I. J. Computer Network and Information Security, 2013, 8, 55-61
Published Online June 2013 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2013.08.07

Establishing Inter Vehicle Wireless Communication in Vanet and Preventing It from Hackers

M. Milton Joe[1], R.S. Shaji[2], K. Ashok Kumar[3]
[1]Assistant Professor, Department of Computer Application, St. Jerome's College of Arts and Science, Nagercoil, Tamilnadu, India.
[2] Professor, Department of IT, Noorul Islam University, Nagercoil, Tamilnadu, India.
[3]Assistant Professor, Department of Computer Application, MAHER – FHS, Meenakshi University,Chikkarayapuram, Chennai – 69, Tamilnadu, India.
m.miltonjoe@gmail.com, shajiswaram@yahoo.com, jas_indians@yahoo.co.in

Abstract — The entire humanity needs a vehicle to travel from one place to another. Obviously a new model vehicle is manufactured by the manufacturing companies to attract its customers every day. All the manufactured vehicles have different advantages, when compared with one another. In this case, we introduce another added advantage to the vehicle is establishing inter vehicle wireless communication in VANET and preventing it from the hackers. This type of inter vehicle wireless communication among vehicles that are moving faster on the road will lead safety and increase Quality of Service (QoS) to the passengers. The proposed wireless inter vehicle communication will allow vehicles to inter change messages from one vehicle to another vehicle with the help of network communication and prevents the communication from the hackers.

Index Terms — Network, Security, Communication, Bluetooth, VANET, Quality of Service (QoS)

I. INTRODUCTION

Making two or more devices (nodes) communicating with on another is called network communication. Similarly forming two or more vehicles to communicate with one another is known as VANET. This VANET communication can be formed by the wireless technologies. Establishing communication between vehicles is to bring out or increase the safety of the passengers along with vehicle. On the road side we could find some of the helping units called Road Side Unit, which passes some sort of information to the vehicles. However, this sort of helping units are not that much helpful to the vehicles, while they move faster on the road side. So in this paper we introduce a new way of communication among vehicles for better communication for the safety of the passengers. This wireless communication will also increase the quality of service among the vehicles, when they were able to interchange messages with one another.

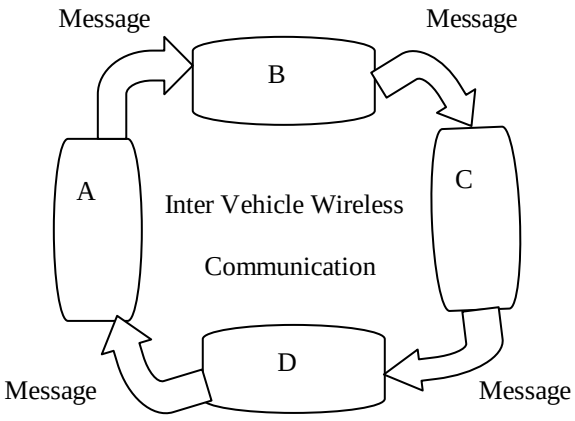

Figure 1: Inter Vehicle Communication

The above Figure 1 shows the simple model of how inter vehicle wireless communication can be formed and message is transferred among them. As shown in the figure, when communication is established among vehicles that help a lot to communicate with one another at the emergency situations, such as no fuel, break down and even vehicle is hijacked by the hijackers. So it is fair to model a network communication in VANET to bring out the safety of the passengers, who are all travel in it. In this paper we model a network communication among vehicles using

Bluetooth technology and also we propose a vital scheme to prevent our modeling network communication from the Bluetooth hackers.

II. RELATED WORK

VANET can be formed with vehicles that move on the roads. The VANET is similar to MANET [6], where the nodes in MANET can move at random and in VANET the nodes (Vehicles) can be only on the road [6]. VANET needs protocol to pass the message from one vehicle to another vehicle; however the same protocol which is used in MANET can also be utilized in VANET [7]. The previous works carried out in VANET by the researches concentrated how to improve the communication between the vehicles and the road side unit and also clustering based communication between vehicles. These road side units will give the information to the vehicles about the nearest petrol bank, motels, atm centers and the direction of the road status. However these road side units on the road will just give some sort of information to the vehicles but it will be good if we could make the vehicles to communicate with one another on the road always. Thus this paper proposes a new methodology to establish a network communication using Bluetooth technology and preventing the network communication from the Bluetooth hackers. Prevention of any network modeling communication from the hackers is really a challenge to the researchers. The Bluetooth device can be hacked easily compare with other communication devices. However we bring out the new schemes to prevent our network communication safer and prevent it from the hackers. The proposed scheme will retain all the security constraints to prevent it from the hackers and to improve the quality of service always. The proposed methodology could be evaluated with the performance of inter vehicle wireless communication.

III. ARCHITECTURE

The figure 2 describes the entire model of our proposed system. In our architecture, we form network communication with vehicles and allow the vehicles to pass message and communicate with one another. Network communication can be modeled as shown in our architecture with the help of Bluetooth technology. Since our architecture works with Bluetooth technology, it is possible for the Bluetooth hackers to hack the vehicle and pass the message to the vehicles without the intervention of the passengers of the vehicle. Every communication must be prevented from the hackers to provide secure communication. In the proposed architecture, we model network communication among vehicles and prevent the communication network from the hackers. As our network communication model works with the Bluetooth technology, it is compulsory for all the vehicles manufactured with the Bluetooth device in it. Bluetooth device of each vehicle must be switched on to communicate with other vehicles, while moving on the road.

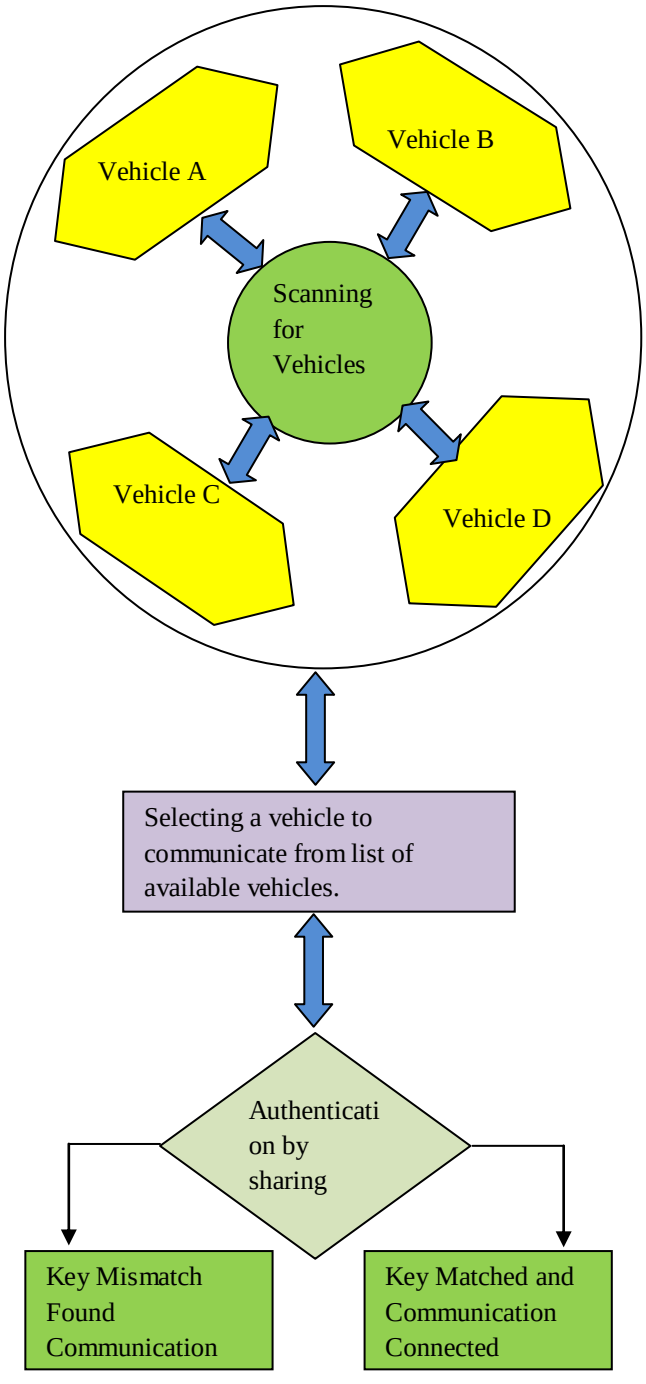

Figure 2: Inter Vehicle Communication & Preventing it from Hackers.

A. Communication Model

Every communication must be securable and should be prevented from the hackers. In our architecture model as shown in the figure 2, we establish the network communication only after successfully authenticating the vehicle. It would be easy for the hackers to hack the vehicle, if we allow the vehicles to communicate with one another without authentication. In order to provide high security to our communication, we allow the network communication only if the vehicles are authenticated successfully. As elaborated in the figure 2, the vehicle wishes to establish a network communication with other vehicle, searches for the available vehicles. Once the vehicles are searched successfully the vehicle selects a vehicle for communication. The communication request is sent to the selected vehicle for approval. If the vehicle is approved and authenticated successfully, the communication will be established between vehicles to pass the message between each other. If the vehicle is not authenticated successfully the communication will be disconnected immediately. This type of authenticated communication will prevent the network communication from the hacker. As we know, the network communication established between vehicles is to pass message and extend some sort of help from the other vehicles during the emergency cases. If communication is allowed without proper authentication, it will be an advantage to the hackers to hack the device and pass wrong information to the vehicle, which will divert the control of the vehicle and lead to major accidents even. The ultimate aim of our architecture is to model a network communication and prevent our communication from the Bluetooth hackers.

IV. PREVENTING FROM HACKERS

A. Master and Slave Key Sharing

Establishment of secure communication and preventing the communication from the hackers our architecture uses sharing of master key and slave key between the vehicles. When a vehicle wants to communicate with another vehicle (Master), it should send the connection request to the particular vehicle. Once the request is received in the other vehicle (Slave), it will be asked to share a master key, if the vehicle is willing to accept the communication request. This key sharing is known as master key sharing. After entering the master key the response will be sent back to the communication requested vehicle (Slave) and the entered master key is displayed on the screen of the vehicle. This same master key should be entered by the communication requested (Slave) vehicle. This key sharing type is called slave key sharing. Master key and the slave key are checked and if both values are matched (Same values) the communication will be established, otherwise the communication will not be established.

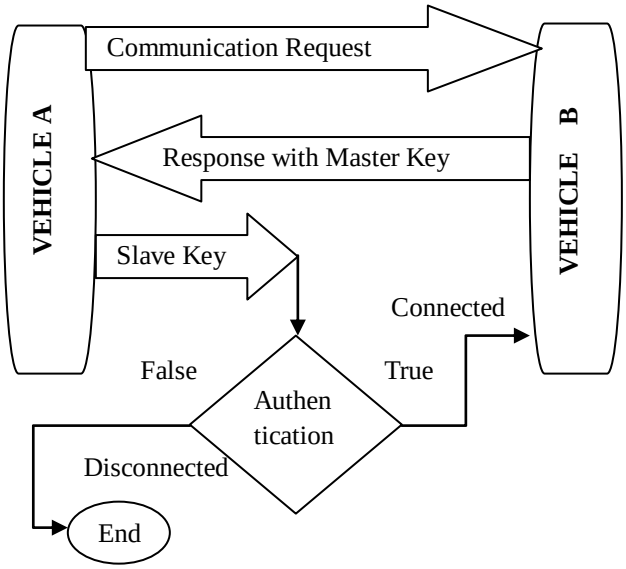

Figure 3: Communication by Sharing Maste Key and Slave Key

The above figure 3 shows, how inter vehicle wireless communication is established between vehicles by sharing master and slave keys. The master and slave keys are set of values within the numeric values from 0 to 9 as shown below.

$$M_i = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$$
$$S_{i=} \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$$

The Master Key M_i can be any combination of values from the set and similarly the Slave key S_i should be the same value of M_i to establish the communication and prevent the communication from the hackers. If mismatch is identified between M_i and S_i the communication will be disconnected to maintain the securable communication and prevent the communication from the hackers.

V. IMPLEMENTATION

A. Pseudo code

Vehicle V
V searches other V for communication
V sends communication request to another V1
V1 enters the Master Key (M_i)
Response comes back to V with the Master Key (M_i)

V enters the Slave Key (S_i)
If (Mi == S_i)
{
Authenticated successfully and communication is established
}
Else
{
Authentication failed and communication is disconnected
}

The presented pseudo code describes the overall process of our architecture and how the communication is modeled and the entire architecture is prevented from the hackers.

B. Performance Evaluation

The performance of our architecture can be evaluated by the following metrics.

- Inter Vehicle Communication
- Reducing Authentication Delay
- Vehicle to Mobile Communication

A. Inter Vehicle Communication

The first metric of our architecture is, inter vehicle communication. This metric will prove how our architecture is efficient among vehicles to pass message while they are moving on the roads. The previous section explained how communication between vehicles could be established by using the technology of master key and slave key sharing. The main advantage of forming a network communication among vehicle is to exchange some essential messages to other vehicles during the emergency situations. The establishment of our network communication should be prevented from the hackers. We make use high securable authentication technology to prevent the hacking our technology. The metric inter vehicle communication can be classified into various categories, which are listed below.

- Single to Single Vehicle Communication
- Single to Many Vehicle Communication
- Many to Single Vehicle Communication
- Many to Many Vehicle Communication

As classified above the inter vehicle communication metric can be evaluated to prove the efficiency of our architecture. Our architecture allows any vehicle can communicate with any number of vehicles at a time, but the only case is all the vehicle communication should be authenticated properly in order to prevent the communication from the hackers. The following diagram represents the entire communication model of our first metric inter vehicle communication.

Figure 4: Single to Single Communication

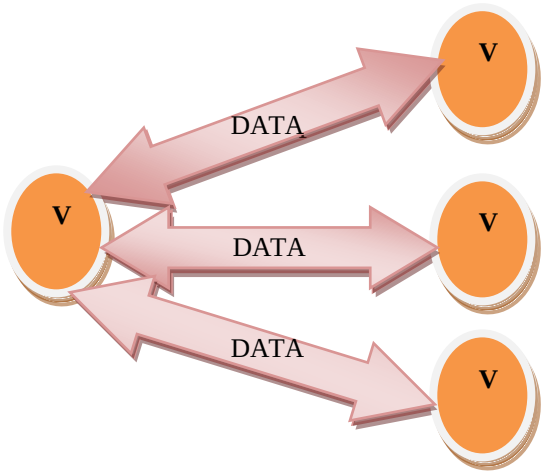

Figure 5: Single to Many Communication

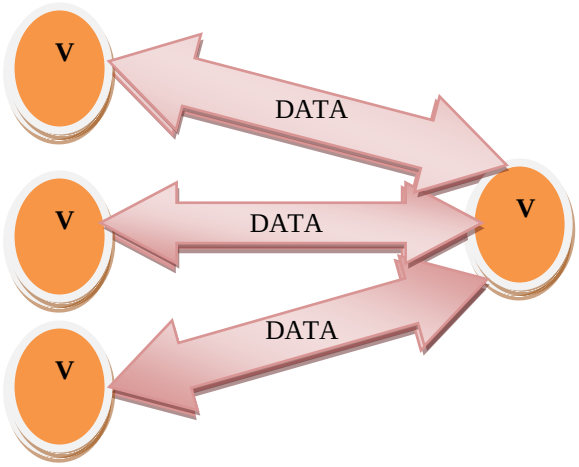

Figure 6: Many to Single Communication

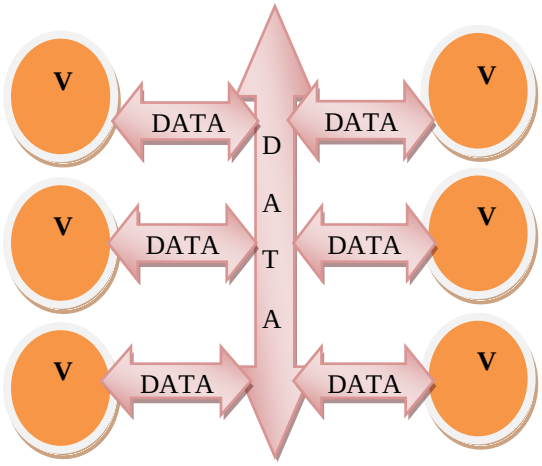

Figure 7: Many to Many Communication

The above figures 4, 5, 6, and 7 shows how inter vehicle communication is achieved. In this metric any vehicle could transfer any type of message to any vehicle, while moving on the road. That is, same message could be sent to more vehicles at a time simultaneously, this metric will be helpful to get immediate help from more vehicles. Ultimately, this metric has more securable communication and brings the safety of the passengers by communicating with other vehicles on the roads.

B. Reducing Authentication Delay

Delay is the most intolerable action in every technology. The efficiency of every technology is estimated by the delay occurred in it. The delay must be reduced to increase the efficiency of every technology. In this paper, our architecture allows to form network communication only after every vehicle is authenticated successfully. Obviously authentication process will take time and the delay will occur to establish a network communication. However the authentication delay must be reduced to improve the efficiency of the proposed network communication system. In order to reduce the authentication delay, we bring out background authentication process, which will reduce the authentication delay ultimately. The working nature of our background authentication process is described below with neat diagram.

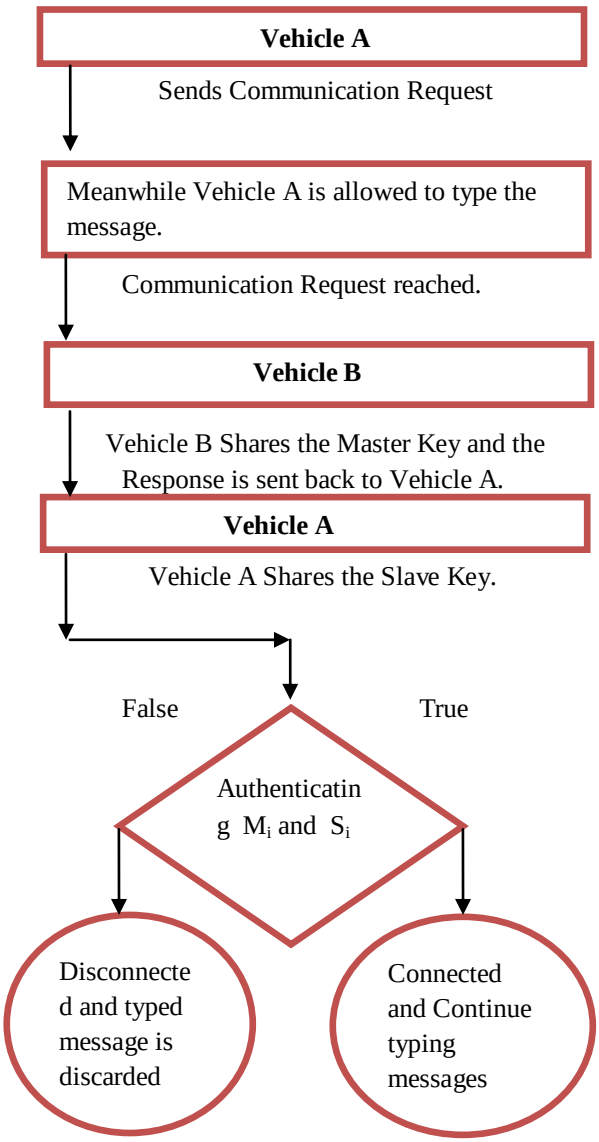

Figure 8: Reducing Authentication Delay

The figure 8 shows, how authentication delay is reduced in our proposed architecture. Vehicle A wants to communicate with vehicle B and sends the communication request. However, vehicle B should be willing to accept the communication request sent by vehicle A and vehicle B should share the master key M_i and vehicle A also should share the slave key S_i before passing any message between each other. It will take time to complete the authentication process. In order to reduce the delay occurs by the authentication process, we allow the vehicle to start typing the message in prior time, which will be passed to other vehicle. That is, as shown in the figure 8 vehicle A sends communication request to vehicle B and after sending the request, vehicle A starts typing the message immediately before authentication process takes place. Once vehicle B shares the master key M_i vehicle A will

be asked to share the slave key S_i by suspending message typing process temporarily. Authentication takes place after sharing the slave key by vehicle A by matching the M_i and S_i. If authentication is successful, the vehicle will be allowed continue typing otherwise the typed message will be discarded. Thus as stated above, the background authentication process evaluated in our architecture will reduce the authentication delay ultimately.

C. Vehicle to Mobile Communication

Another metric provided by our architecture is form network communication between vehicles and mobile phones. This metric will also bring the safety of the passengers, while travelling on the road. Forming network communication between vehicles and mobile phones will also helpful to pass the communication messages, when they in need of help. The reverse of the metric is also possible in our architecture that is, communication between mobile phones and vehicles. The establishment of network communication between vehicles and mobile phones will follow the same methodology used in forming network communication between vehicles. Similarly the network communication will be established only after authenticating both vehicles and mobile phones. The same authentication process will be carried forward by matching the master key M_i and slave key S_i. This metric brings communication between vehicles and mobile phones and allows exchanging messages with one another, whenever needed.

VI. CONCLUSION

In this paper, we modeled network communication between vehicles and also we brought out network communication between vehicles and mobile phones. We studied the comprehensive characteristics of vehicles moving on the road and Bluetooth technology. We form the network communication among vehicles using Bluetooth technology. In order to provide securable communication between vehicles and prevent our network architecture from the hackers, we have provided securable communication between vehicles by authenticating the vehicles in a securable manner. Our authentication process takes place by matching the master key and slave key shared by the vehicles. We have also provided background authentication mechanism to reduce the authentication delay. Our mechanism works well and it is evaluated by the metrics provided.

REFERENCES

[1] Hassnaa Moustafa, Sidi Mohammed Senouci, Moez Jerbi “Introduction to Vehicular Networks” 10th November 2008.

[2] Lin Yang Jingdong Xu Gongyi Wu Jinhua Guo, Nankai Univ Tianjin, China “Road Probing: RSU Assisted Data Collection in Vehicular Networks” Wireless Communications, Networking and Mobile Computing, Beijing, page: 1-4.

[3] Wern-Yarng Shieh Wei-Hsun Lee Shen ,”Analysis of the Optimum Configuration of Roadside Units and Onboard Units in Dedicated Short-Range Communication Systems”, Intelligent Transportation Systems, IEEE Transactions on Issue Date : Dec. 2006 Volume : 7 , Issue:4 On page(s): 565 – 571.

[4] Biswas, S. Misic, J. “Proxy signature-based RSU message broadcasting in VANETs”, Communications (QBSC), 2010 25th Biennial Symposium on Date: 12-14 May 2010 On page(s): 5 - 9 Location: Kingston.

[5] B. Ramakrishnan, Dr. R. S. Rajesh, R. S. Shaji, “An efficient vehicular communication outside the city environments” International Journal of Next-Generation Networks (IJNGN) Vol.2, No.4, December 2010.

[6] Saxena, N.; Tsudik, G.; Jeong Hyun Yi; Polytech. Univ., Brooklyn”Efficient Node Admission and Certificateless Secure Communication in Short-Lived MANETs”, Parallel and Distributed Systems, IEEE Transactions - Feb. 2009, Volume: 20 Issue:2 On page(s): 158 – 170.

[7] Tuteja, Asma Gujral, Rajneesh Thalia, Sunil,” Comparative Performance Analysis of DSDV, AODV and DSR Routing Protocols in MANET Using NS2”, ACE, International Conference on 2010, page(s): 330 – 333.

[8] B.Ramakrishnan, Dr.R.S.Rajesh, R.S.Shaji, “An Intelligent Routing Protocol for Vehicle safety communication in Highway Environments”, journal of computing-Volume 2, Issue 11, November 2010dec 2010.

Mr. M. Milton Joe received his MCA degree from Anna University. Presently he is working as Assistant Professor in St. Jerome’s College. He has two years of research experience and published four international journals. His research interests include Network Security, Vehicular Network and Social Networks.

Dr. R.S. Shaji received his M.Tech in Computer Science and Engineering from Pondicherry University and PhD from Manonmaniam Sundaranar University. Presently he is working as Professor in Noorul Islam University. He has seven years of research experience and published more than twenty international journals. His research interests include Mobile and pervasive Networks.

Mr. K. Ashok Kumar received his MCA degree from Anna University and M.phil from Thiruvalluvar University. He has three years of teaching experience and published two international journals. His research interests include Network Security, Data Mining and Warehousing.