⊕SQN AK.
   - Assembles the authentication token AUTN = SQN⊕[AK] || AMF || MAC-A and the quintet Q = (RAND, XRES, CK, IK, AUTN) and updates the counter SQN_{HE}.
3) AUC sends that ordered array of n quintets to the VLR.
4) When the VLR initiates the authentication scheme it selects the next quintet from an array held in the VLR and sends the parameters RAND and AUTN to the user.
5) After receiving of a (RAND, AUTN) from the VLR, USIM in MS computes the following procedure:
   - If the sequence number is concealed, the USIM computes the anonymity key AK = $f5_K$ (RAND) and retrieves from AUTN the unconcealed sequence number SQN = (SQN AK).
   - The USIM then computes XMAC-A = $f1_K$ (SQN || RAND || AMF) and compares XMAC-A with MAC-A which is included in AUTN.
   - If they are not matching i.e. MAC-A ≠ XMAC-A, the USIM directs the MS to fail a user authentication response with indication of integrity failure to the VLR and cancels the further execution.

   If they are matched i.e. MAC-A = XMAC-A, the USIM computes the following:
   - The USIM verifies that the received sequence number SQN is acceptable or not.
   - If the sequence number SQN is not acceptable, the USIM computes the re-synchronization token AUTS and directs the MS to fail a user authentication response, with an indication of synchronization failure, including the re-synchronization token AUTS and abandons the procedure.

   If SQN is acceptable, the USIM progresses through the following procedures:
   - The USIM then computes the response RES = f2K(RAND) and directs the MS to send back a user authentication response back to the VLR, with an indication of successful receipt of the signed challenge and including the response RES.
6) The VLR compares the received RES with XRES. If they identical, the VLR confirms that the MS (USIM) is authentic and therefore authentication proceeding is successfully completed.

B. Authentication for Packet Switching in 3-G Mobile Communications Network

Authentication for packet switching [3] is done by AAA (Authentication, Authorization and Accounting) server [1], [4], [5]. Authentication requires the user to provide an account number or identifier and password i.e. exchange of logical keys or certificates between the client (MS) and the server in PDSN. If this authentication is correct, then MS is permitted for packet data service by Authorization.

An AAA server is a server program that handles user requests for access to network resources. The AAA server typically interacts with network access and gateway servers and with databases and directories containing user information.

III. Proposed Artificial Intelligence Based Authentication Technique In 3-G Mobile Communications Network

The proposed artificial intelligence based authentication scheme can be applied to either circuit switching or packet switching mobile communications network to provide voice, data, multimedia services etc. It is a collection of two different phases, namely, Subscriber Enrollment Phase and Subscriber Authentication Phase. These two phases are explained below.

A. Subscriber Enrollment Phase

In subscriber enrollment phase, the subscriber is enrolled to particular AAA server or switch belonging to the network. This phase is executed only once for one subscriber.

ASE1: The subscriber sends an application request to the authority concerned (mobile service provider) for new SIM.

ASE2: After receiving the request, the authority asks to submit his different parameters of talking and flipping sound and tests his different talking habit. Clapping sound is made by striking the two hand's palms simultaneously, whereas flipping sound is made by rubbing the thumb and the middle finger's topmost portion of the subscriber (MS).

These two type of sounds, either clapping sound or flipping sound, are produced according to the physical characteristics of the subscriber (MS) i.e. this sound depends on construction of palms at the hands or the fingers whose formation quietly rests on heart and muscle capacity with other physical parameters of the subscriber's body. This clapping or flipping sound is varying in frequency from subscriber to subscriber. The actual frequency component of clapping or flipping sound has to identify by highly sophisticated electronics instrument which can analyze exact frequency range in Hz. Since flipping sound is more convenient to produce at the time of making a mobile call, we consider flipping sound. F is average value of flipping frequency of a subscriber in Hz from five consecutive flipping sounds made by the subscriber.

ASE3: After that authority examines those tests thoroughly and performs a feasibility study of talking habit of the subscriber. The authority records the followings,

(i) Which frequency range in voices is appearing most frequently, more frequently and less frequently used by the subscriber in course of a salutation or greeting word talking? For detecting the voice frequency of a salutation word, highly sophisticated electronics instrument is fitted either at the MS or the server which can detect the exact frequency in Hz.

(ii) What are most frequently, more frequently and less frequently frequency of flipping sound?

(iii) Which subscriber's face image in the database is most frequently, more frequently and less frequently matched with the calling subscriber's face image while start talking?

(iv) Which salutation words are most frequently, more frequently and less frequently used by the subscriber at the time of starting a mobile call?

Frequency of salutation word and flipping sound are measured by sophisticated electronic instrument in Hz and face image of the subscriber is taken by digital camera with high resolution, generally both these instruments are inbuilt in mobile phone (MS).

ASE4: The authority uses four databases in the sever for storing the above subscriber parameters based on talking habit. The first database, D_V stores the subscriber most frequently, more frequently and less frequently used voice frequencies for each salutation word and its corresponding relative grades. The first range of voice frequency for the salutation word emanating from the subscriber is D_{VR1} of D_V, which stores the most frequently (dominant) used voice frequency of the salutation word and its relative grade which is assigned by 0.65. The second class D_{VR2} of D_V, stores the more frequently used voice frequency of the salutation word and its relative grade which is assigned by 0.23. The third range D_{VR3} of D_V, stores the less frequently used voice frequency of the salutation word and its relative grade, assigned by 0.12. Likewise a database is prepared for voice frequency range most frequently, more frequently and less frequently for predicted all salutation words used by the subscriber. D_{VR1}, D_{VR2}, D_{VR3} of D_V are calculated as per following formula. Suppose D_V ranges between a Hz (lower frequency) to b Hz (higher frequency), compute c = (a+b)/2 and d = (b-a)/6 [since three equal divisions are made]. D_{VR1} ranges between e = (c-d) Hz to f = (c+d) Hz. D_{VR2} ranges between g = (e-d) Hz to h = (e-1) Hz and i = (f+1) Hz to j = (f+d) Hz. D_{VR3} ranges between k = (g-d) Hz = a Hz to l = (g-1) Hz and m = (j+1) Hz to n = (j+d) Hz = b Hz.

The second database, D_F stores the most probable, more probable and less probable flipping frequency of the subscriber and its relative grades. The first range of flipping frequency emanating from the subscriber is D_{FR1} of D_F, which stores the most frequently (dominant) used frequency of the flipping sound and its relative grade which is assigned by 0.9. The second class D_{FR2} of D_F, stores the more frequently used frequency of the flipping sound and its relative grade which is assigned by 0.6. The third range D_{FR3} of D_F, stores the less frequently used voice frequency of the flipping sound and its relative grade, assigned by 0.3. Likewise a database is prepared for flipping frequency range most frequently, more frequently and less frequently for flipping sound used by the subscriber. D_{FR1}, D_{FR2}, D_{FR3} of D_F are calculated as per following formula. Suppose D_F ranges between x Hz (lower frequency) to y Hz (higher frequency), compute p = (x+y)/2 and q = (y-x)/6 [since three equal divisions are made]. D_{FR1} ranges between r = (p-q) Hz to s = (p+q) Hz. D_{FR2} ranges between t = (r-q) Hz to u = (r-1) Hz and v = (s+1) Hz to w = (s+q) Hz. D_{FR3} ranges between k = (t-q) Hz = x Hz to l = (t-1) Hz and m = (w+1) Hz to n = (w+q) Hz = y Hz.

The third database, D_I stores face image of all subscribers with their statistical attributes like mean, standard deviation (std), moments, correlation coefficient, covariance etc or any other attributes like histogram, region, pixel indexing etc in the server or switch of a network e.g. each face image consisting of 16x16 pixels with its statistical parameters. First calling subscriber's face image matching is done by comparing statistical attributes (parameters) of the calling subscriber's face image with that of each stored data base image, accordingly the best match i.e. nearest image is search out. Then the calling subscriber's image is again compared with the best match image by matching each location pixels i.e. pixel wise. The number of pixels are matched either having same values or thresholding i.e. difference between the pixel values upto certain range say 10 or 15 or any appropriate value. If the best match face image in the data base to the calling subscriber's face image falls under category of 81% to 100% pixels matching, then relative grade is 0.9 and is stored in D_{IR1}. If 61% to 80% pixels are matched for the best match image, relative grade is 0.8 and is stored in D_{IR2}. If 41% to 60% pixels are matched for the best match image, relative grade is 0.3 and is stored in D_{IR3}.

The fourth database, D_W stores the most frequently, more frequently and less frequently used salutation words (starting time spoken) and their corresponding relative grades. The first row, D_{WR1} of D_W, stores the most frequently used salutation words and their relative grade which is assigned by 0.9. The second row, D_{WR2} of D_W, stores the more frequently used salutation words and their relative grade which is assigned by 0.6. The third row, D_{WR3} of D_W, stores the less frequently used salutation words and their relative grade which is assigned by 0.3.

Since these four parameters are completely different and independent to each other, therefore to make a fuzzy relation with mutual exclusive functions, we are imposing different weightage to these parameters. The ratio of weightage to probability of particular range of frequencies for the salutation word, frequency of flipping sound, face image matching of the calling subscriber with data base images, particular salutation or greeting word at call connecting time is considered like, $D_V : D_F : D_I : D_W = 1 : 0.9 : 0.8 : 0.75$. We are multiplying the relative grades by corresponding weightage to have the modified relative grades.

ASE5: If the authority does not get sufficient information, request for resubmission correct signature or database of the subscriber is placed. Then the authority executes the above steps again to create a strong database.

B. Subscriber Authentication Phase

When a subscriber requests for connecting a call, an announcement from the server (switch) may be issued to speak the salutation word which is intending to use by the calling subscriber for the called subscriber. After receiving salutation word from the calling subscriber, authentication process starts. If successfully authenticated, the calling subscriber is extended connection to the called subscriber, otherwise connection is denied. Thus after receiving the salutation or greeting word from a calling subscriber at the starting time of a call, the server (switch) executes the following operations:

ASA1: Finds the matched frequency of the salutation word within the rows D_{VR1}, D_{VR2}, D_{VR3} of D_V.

ASA1.1: After hearing the first speech from a subscriber, either MS or server computes frequency of the salutation word in Hz, then match the voice frequency of the salutation word within the stored range D_{VR1}, D_{VR2}, D_{VR3} of D_V and its corresponding relative grade which is taken as v1,

If not match, v1 = 0.

The membership functions of a fuzzy set F1 can be defined as follows,

$\mu_{F1}(a1) = v1$, [Since, weightage of v1 is 1]

Hence, $F1 = \{(a1, v1)\}$

ASA2: Finds the matched flipping frequency within the rows D_{FR1}, D_{FR2}, D_{FR3} of D_F.

ASA2.1: If the flipping frequency of the MS is matched, then stores p1= Relative grade of matched location in row, otherwise p1=0. The modified value of p1 according to the weightage is $p1_m$, where $p1_m = (p1) \times 0.9$,

The membership functions of a fuzzy set F2 can be defined as follows,

$\mu_{F2}(a2) = p1_m$

Hence, $F2 = \{(a2, p1_m)\}$

ASA3: Finds the matched subscriber face image within the rows D_{IR1}, D_{IR2}, D_{IR3} of D_I.

ASA3.1: If the face image of the MS (calling subscriber) is compared with the stored best match database image in the server or switch which is obtained by differencing statistical or any other attributes, then stores value q1= Relative grade of matched location in row, otherwise q1=0. Thus the modified value of q1 according to the weightage is $q1_m$, where $q1_m = (q1) \times 0.8$,

The membership functions of a fuzzy set F3 can be defined as follows,

$\mu_{F3}(a3) = q1_m$

Hence, $F3 = \{(a3, q1_m)\}$

ASA4: Finds the matched salutation or greeting word within the rows D_{WR1}, D_{WR2}, D_{WR3} of D_W.

ASA4.1: If the salutation word is matched within the stores value of D_{WR1}, D_{WR2}, D_{WR3}, then it stores w1= Relative grade of the matched salutation word in row, otherwise w1=0. The modified value of w1 according to weightage is $w1_m$, where $w1_m = (w1) \times 0.75$,

The membership functions of a fuzzy set F4 can be defined as follows,

$\mu_{F4}(a4) = w1_m$

Hence, $F4 = \{(a4, w1_m)\}$

ASA5: Computes fuzzy operations,

ASA5.1: $\mu_{F1 \cap F2 \cap F3 \cap F4}(a) = \min\{\mu_{F1}(a1), \mu_{F2}(a2), \mu_{F3}(a3), \mu_{F4}(a4)\}$

ASA5.2: $\mu_{F1 \cup F2 \cup F3 \cup F4}(a) = \max\{\mu_{F1}(a1), \mu_{F2}(a2), \mu_{F3}(a3), \mu_{F4}(a4)\}$

ASA6: For ascertaining the mobile subscriber (MS) as well as the network (MSC or PDSN) authenticity, an invented Fuzzy Rule (condition) on result of the fuzzy operations has been implied.

If $\mu_{F1 \cap F2 \cap F3 \cap F4}(a) \geq 0.22$ and

$\mu_{F1 \cup F2 \cup F3 \cup F4}(a) \geq 0.65$ satisfies, then only the server ensures that the subscriber is authentic, hence their mutual authenticity is verified. The server checks or computes the authentication process. Since primary databases are kept at the server (switch), if that stored values in respect of the parameters of the subscriber at the server are not matched with that of the subscriber as currently transmitted, further processing will be stopped which identifies that the network is unauthentic. Also if the above two fuzzy conditions are not satisfied, the server ensures that the user or the subscriber (MS) is unauthentic. In both the cases the server sends an authentication failure message to the subscriber.

IV. Results And Discussion

First of all the feasibility study of all subscribers talking habit from subscriber test and documents are made and the authority stores in server or switch those databases having different parameters with values.

Example1: A subscriber sends flipping frequency having 1275 Hz, starts talking with "Hi" frequency in 2325 Hz and transmits his face image which matches with the best (nearest) match face image with 55% pixels, examine authenticity of the subscriber and the network.

After testing voice frequency of the subscriber's salutation word "Hi" stored in the server, the range of voice frequency of the subscriber's particular salutation word "Hi" is found from 2235 Hz to 2726 Hz.

If the voice frequency of the subscriber's salutation word "Hi" is within 2398 Hz to 2562 Hz then the value D_{VR1} of D_V is 0.65.

If the voice frequency of the subscriber's salutation word "Hi" is within 2316 Hz to 2397 Hz and 2563 Hz to 2645 Hz, the value D_{VR2} of D_V is 0.23.

If the voice frequency of the subscriber's salutation word "Hi" is within 2235 Hz to 2315 Hz and 2646 Hz to 2726 Hz, the value D_{VR3} of D_V is 0.12.

After testing flipping frequency of the subscriber, the range of flipping frequency of the subscriber particular is found from 1210 Hz to 1292 Hz.

If the flipping frequency of the subscriber is within 1235 Hz to 1267 Hz then the value D_{FR1} of D_F is 0.9.

If the flipping frequency of the subscriber is within 1223 Hz to 1234 Hz and 1268 Hz to 1279 Hz, the value D_{FR2} of D_F is 0.6.

If the flipping frequency of the subscriber is within 1210 Hz to 1222 Hz and 1280 Hz to 1292 Hz, the value DFR3 of DF is 0.3.

After capturing face image of 16x16 pixels of subscriber with computing statistical or any other attributes (parameters), server or switch stores that image with the attributes in D_I. Firstly attributes of the calling subscriber image is compared with that of the stored images and the best match image is found. Then each position pixels of the subscriber's face image is compared with that of the best match image in the server or switch.

If 81% to 100% pixels of the face image of calling subscriber match with the stored best match image in D_I, then the value of D_{IR1} is 0.9. If 61% to 80% pixels of the face image of calling subscriber match with the stored best match image in D_I, then the value of D_{IR2} is 0.8. If 41% to 60% pixels of the face image of calling subscriber match with the stored best match image in D_I, then the value of D_{IR3} is 0.3.

The salutation or greeting words are stored in the server for the subscriber in D_{WR1} of D_W like,

Hello, Oh God, Jai-Ram, Adab, Namaste.

The salutation words are stored in the server for the subscriber in D_{WR2} of D_W like,

Good Morning, Good Afternoon, Radhe-Radhe, Namaskar, Kaisa-Hai.

The salutation words are stored in the server for the subscriber in D_{WR3} of D_W like,

Hi, Assalamo-Alaokum, Joyguru, Hare-Ram, Hare-Krishna.

Let the relative grade of D_{WR1} is 0.9, D_{WR2} is 0.6 and D_{WR3} is 0.3.

For salutation word "Hi" of the subscriber, it is in D_{WR3} whose relative grade (w1) is 0.3

Hence, the matched frequency of the salutation word (2325 Hz) from the subscriber in $D_{VR2.}$

Therefore, v1= 0.23

μ_{F1} (a1) = v1 = 0.23,

Hence, F1 = {(a1, 0.23)}

The matched flipping frequency (1275 Hz) of the subscriber in $D_{FR2.}$

Therefore, p1= 0.6, $p1_m$ = p1 × 0.9 = 0.6 × 0.9 = 0.54

μ_{F2} (a2) = $p1_m$ = 0.54,

Hence, F2 = {(a2, 0.54)}

Since face image is matched with the best match (nearest) face image from database in server by 55% pixels in D_{IR3},

Therefore, q1= 0.3, $q1_m$ = q1 × 0.8 = 0.3 × 0.8 = 0.24

μ_{F3} (a3) = $q1_m$ = 0.24,

Hence, F3 = {(a3, 0.24)}

The matched the salutation (greeting) word of the subscriber in $D_{WR3.}$

Therefore, w1= 0.3, $w1_m$ = w1 × 0.75 = 0.3 × 0.75 = 0.225

μ_{F4} (a4) = $w1_m$ = 0.225,

Hence, F4 = {(a4, 0.225)}

Now, $\mu_{F1 \cap F2 \cap F3 \cap F4}$ (a) = min {0.23, 0.54, 0.24, 0.225} =0.225;

$\mu_{F1 \cup F2 \cup F3 \cup F4}$ (a) = max {0.23, 0.54, 0.24, 0.225} = 0.54

As fuzzy rule $\mu_{F1 \cap F2 \cap F3 \cap F4}$ (a) ≥ 0.22 and $\mu_{F1 \cup F2 \cup F3 \cup F4}$ (a) ≥ 0.65 is not true, so the sever ensures that the subscriber is not authentic, hence they are not mutual authenticated followed by authentication failure message.

Example2. The subscriber (same subscriber as in Ex1) starts talking with "Good Morning" in 1915 Hz, sends flipping frequency in 1231 Hz and face image matching with the best match (nearest) image by 78% pixels, examine mutual authenticity of the subscriber with the network.

After testing voice frequency of the subscriber's salutation word "Good Morning" from the server, the range of voice frequency of the subscriber's particular salutation word "Good Morning" is found from 1734 Hz to 2256 Hz.

If the voice frequency of the subscriber's salutation word "Good Morning" is within 1908 Hz to 2082 Hz then the value D_{VR1} of D_V is 0.65.

If the voice frequency of the subscriber's salutation word "Good Morning" is within 1821 Hz to 1907 Hz and 2083 Hz to 2169 Hz, the value DVR2 of DV is 0.23.

If the voice frequency of the subscriber's salutation word "Good Morning" is within 1734 Hz to 1820 Hz and 2170 Hz to 2256 Hz, the value D_{VR3} of D_V is 0.12.

Hence, the matched voice frequency of the salutation word (1915 Hz) from the subscriber in D_{VR1}

Therefore, v1= 0.65

μ_{F1} (a1) = v1 = 0.65,

Hence, F1 = {(a1, 0.65)}

D_F and DW are remaining same value as in Example1 since the same subscriber is talking, otherwise D_F and D_W have to be computed separately.

The matched flipping frequency (1231 Hz) of the subscriber in D_{FR2} of $D_{F.}$

Therefore, p1= 0.6, $p1_m$ = p1 × 0.9 = 0.6 × 0.9 = 0.54

μ_{F2} (a2) = $p1_m$ = 0.54,

Hence, F2 = {(a2, 0.54)}

Since face image is matched with the best match (nearest) face image from database in server by 78% pixels in D_{IR2},

Therefore, q1= 0.8, q1m = q1 × 0.8 = 0.8 × 0.8 = 0.64

$\mu F3\ (a3) = q1_m = 0.64$,

Hence, $F3 = \{(a3, 0.64)\}$

The matched the salutation (greeting) word "Good Morning" of the subscriber in D_{WR2} of D_W.

Therefore, $w1 = 0.6$, $w1_m = w1 \times 0.75 = 0.6 \times 0.75 = 0.45$

$\mu_{F4}\ (a4) = w1_m = 0.45$,

Hence, $F4 = \{(a4, 0.45)\}$

Now, $\mu_{F1 \cap F2 \cap F3 \cap F4}\ (a) = \min\ \{0.65, 0.54, 0.64, 0.45\} = 0.45$;

$\mu_{F1 \cup F2 \cup F3 \cup F4}\ (a) = \max\ \{0.65, 0.54, 0.64, 0.45\} = 0.65$.

As fuzzy rule set as, $\mu_{F1 \cap F2 \cap F3 \cap F4}\ (a) \geq 0.22$ and $\mu_{F1 \cup F2 \cup F3 \cup F4}\ (a) \geq 0.65$ is true i.e. the fuzzy rule satisfies results of the fuzzy operations, so the server ensures that the subscriber is authentic, hence they are mutual authenticated.

V. Advantages Of The Proposed Authentication Technique

This technique is highly efficient due to artificial intelligence used and no further information has to be supplied by the subscriber (MS) while making a call. The characteristics of this authentication scheme are,

1) This mobile subscriber as well as network authentication technique enjoys the advantages of artificial intelligence and fuzzy theory, so it is a unique one.
2) Artificial intelligence is efficiently employed to the server and subsequently it takes part to authenticate correct subscriber as well as network (server or switch).
3) Authenticity is decided by the subscriber's talking characteristics (habit) and face image analysis with database consisting of face images with attributes, flipping frequency, salutation word's frequency, salutation word's probability of all subscribers in the network at the server or switch.
4) No cryptography algorithm or any complex functions are applied for this authentication purpose.
5) The authentication technique depends on the assigned values of the Fuzzy Rule (condition), more accuracy is obtained by presuming suitable or proper values.
6) This authentication technique ensures result with in a real time basis.

VI. Conclusion

In our proposed artificial intelligence based technique, subscriber as well as network mutual authentication scheme is developed. A novel artificial intelligence is introduced to the server for this mutual authentication purpose. Thus this authentication technique can be spread out in various wireless communication networks within a real time basis.

References

[1] William C. Y. Lee, Wireless and Cellular Communications, 3rd Edition McGraw Hill Publishers 2008.

[2] T. S. Rappaport, Wireless Communication: Principles and Practice, Prentice Hall Pub Ltd, 2nd Ed, 2007.

[3] C. T. Bhunia, Information Technology Network and Internet, New Age International Publishers, India, 5th Edition (Reprint), 2006.

[4] H. Kim, H. Afifi, "Improving Mobile Authentication With New AAA Protocols", IEEE International Conference on Communication (ICC 2003) vol 1, pp 497-501, May, 2003.

[5] C. Koner, P. K. Bhattacharjee, C. T. Bhunia, U Maulik, "A Novel Approach for Authentication Technique in Mobile Communications", International Journal of Computer Theory and Engineering, Singapore, vol. 1, no. 3, pp. 225-229, 2009.

[6] Vilem Novak, Jiri Mockor, Irina Perfilieva, Mathematical Principles of Fuzzy Logic, Kluwer Academic Publisher, 2006.

Dr. Pijush Kanti Bhattacharjee is associated with the study of Engineering, Management, Law, Indo-Allopathy, Herbal, Homeopathic and Yogic medicines. He is having qualifications ME, MBA, MDCTech, AMIE, BSc, BA, LLB, BIASM, CMS, PET, EDT, FWT, DATHRY, BMus, KOVID, DH, ACE, FDCI etc. He worked in Department of Telecommunications (DoT), Govt. of India from June 1981 to Jan 2007 (26 years), lastly holding Assistant Director post at RTEC [ER], DoT, Kolkata, India. Thereafter, he worked at IMPS College of Engineering and Technology, Malda, WB, India as an Assistant Professor in Electronics and Communication Engineering Department from Jan,2007 to Feb,2008 and Feb, 2008 to Dec, 2008 at Haldia Institute of Technology, Haldia, WB, India. In Dec, 2008 he joined at Bengal Institute of Technology and Management, Santiniketan, WB, India in the same post and department. He has written two books "Telecommunications India" & "Computer". He is a Member of IE, ISTE, IAPQR, IIM, India; CSTA, USA; IACSIT, Singapore and IAENG, Hongkong. His research interests are in Mobile Communications, Image Processing, Network Security, VLSI, Nanotechnology etc.

Mr. Chandan Koner did his B.Tech in 2005 and M.Tech in 2007 respectively. He is currently an Assistant Professor in the Department of Computer Science and Engineering, Bengal Institute of Technology and Management, Santiniketan, P.O. Doranda, West Bengal, Pin-731236, India. He is pursuing PhD course in Computer Science and Engineering from Jadavpur University, Kolkata, India. Mr. Koner is a Member of IACSIT, Singapore and IAENG,Hongkong. His research interests include Mobile Communications, Network Security, Data Mining and Sensor Networks etc.

Dr. Chandan Tilak Bhunia did his B. Tech and M. Tech in Radio Physics and Electronics in 1982 and 1984 and Ph.D in Computer Science and Engineering. He is currently Director, Bengal Institute of Technology and Management, Santiniketan, P.O. Doranda, West Bengal, Pin-731236, India. He is a Senior Associate of International Center for Theoretical Physics (ICTP), Italy. Dr. Bhunia is a Fellow of Institution of Electronics and Telecommunication Engineers (IETE) and Institution of Engineers (IE), India and a Senior Member of Institute of Electrical and Electronics Engineers (IEEE). His research interests include Mobile Communications, Network Security, Computer Networks, Electronics Semiconductors and Multimedia Systems.

Dr. Ujjwal Maulik did his BS in Physics and Computer Science in 1986 and 1989 respectively, and MS and Ph.D in Computer Science in 1991 and 1997 respectively. He is currently a Professor in the Department of Computer Science and Technology, Jadavpur University, Kolkata, India. Dr. Maulik received the fellowships from International Center for Pure and Applied Mathematics, CIPA, France, in 1994, 1996 and 2006 and International Center for Theoretical Physics (ICTP), Italy in 2007. Dr. Maulik is also a Fellow of Institution of Electronics and Telecommunication Engineers (IETE) and Institution of Engineers (IE), India, and a Senior Member of Institute of Electrical and Electronics Engineers (IEEE). His research interests include Soft Computing, Pattern Recognition, Data Mining, Bioinformatics, Parallel and Distributed Systems.