Artificial Intelligence Based Authentication Technique with Three Attributes in Vehicular Ad Hoc Network

Pijush Kanti Bhattacharjee, *Member,IACSIT*, Utpal Roy and Anup Kumar Bhattacharjee

***Abstract*—Vehicular Ad Hoc Network (VANET) is one of the wireless ad hoc networks which are based on IEEE 802.11 wireless standard enabling vehicle to vehicle and vehicle to roadside communications through air interface. Information (voice, message, data, image etc) are routed in the cells or networks, any node or person can hack or tamper the information. A new artificial intelligence based mutual authentication technique is developed. Since human 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 selective words used by the subscriber (driver of a vehicle or node) at the beginning of conversation like Hello, Good Morning, Namaskar etc is taken as first entity for the authentication purpose. Second entity is taken as probability of salutation or greeting word from subscriber's talking habit (set of salutation words) whiles the subscriber starts a call. Third entity is chosen as probable location (place) of the subscriber (node or vehicle) from the selective locations at the time of initializing a call i.e. distance between the subscriber and the network. These three entities such as probability of particular range of frequencies for the salutation word, particular salutation or greeting word, location at the time of starting a call are used with most frequently, more frequently and less frequently by the subscriber (node) 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 the assigned weightage of the relative grades. Then Fuzzy operations are performed on modified relative grades (sets). A Fuzzy Rule (condition) is invented. If the results obtained from fuzzy operations are satisfied by the fuzzy rule, the nodes (vehicles) or a node and the server (switch) are mutually authenticated in a Vehicular Ad Hoc Network.**

***Index Terms*—VANET, DSRC, CSMA/CA, MAC layer, Distributed Coordination Function, Authentication system, Fuzzy Rule**

I. Introduction

The basic mobile communications [1]-[4] is a costlier one and can not afford communications covering all regions in the world, especially in remote and less dense populated area where the normal mobile communications are not economically viable like long distance roadways or railway trucks etc.

In this case ad hoc network is the best solution. Two types of ad hoc wireless networks are invented, one is Mobile Ad Hoc Network (MANET), the other is Vehicular Ad Hoc Network (VANET) [5]-[8]. MANET and VANET is self forming network i.e. they can work without any centralized control like Base Station (BTS) or Switch (BSC, MSC etc) in mobile network or Access Point (AP) like server in LAN. Each terminal or node (either mobile phone or small computer) in a MANET or a VANET connecting through wireless media acts a voice or data terminal as well as a router or switch. A node in a cell communicates with the other nodes in its transmitting range through wireless medium. Thus a VANET is a subset of a MANET. In a VANET communications, certain number of moving vehicles in a small region constitutes a cell. It means that the range of wireless signal i.e. transmitting zone from a moving vehicle is within a limited area. A vehicle, called a node, can do transmitting, receiving and routing (connecting) to other nodes without any help of any switch like base station (BTS) connecting with other switches (BSC, MSC, PDSN etc) in mobile network or Access Point (AP) in LAN. Also the moving vehicle in a VANET cell can be connected to other nodes lying in other cell or other network with the help of basic mobile network, Internet etc. Therefore total connectivity in a VANET is assured. VANET are also known under different name like Dedicated Short Range Communications (DSRC), Inter Vehicle Communications (IVC) etc. Thus VANET will help the drivers of vehicles to communicate the information in form of voice, data, image, multimedia etc and ensure safe journey by minimizing road accidents, diverting or instructing the vehicle's direction in less populated roads avoiding traffic jam, to entertain each other by sending message, broadcasting etc. Vehicles in a VANET are having high degree of mobility i.e. the vehicles are moving very fast, especially in high ways. As a result the two vehicles are in a direct communication range staying about one minute time only i.e. two vehicles remain in one cell about 1 minute time when they are moving parallel direction, or even less than 1 minute when they are going in opposite direction. For this, VANET cell configuration and number of nodes in a particular cell is always changing in nature.

VANET is based on IEEE 802.11 wireless standard [6]-[8] which is mainly framed for WLAN, WiFi, MANET and VANET.

Pijush Kanti Bhattacharjee is an Assistant Professor in the Department of Electronics and Communication Engineering, Bengal Institute of Technology and Management, Santiniketan, WB, India. He was an Ex Asssitant Director in the Department of Telecommunications (DoT), Government of India, India. He is a member of IACSIT, IAEng, CSTA, IE. (phone: +91-33-25954148; email: pijushbhatta_6@hotmail.com).

Utpal Roy is an Associate Professor in Computer & System Science Department, Viswbharati University, Santiniketan, West Bengal, India. (phone: +91-3463-262751-56; email: roy.utpal@gmail.com)

Anup Kumar Bhattacharjee is a Professor in Electronics and Communications Engineering Department at National Institute of Technology, Durgapur, West Bengal, India.(phone: +91-343-2755221; email: akbece12@yahoo.com)

Initially 802.11 are implemented on WLAN at a speed of 1 or 2 Mbps (very slow) in 1997. Then IEEE 802.11 protocol family is upgraded into different versions. 802.11a uses Orthogonal Frequency Division Multiplexing (OFDM) modulation to deliver upto 54 Mbps in the wider frequency 5 GHz ISM band. 802.11b applies High Rate Direct Sequence Spread Spectrum (HR-DSSS) to achieve 11 Mbps in 2.4 GHz ISM band. 802.11g implements OFDM modulation, but operates narrow 2.4 GHz ISM band. The Federal Communications Commission (FCC) suggests for VANET frequency spectrum (bandwidth) of 75 MHz in the range of 5.850 GHz to 5.925 GHz in USA. In this seven channels are fragmented, having each 10 MHz bandwidth. Six channels are used for services and one channel is used for control purpose like broadcast services e.g. safety message, announcement etc. The 802.11 protocols apply Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) with acknowledgements for reliable communications and avoiding collision between packets. In a VANET, Medium Access Control (MAC) layer determines a contention based access protocol, termed Distributed Coordination Function (DCF). Actually MAC sublayer determines how the channel is allocated i.e. who will transmit next. Above MAC, there is Logic Line Control (LLC) to hide the difference between different 802 variants.

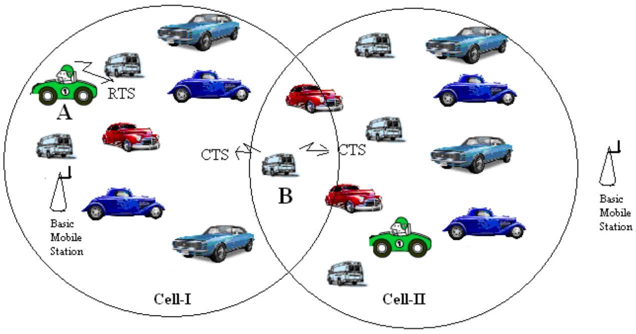

Fig. 1. Block Diagram of VANET Cells

In Fig. 1 Station A in Cell-I makes a call with station B in the same cell, first Request to send (RTS) signal from station A is transmitted to station B, after receiving RTS from station A, station B sends Clear to send (CTS) signal, provided that it is not engaged in any other communications. After receiving CTS from B, the station A sends the actual information (voice or data) in form of packets to station B. During information (voice or data) exchange between the stations A and B, the stations A and B are not disturbed or interrupted by any node within or without the cell-I. If transmitting power of a node (vehicle) increases in a VANET, signal from the node will spread more area i.e. the cell size becomes large, but throughput of the network i.e. information handling capacity will decrease. The number of hops (cells) increases in a region, then expected life of a path decreases. The transmission signal in a VANET is having interferences due to multipath fading, different type of noises, power supply fluctuation and out of cover range (mobility) etc. All vehicles (nodes) in a cell can be assigned station code or ID like Internet Protocol (IP) address and the packets (data) are routed to the node ID address. This station code is liable to change very frequently as the vehicles are going inside or leaving outside a cell in rapid manner, so in a node ID address, cell number or cell ID is also mentioned e.g. a node having ID 2C32 means, it moves in the Cell ID 2C having node number 32. Since information (voice, message, data, image etc) are routed in the cell (network), any node within or beyond the cell can monitor or tamper the information. To avoid tampering or hacking, certain authentication (security) [10] measures in the VANET communications are to be implied.

This provides a research challenge for application of Artificial Intelligence (AI) on node or vehicle authentication. We propose to use parameter of vehicle driver's (subscriber) talking habit. It means which particular range of frequency of the salutation (greeting) word, salutation word, location (place) 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 (driver or node). Fuzzy sets [9] are derived from the modified relative grades which are obtained by assigning weightage. Then fuzzy operations [9] 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, all nodes (vehicles) or nodes as well as the network (MSC or PDSN) are authenticated, otherwise not.

Therefore we propose an Artificial Intelligence based node authentication technique that will check the authenticity of a subscriber (driver or node) by fuzzy operations on fuzzy sets which are derived from talking habit of the vehicle driver especially salutation word and location of the node (ID address) at starting time of a call.

II. Proposed Artificial Intelligence Based Authentication Technique in Vehicular AD HOC Network

The proposed artificial intelligence based authentication scheme can be applied to either circuit switching or packet switching Vehicular Ad Hoc Network (VANET) 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 all nodes or a particular switch or AAA server connecting to the network. This phase is executed only once for one subscriber (node).

ASE1: The subscriber (driver) sends an application requesting to the authority concerned (VANET service provider) for new service card like SIM.

ASE2: After receiving the request, the authority asks to submit his different parameters of talking and tests his different talking habit.

ASE3: After that authority examines those tests thoroughly and performs a feasibility study of talking habit of 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, sophisticated electronics instrument is to be fitted all nodes and the server (switch) for detecting exact frequency in Hz.

(ii) Which salutation words are most frequently, more frequently and less frequently used by the subscriber (driver) while starts talking?

(iii) What are most frequently, more frequently and less frequently location i.e. place (knowing by cell ID of the subscriber) with respect to time while starting a call?

ASE4: The authority uses three databases in all nodes as well as sever for storing the above subscriber parameters based on talking habit. The first database, DF 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 DFR1 of DF, 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 DFR2 of DF, stores the more frequently used voice frequency of the salutation word and its relative grade which is assigned by 0.23. The third range DFR3 of DF, 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. DFR1, DFR2, DFR3 of DF are calculated as per following formula. Suppose DF 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]. DFR1 ranges between e = (c-d) Hz to f = (c+d) Hz. DFR2 ranges between g = (e-d) Hz to h = (e-1) Hz and i = (f+1) Hz to j = (f+d) Hz. DFR3 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, DW stores the most frequently, more frequently and less frequently used salutation words (starting time spoken) by calling subscriber and their corresponding relative grades. The first row, DWR1 of DW, stores the most frequently used salutation words and their relative grade which is assigned by 0.9. The second row, DWR2 of DW, stores the more frequently used salutation words and their relative grade which is assigned by 0.6. The third row, DWR3 of DW, stores the less frequently used salutation words and their relative grade which is assigned by 0.3.

This first and second databases can be joined together to make one table whose columns are showing different range of voice frequencies with its relative grades for the salutation words (generally divided into three groups), relative grades for the salutation words while the rows are showing the salutation words used by the subscriber.

The third database, DL stores the most probable, more probable and less probable location i.e. place known with the cell ID of the calling subscriber (vehicle) with respect to time while starting a call i.e. distance of a calling subscriber (vehicle) from another called vehicle or the network or a particular place which also can be measured by received power level and their corresponding relative grades. This database is divided into two parts, DL1 (For the time 9:00 AM to 5:59 PM) and DL2 (For the time 6:00 PM to 8:59 AM). The first row, DL1R1 of DL1, stores the most probable location of calling subscriber and their relative grade which is assigned by 0.9. The second row, DL1R2 of DL1, stores the more probable location of calling subscriber and their relative grade which is assigned by 0.6. The third row, DL1R3 of DL1, stores the less probable location of calling subscriber and their relative grade which is assigned by 0.3.

The first row, DL2R1 of DL2, stores the most probable location of calling subscriber and their relative grade which is assigned by 0.9. The second row, DL2R2 of DL2, stores the more probable location of calling subscriber and their relative grade which is assigned by 0.6. The third row, DL2R3 of DL2, stores the less probable location of calling subscriber and their relative grade which is assigned by 0.3.

Since these three 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 is considered like, DF : DW : DL = 1 : 0.66 : 0.5. We are multiplying 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 (node) is placed. Then the authority executes the above steps again to create a strong database. Also time to time authority upgrades or modifies the database for each subscriber (node).

B. Subscriber Authentication Phase

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

ASA1: Finds the matched frequency of the salutation word within the rows DFR1, DFR2, DFR3 of DF.

ASA1.1: After hearing the first speech from a calling subscriber (node), either called node or server computes frequency of the salutation word in Hz, then match the voice frequency within the stored range of DF 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,

$\mu F1\ (a1) = v1$,

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

ASA2: Finds the matched salutation or greeting word within the rows DWR1, DWR2, DWR3 of DW.

ASA2.1: If the salutation word is matched within the stores value of DWR1, DWR2, DWR3, 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 w1m, where w1m = (w1) X 0.66,

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

$\mu F2\ (a2) = w1m$

Hence, $F2 = \{(a2, w1m)\}$

ASA3: Called node or Server watches the time and selects the database for location of the calling node (DL1 or DL2) at the starting time of a call. Finds the matched location within the rows DL1R1, DL1R2, DL1R3 for DL1 or DL2R1, DL2R2, DL2R3 for DL2 depending on call initializing or starting time.

ASA3.1: If the location of the calling node 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 p1m, where p1m = (p1) X 0.5,

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

$\mu F3\ (a3) = p1m$

Hence, $F3 = \{(a3, p1m)\}$

ASA4: Computes fuzzy operations,

ASA4.1: $\mu F1 \cap F2 \cap F3\ (a) = \min \{\mu F1\ (a1), \mu F2\ (a2), \mu F3\ (a3)\}$

ASA4.2: $\mu F1 \cup F2 \cup F3\ (a) = \max \{\mu F1\ (a1), \mu F2\ (a2), \mu F3\ (a3)\}$

ASA5: For ascertaining the calling node with the called node or the network (MSC or PDSN) authenticity, an invented Fuzzy Rule (condition) on result of the fuzzy operations has been implied.

If $\mu F1 \cap F2 \cap F3\ (a) \geq 0.15$ and $\mu F1 \cup F2 \cup F3\ (a) \geq 0.45$ satisfies, then only the called node or the server ensures that the calling node (subscriber) is authentic, hence their mutual authenticity is verified. The called node or the server checks or computes the authentication process. Since primary databases are kept at the all nodes or server (switch), if that stored values in respect of the parameters of the node at the other nodes or the server are not matched with that of the calling node as currently transmitted, further processing will be stopped which identifies that the nodes or the network are unauthentic. Finally if the above two fuzzy conditions are not satisfied, the called node or the server ensures that the calling node (vehicle driver) is unauthentic. In both the cases the called node or the server sends an authentication failure message to the calling node in this VANET.

III. Results And Discussion

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

Example1: A vehicle driver (calling subscriber) having ID-1C15 (Cell ID-1C, Node number-15) in a VANET starts talking with "Namaskar" in 2325 Hz on 10:24 AM at Cell-1C with another node having ID-1C32, examine authenticity of the nodes.

After testing voice frequency of the driver's salutation word "Namaskar" stored in the called node ID-1C32, the range of voice frequency of the driver's particular salutation word "Namaskar" is found from 2235 Hz to 2726 Hz.

If the voice frequency of the calling subscriber's salutation word "Namaskar" is within 2398 Hz to 2562 Hz then the value DFR1 of DF is 0.65.

If the voice frequency of the calling subscriber's (driver's or node's) salutation word "Namaskar" is within 2316 Hz to 2397 Hz and 2563 Hz to 2645 Hz, the value DFR2 of DF is 0.23.

If the voice frequency of the calling subscriber's salutation word "Namaskar" is within 2235 Hz to 2315 Hz and 2646 Hz to 2726 Hz, the value DFR3 of DF is 0.12.

So, the voice frequency of the calling driver 2325 Hz in DFR2 of DF.

The salutation or greeting words are stored in the called subscriber (node) for the calling subscriber (driver) in DWR1 of DW like,

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

The salutation words are stored in the called subscriber (node) for the calling subscriber in DWR2 of DW like,

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

The salutation words are stored in the called node for the calling subscriber (node) in DWR3 of DW like,

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

Let the relative grade of DWR1 is 0.9, DWR2 is 0.6 and DWR3 is 0.3.

For salutation word "Namaskar" of the calling node (subscriber), it is in DWR3 whose relative grade (w1) is 0.3

For the time period 9:00 AM. to 5:59 PM,

If location of the calling subscriber (driver or node) is in

cell-1A, 1D, 2A, 3B, 4C, the value of DL1R1 of DL1 is 0.9.

If location of the calling node is in cell-1B, 2C, 3A, 4B, 4D, then the value of DL1R2 of DL1 is 0.6.

If location of the calling node is in Cell-1C, 1E, 2B, 3C, 4A or Elsewhere, then the value of DL1R3 of DL1 is 0.3.

For the time period 6:00 PM. to 9:00 AM,

If location of the calling node is in Cell-1B, 2A, 2C, 3D, 4B, then the value of DL2R1 of DL2 is 0.9.

If location of the calling node is in Cell-1A, 2B, 3A, 3B, 4A,

then the value of DL2R2 of DL2 is 0.6.

If location of the calling node is in Cell-1C, 2D, 3C, 4C, 4D or Elsewhere, then the value of DL2R3 of DL2 is 0.3.

The calling subscriber (node) on 10:24 AM at Cell-1C in DL1R3 whose relative grade (p1) is 0.3,

Hence, the matched frequency of the salutation word (2325 Hz) from the calling subscriber in DFR2.

Therefore, v1= 0.23

$\mu F1\ (a1) = v1 = 0.23$,

Hence, $F1 = \{(a1, 0.23)\}$

The matched the salutation (greeting) word of the calling subscriber in DWR3.

Therefore, w1= 0.3, w1m = w1 X 0.66 = 0.3 X 0.66 = 0.20

$\mu F1\ (a2) = w1m = 0.20$,

Hence, $F2 = \{(a2, 0.20)\}$

The matched the location of the calling node (ID-1C15) in DL1R3.

Therefore, $p1=0.3$, $p1m = p1 \times 0.5 = 0.3 \times 0.5 = 0.15$

$\mu F1 (a3) = p1m = 0.15$,

Hence, $F3 = \{(a3, 0.15)\}$

Now, $\mu F1 \cap F2 \cap F3 (a) = \min \{0.23, 0.20, 0.15\} = 0.15$;

$\mu F1 \cup F2 \cup F3 (a) = \max \{0.23, 0.20, 0.15\} = 0.23$

As fuzzy rule set $\mu F1 \cap F2 \cap F3 (a) \geq 0.15$ and

$\mu F1 \cup F2 \cup F3 (a) \geq 0.45$ is not true, so the called node (or the server) ensures that the calling subscriber (node) is not authentic, hence they are not mutual authenticated followed by authentication failure message.

Example2. The node with ID-2B21 (same subscriber as in Ex1 in Cell-2B, node number-21) starts talking with "Good Morning" in 1915 Hz on 7.36 AM with the called node ID-2B05, examine mutual authenticity of the nodes.

After testing voice frequency of the calling node's (driver's) salutation word "Good Morning" from the called node, the range of voice frequency of the calling node's particular salutation word "Good Morning" is found from 1734 Hz to 2256 Hz.

If the voice frequency of the calling node's salutation word "Good Morning" is within 1908 Hz to 2082 Hz then the value DFR1 of DF is 0.65.

If the voice frequency of the calling node's salutation word "Good Morning" is within 1821 Hz to 1907 Hz and 2083 Hz to 2169 Hz, the value DFR2 of DF is 0.23.

If the voice frequency of the calling node's salutation word "Good Morning" is within 1734 Hz to 1820 Hz and 2170 Hz to 2256 Hz, the value DFR3 of DF is 0.12.

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

Hence, the matched frequency of the salutation word (1915 Hz) from the calling subscriber in DFR1

Therefore, $v1= 0.65$

$\mu F1 (a1) = v1 = 0.65$,

Hence, $F1 = \{(a1, 0.65)\}$

The matched the salutation (greeting) word of the calling subscriber in DWR2.

Therefore, $w1= 0.6$, $w1m = w1 \times 0.66 = 0.6 \times 0.66 = 0.40$,

$\mu F1 (a2) = w1m = 0.40$,

Hence, $F2 = \{(a2, 0.40)\}$

The matched the location of the calling subscriber in DL2R2.

Therefore, $p1=0.6$, $p1m = 0.6 \times 0.5 = 0.30$,

$\mu F1 (a3) = p1m = 0.30$,

Hence, $F3 = \{(a3, 0.30)\}$

Now, $\mu F1 \cap F2 \cap F3 (a) = \min \{0.65, 0.40, 0.30\} =0.30$;

$\mu F1 \cup F2 \cup F3 (a) = \max \{0.65, 0.40, 0.30\} = 0.65$

As fuzzy rule set as, $\mu F1 \cap F2 \cap F3 (a) \geq 0.15$ and

$\mu F1 \cup F2 \cup F3 (a) \geq 0.45$ is true i.e. the fuzzy rule satisfies results of the fuzzy operations, so the called subscriber (node) ensures that the calling subscriber (node) is authentic, hence they are mutual authenticated.

IV. 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 calling subscriber (vehicle driver or node) while making a call. The characteristics of this authentication scheme are,

(i) This mobile vehicles (nodes) as well as network authentication technique enjoys the advantages of artificial intelligence and fuzzy theory, so it is a unique one.

(ii) Artificial intelligence is efficiently employed to the nodes or the server and subsequently it takes part to authenticate correct nodes with the network.

(iii) Authenticity is decided by the calling subscriber's (driver's) talking characteristics (habit) and distance of the calling subscriber (vehicle or node) from the other i.e. called node or base station or particular place in a cell etc.

(iv) No cryptography algorithm or any complex functions are applied for this authentication purpose.

(v) Flexible simple fuzzy operations are performed on fuzzy set for this authentication decision.

(vi) This authentication technique specifies result with in a real time basis.

V. Conclusion

In this proposed artificial intelligence based technique, the nodes (calling and called) or a node as well as the network (switch or server) mutual authentication technique is developed in a real time basis. A novel artificial intelligence is introduced to all nodes or the server for this in Vehicular Ad Hoc Network (VANET) communications.

References

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

[2] A. S. Tannenbaum, Computer Networks, 4th Edition, Pearson Education, 2007.

[3] P. K. Bhattacharjee, "A New Era in Mobile Communications- GSM and CDMA" in National Conference on Wireless and Optical Communications (WOC-07) at Punjab Engineering College (D.U), India, pp 118- 126, on 13th- 14th Dec, 2007.

[4] T. S. Rappaport, Wireless Communication: Principles and Practice, Prentice Hall Pub Ltd, 2nd Ed, 2006.

[5] H. Alshear and E. Horlait, "An optimized Adaptive Broadcast Scheme for Inter-Vehicle Communications", IEEE Vehicular Technology Conference, Stockholm, Sweden, May 2005.

[6] M. Torrent-Moreno, D. Jiang and H. Hartenstein, "Broadcast Reception Rates and Effects of Priority Access in 802.11-Based Vehicular Ad-Hoc Networks", Proceedings of the 1st International Workshop on Vehicular Ad Hoc Networks, ACM, pp 10-18, Philadelphia, PA, USA, October 2004.

[7] J. Blun, A. Eskandarian and L. Hoffman, "Challenges of Intervehicle Ad Hoc Networks", IEEE Transactions of Intelligent Transportation Systems, Vol. 5, No. 4, December 2004.

[8] Q. Xu, T. Mak and R. Sengupta, "Vehicle-to-Vehicle Safety Messaging in DSRC", in Proc ACM VANET, Philadelphia, October 2004.

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

[10] 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, August, 2009.

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 & IAENG, Hongkong. His research interests are in Mobile Communications, Network Security, Nanotechnology, VLSI etc.

Dr. Utpal Roy did his graduation and post graduation from Visva-Bharati University, Santiniketan, India. Subsequently he did Ph.D. from Visva-Bharati. In 1994 he joined the Department de physique, Uiversite Laval, Quebec Canada as a Post Doctoral Fellow. In 1996 he joined Indian Association for the Cultivation of Science as a Senior Research Associate (CSIR). Thereafter he joined Visva-Bharati University as a Lecturer in Computer Science in 1997. He spent more than a year as a Visiting Fellow in the Academia Sinica, Taipei, Taiwan. Formerly he worked as a professor in Information Technology at Assam University, Silchar. Now he is an Associated Professor in the Department of Computer & System Sciences, Visva-Bharati University, India. His research area is in Mobile Communications, Network Security, Image Processing, Computer Software etc.

Dr Anup Kumar Bhattacharjee received his BE in Electronics and Telecommunication Engineering from BE College Shibpur, Howrah in 1983. He received his ME TelE and Ph.D. from Jadavpur University, Kolkata in 1985 and 1989 respectively. Presently he is attached with Electronics and Communication Engineering Department, in National Insititute of Technology, Durgapur, West Bengal, India as a Professor. His area of research is in Microstrip Antenna, Embedded System, Mobile Communications etc.