Identification, Authentication and Tracking Algorithm for Vehicles Using VIN in Centralized VANET

Atanu Mondal[1] and Sulata Mitra[2]

[1] Department of Computer Science & Engineering,
Camellia Institute of Technology, Kolkata, India
atanumondal@hotmail.com
[2] Department of Computer Science and Technology,
Bengal Engineering and Science University, Shibpur, India
sulata@cs.becs.ac.in

Abstract. The VANET should allow only the authentic vehicles to participate in the system for efficient utilization of its available resources. The proposed system architecture contains multiple base stations in the coverage area of a certifying authority. The base station verifies the identification of the vehicle and the certifying authority verifies the authentication of the vehicle using its vehicle identification number. The certifying authority also generates a digital signature for each authentic vehicle and assigns it to the corresponding vehicle through base station. The base station allocates a channel to each authentic vehicle. The channel remains busy as long as the vehicle is within the coverage area of this base station. So the base station is able to track an authentic vehicle by sensing the allocated channel within its coverage area.

Keywords: VANET, Authentication, VIN, Dedicated Short Range Communication.

1 Introduction

The unique identification of a vehicle at a very fast speed using vehicle tracking system helps to track it at various check points within a boundary or premises. It manages the security of vehicles in case of theft or any unwanted incident. Along with identification and tracking it is also required to protect the communication in a secured VANET system from unauthorized message injection and message alteration.

Several identification, tracking and authentication schemes have been proposed so far. The automatic vehicle identification techniques are discussed in [1]. One such technique uses barcode which is affixed to each vehicle. The optical reader may be used to read it. But its quality is affected by weather. Most current automatic vehicle identification technology relies on radio frequency identification in which an antenna is used to communicate with a transponder on the vehicle using DSRC. It has excellent accuracy even at highway speed. But the major disadvantage is the cost of transponder. The close circuit television technology [2] may be used in vehicle tracking system. But the image quality is affected by the lighting or the presence of trees. The global positioning system (GPS) may be used to know the current position of a vehicle [3].

V.V. Das and J. Stephen (Eds.): CNC 2012, LNICST 108, pp. 115–120, 2012.

But it cannot distinguish one vehicle from another. Moreover satellite communication is required to process data which is obtained from GPS. But satellite communication is not adequate at urban and forest area. Any storms having ionized particle may introduce noise in the collected information. In [4], each vehicle has a unique identity along with a public and private key. The public key is used to encrypt the unique identity before sending it to the receiver and the public key is used to decrypt any received message. But the pattern of the unique identity is not mentioned in this scheme. Moreover it needs considerable amount of time for encryption. The biometric information of the driver is used for authentication in [5]. It hampers the privacy of the driver. Moreover it is applicable if the driver in the vehicle is a fixed person. In [6], CA assigns a public key to each vehicle for V2V and V2I communication. The vehicle uses the public key for encryption. CA generates a signature from the said public key and assigns it to the vehicle in case the vehicle wants to get any service from the network. But any intruder may get the public key of a vehicle and may start some communication.

The proposed VANET is a hierarchy having certifying authority (CA) at the root level, base stations (BSs) at the intermediate level and vehicles at the leaf level. The dedicated short range communication (DSRC) protocol [7] is proposed for short distance V2I communication among vehicles and CA through BS in the form of data. The range of frequency provided by DSRC is 5.850 – 5.925 GHz. So the available bandwidth at each BS is 75MHz, out of which 70 MHz is usable and rest 5 MHz is used as guard frequency [8]. The 70 MHz bandwidth at each BS is divided into 7 links, out of which 6 links are reserved for service and 1 link is used for control purposes. So the bandwidth of each link is 10 MHz and it is allocated to authentic vehicle on demand at a rate 1.28 MHz. So each 10 MHz link is divided into (10 MHz / 1.28 MHz) ≈ 8 channels and so the total number of available channels to provide service at each BS is 48. Each BS allocates one channel to each authentic vehicle within its coverage area and so can provide service to 48 vehicles using 48 channels. The proposed scheme uses identification algorithm to identify a vehicle uniquely using its vehicle identification number (VIN). The authentication algorithm is used for verifying the authenticity of a vehicle during its initial registration phase. It assigns a digital signature (D_Sig) to an authentic vehicle. The tracking algorithm is used by each BS to track an authentic vehicle within its coverage area. Each BS maintains a VIN database to store the encrypted VIN and D_Sig pair of all the authentic vehicles. CA maintains a VIN database to store the available VINs. The use of VIN for identification and authentication is advantageous as it is impossible to transfer VIN among vehicles and to alter the information on it. Moreover VIN of a vehicle remains intact even in typical environmental condition. It contains information about the manufacturer of the vehicle and description of the vehicle. So other than identification and authentication VIN can also be used to know the manufacturing details and the details description of a vehicle which may require in case of accidents etc.

2 Present Work

In this section a modified VIN structure is proposed. The identification algorithm and authentication algorithm of v^{th} vehicle (V_v) are elaborated. The tracking algorithm for V_v is also considered for discussion.

2.1 Modified VIN Structure

VIN has 17 characters which are divided into 3 fields [9]. There are four competing standards to represent VIN worldwide [9]. The first standard (S1) is FMVSS 115, Part 565, the second standard (S2) is ISO 3779, the third standard (S3) is SAEJ853 and the fourth standard (S4) is ADR 61/2. The WMI field contains 3 characters for all the 4 standards, VDS field contains 6 characters for S2, S3, and S4 whereas 5 characters for S1. The VIS field contains 8 characters for all the 4 standards. In S1 the 9th character is used to detect error in VIN which may occur during its communication through unreliable channel. In S2, S3, S4 out of 6 characters in VDS field 5 characters are used as VDS and the 6th character which is actually the 9th character of VIN remains unused [9].

The above VIN structure is modified in the proposed scheme. The WMI field has 4 characters, VDS field has 5 characters and VIS field has 8 characters in the modified VIN. The valid range of each character in all the 3 fields is discussed in [10]. Now currently available number of manufacturers is 836 and number of countries is 78 [11]. So it is required to identify 65,208 numbers of manufacturers in case all the countries have 836 numbers of manufacturers. It is possible to identify only 35,035 numbers of manufacturers using 3 characters in WMI field. The use of 4 characters in WMI field helps to identify 11,55,517 number of manufacturers. The extra 10,90,309 number of manufacturers may be utilized to satisfy any future requirement. The VIN database at CA stores the currently available VINs. It is updated whenever a new vehicle is manufactured. The possibility of error in the proposed fast short distance V2I communication is assumed as negligible. So an extra character for error detection like S1 is not required in the modified VIN. However the 9th character which is the error detection character in S1 and unused character in S2, S3, S4 is incorporated in WMI field of the modified VIN structure to identify more manufacturers.

2.2 Identification, Authentication and Tracking Algorithm

Let V_v ($1 \leq v \leq V$) enters into the coverage area of Bth BS (BS_B, $1 \leq B \leq S$), where V is the total number of vehicles and S is the total number of BSs in the proposed VANET environment. In the proposed scheme it is assumed that each vehicle has an electronic license plate (ELP) in which the encrypted VIN of the vehicle is embedded by the vehicle manufacturer. The ELP of a vehicle broadcasts (as per IEEE P1069 and IEEE 802.11p) the encrypted VIN after entering into the coverage area of a new BS. So the ELP of V_v (ELP_v) broadcasts the encrypted VIN (E_VIN_v). The identification algorithm at BS_B receives E_VIN_v from V_v and searches its VIN database ($BS_B\_VIN\_DATABASE$) for E_VIN_v using BS_VIN_SEARCH algorithm Fig 1. If found V_v is an authentic vehicle. So its initial registration phase is already over. The identification algorithm at BS_B reads D_Sig of V_v (D_Sig_V) from $BS_B\_VIN\_DATABASE$ and triggers the tracking algorithm by sending D_Sig_v to it. Otherwise the identification algorithm at BS_B starts the initial registration phase of V_v by triggering authentication algorithm.

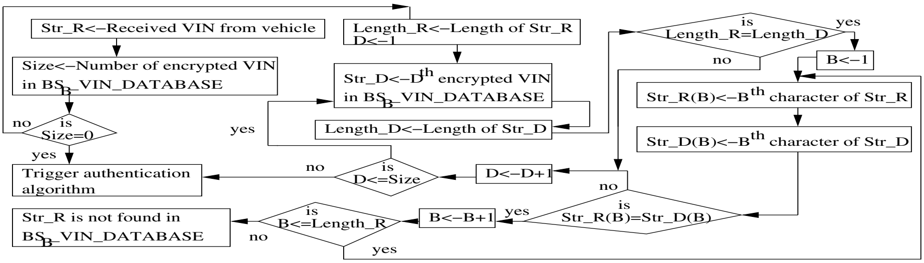
Str_R<–Received VIN from vehicle
Size<–Number of encrypted VIN in BS_B_VIN_DATABASE
is Size=0
no
yes
Trigger authentication algorithm
Str_R is not found in BS_B_VIN_DATABASE
Length_R<–Length of Str_R D<–1
Str_D<–D^th encrypted VIN in BS_B_VIN_DATABASE
Length_D<–Length of Str_D
yes
no
is D<=Size
D<–D+1
is B<=Length_R
no
B<–B+1
yes
yes
is Length_R=Length_D
yes
no
B<–1
Str_R(B)<–B^th character of Str_R
Str_D(B)<–B^th character of Str_D
no
is Str_R(B)=Str_D(B)

Fig. 1. Flow chart of BS_VIN_SEARCH Algorithm

The authentication algorithm at BS$_B$ adds E_VIN$_v$ in its VIN queue (BS$_B$_VIN_Queue) and calls the verification function at CA by sending E_VIN$_v$ to it. The verification function at CA adds E_VIN$_v$ in its VIN queue (CA_VIN_Queue) and decrypts E_VIN$_v$ to generate D_VIN$_v$ using RSA algorithm. It verifies each character in the 3 fields of D_VIN$_v$ for its validity [10]. If D_VIN$_v$ is not valid the verification function at CA generates a security message for the police or checking personnel to make them aware about V$_v$. Otherwise it generates a unique D_Sig (D_Sig$_v$) from D_VIN$_v$ using SHA-1 algorithm. It constructs B$_v$ which contains (E_VIN$_v$,D_Sig$_v$) pair and calls the insertion function at all the BSs under the coverage area of CA by sending B$_v$ to them. The insertion functions at all the BSs under CA insert (E_VIN$_v$, D_Sig$_v$) pair in their VIN database. During this span of time V$_v$ may reside within the coverage area of BS$_B$ or may move to the coverage area of another BS. The insertion function at the BS within which the vehicle is currently passing through (Current_BS$_v$) triggers the tracking algorithm. The tracking algorithm at BS assigns D_Sig$_v$ to V$_v$ and allocates a channel (CH$_v$) to V$_v$. It also switches on a timer $\tau_{v.}$ The timer$\tau_v$indicates the time span during which D_Sig$_v$ is assigned to V$_v$. It senses CH$_v$ when $\tau_v$expires.If CH$_v$ is free, the tracking algorithm removes $\tau_v$and frees CH$_v$. Otherwise reassigns D_Sig$_v$ to V$_v$ and switches on τ_v again.

3 Simulation

In this section the simulation parameters and the simulation results are considered for discussion. The coverage area of CA (Area_CA) is assumed as1000 meter to support DSRC and the coverage area of BS (Area_BS) is assumed as 300 meter during simulation. So the maximum distance from BS to CA (Dist_BS_CA) is 300 meter and from vehicle to BS (Dist_V_BS) is300 meter. The maximum number of BSs (S) is the ratio of Area_CA to Area_BS and the maximum number of vehicles (V) is 48S. The data transmission time among various components in the proposed VANET is the ratio of the distance between source and destination to data transmission rate. The data transmission rate (Data_TR) is assumed as 6 Mb/s [12].

The size of E_VIN$_v$ (Size_E_VIN$_v$) is 17N bits where N = $\log_2[\ 2^{\max(P,\ Q)} - 1]$. P and Q are the prime numbers used in RSA algorithm. K$_p$ and K$_s$ are the public and private key respectively used in RSA algorithm. Fig.2 shows the plot of the transmission time of E_VIN$_v$ from V$_v$ to BS$_B$ (TT_VBS_E_VIN$_v$) vs. Size_E_VIN$_v$.

TT_VBS_E_VIN$_v$ is computed as (Dist_V_BS * Size_E_VIN$_v$)/Data_TR. TT_VBS_E_VIN$_v$ is almost negligible up to Size_E_VIN$_v$ equal to 33554432 bits, after this it increases linearly with Size_E_VIN$_v$. The searching time of BS$_B$_VIN_DATABASE for E_VIN$_v$ (ST_BSB_E_VIN$_v$) depends upon Size_E_VIN$_v$ and size of BS$_B$_VIN_DATABASE. As BS$_B$_VIN_DATABASE stores the encrypted VIN of all the authentic vehicles so it's maximum size depends upon the number of authentic vehicles in the proposed VANET environment and it is 48S. So ST_BSB_E_VIN$_v$ is proportional to Size_E_VIN$_v$ for the maximum size of BS$_B$_VIN_DATABASE. The waiting time of E_VIN$_v$ at BS$_B$_VIN_Queue (WT_BSB_E_VIN$_v$) is$\sum_{i=1}^{J}(\text{ST_BSB_}E_VIN_i)$, where ST_BSB_E_VIN$_i$ is the searching time of BS$_B$_VIN_DATABASE for E_VIN$_i$ of ith vehicle and J is the number of encrypted VIN waiting in BS$_B$_VIN_Queue in front of E_VIN$_v$. As each BS can provide service to 48 vehicles so the maximum possible length of BS$_B$_VIN_Queue is 48 and the maximum value of J is 48. Fig.3 shows the plot of the transmission time of E_VIN$_v$ from BS$_B$ to CA (TT_BSCA_E_VIN$_v$) vs. Size_E_VIN$_v$. TT_BSCA_E_VIN$_v$ is computed as (DIST_BS_CA*Size_E_VIN$_v$) /Data_TR. TT_BSCA_E_VIN$_v$ is almost negligible up to Size_E_VIN$_v$ equal to 33554432 bits after this it increases linearly with Size_E_VIN$_v$.

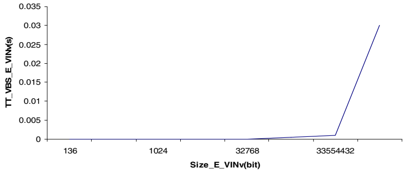

Fig. 2. TT_VBS_E_VINv vs. Size_E_VIN$_v$

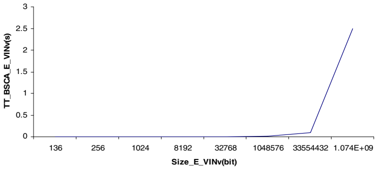

Fig. 3. TT_BSCA_E_VIN$_v$ vs. Size_E_VIN$_v$

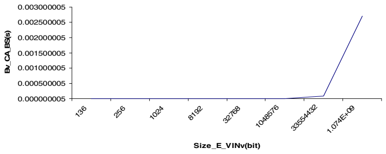

Fig. 4. Bv_CA_BS vs. Size_E_VIN$_v$

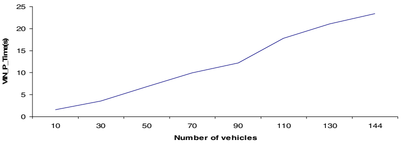

Fig. 5. VIN_P_Time vs. number of vehicles

The time to check D_VIN$_v$ for its validity (VT_CA_D_VIN$_v$) depends upon the size of D_VIN$_v$. The decryption time of E_VIN$_v$ (D_Time) depends upon the size of K$_s$ in RSA algorithm [13]. As D_Sig is generated using SHA-1 algorithm [13] so the D_Sig_Time is constant and it is 15 msec which has been observed during simulation. The waiting time of E_VIN$_v$ at CA_VIN_Queue (WT_CA_E_VIN$_v$) is$\sum_{i=1}^{\mathrm{T}}(\text{WT_CA_}E_VIN_i)$, where WT_CA_E_VIN$_i$ is the waiting time of E_VIN$_i$ at CA_VIN_Queue and T is the number of encrypted VIN waiting in CA_VIN_Queue in front of E_VIN$_v$. WT_CA_E_VIN$_i$ is the sum of D_Time, VT_CA_D_VIN$_i$ and D_Sig_Time. The maximum size of CA_VIN_Queue depends upon the number of vehicles in the proposed VANET environment and it is 48S. Fig.4 shows the plot of the time required to broadcast B_v by CA (B_v_CA_BS) vs. Size_E_VIN$_v$. B_v_CA_BS is computed as (Dist_BS_CA*Size_B_v)/Data_TR. The size of D_Sig (Size_D_Sig) is 160 bits. The size of B_v (Size_B_v)is (Size_E_VIN$_v$+Size_D_Sig) bits. The time required to assign D_Sig$_v$ to V_v by Current_BS$_v$ (V_BS_D_Sig$_v$) is (Dist_V_BS*Size_D_Sig)/Data_TR. B_v_CA_BS is almost negligible up to Size_E_VIN$_v$ equal to 33554432 bits, after this it increases linearly with Size_E_VIN$_v$.Fig.5 shows the plot of VIN processing time (VIN_P_Time) vs. number of vehicles. VIN_P_Time is the sum of TT_VBS_E_VIN$_v$, ST_BSB_E_VIN$_v$, WT_BSB_E_VIN$_v$, TT_BSCA_E_VIN$_v$, VT_CA_D_VIN$_v$, WT_CA_E_VIN$_v$, D_Time, D_Sig_Time, B_v_CA_BS and V_BS_D_Sig$_v$. VIN_P_Time increases slowly up to the number of vehicles equal to 80. After this the increase in the number of vehicles increases the length of queue at BS and CA which in turn increases VIN_P_Time at a rapid rate.

4 Conclusion

The present work is an identification and authentication mechanism of vehicles in a centralized VANET environment. It uses VIN of a vehicle for its identification and authentication. The performance of the proposed algorithms may be studied in a distributed VANET environment. Moreover in this work we concentrate on V2I communication only. It can be extended to V2V communication.

References

1. http://ec.europa.eu/transport/roadsafety_library/publications/evi_executive_summary.pdf
2. Parliamentary Office of Science and Technology. Postnote 175 (2002)
3. Balon, G.N.: Vehicular Ad-hoc Networks and Dedicated Short Range. University of Michigan, Dearborn (2006)
4. Papadimitratos, P., Gligor, V., Hubaux, J.P.: Securing Vehicular Communications - Assumptions, Requirements, and Principles. ESCAR (2006).
5. Raya, M., Padimitratos, P., Hubaux, J.P.: Secure Vehicular Communications, EPFL. IEEE Wireless Communications (2006)
6. Calandriello, G., Padimitrators, P., Hubaux, J.P., Lioy, A.: Efficient and Robust Pseudonymous Authentication in VANET. In: ACM VANET 2007 (2007)
7. Persad, K., Walton, C.M., Hussain, S.: Electronic Vehicle Identification: Industry Standards, Performance. Project 0-5217, Texas Department of Transportation (August 2006)
8. Zang, Y., Stibor, L., Walke, B., Reumerman, H.J., Barroso, A.: Towards Broadband Vehicular Ad-Hoc Networks-The Vehicular Mesh Network (VMESH) MAC Protocol. IEEE Communication Society (2007)
9. Scully, J., Fildes, B., Logan, D.: Use of Vehicle Identification Number for Safety Research. Monash University Accident Research Centre, Melbourne, Australia (2005)
10. http://www.angelfire.com/ca/TORONTO/VIN/VIS.html
11. http://en.wikipedia.org/wiki/List_of_cars
12. Towards Effective Vehicle Identification, The NMVTRC's Strategic Framework for Improving the Identification of Vehicles and Components (2004)
13. Kahate, A.: Cryptography and Network Security, 2nd edn. TMH (2010)