A Study of Improved Security in VANET by using a Digital Signature and Hash Chain

Nazrul Islam
Dept. of ICT
Mawlana Bhashani Science and Technology University
Tangail, Bangladesh

Sajjad Waheed
Dept. of ICT
Mawlana Bhashani Science and Technology University
Tangail, Bangladesh

Abul Hasnat Anik
Dept. of ICT
Mawlana Bhashani Science and Technology University
Tangail, Bangladesh

Sudarsan Pal
Dept. of ICT
Mawlana Bhashani Science and Technology University
Tangail, Bangladesh

ABSTRACT
Day by day the total number of vehicles around the world is increasing enormously. It needs to control the vehicles for road safety. The vast development of technologies, especially the wireless technologies provide a new type of networks, such as Vehicular Ad Hoc Networks (VANETs) which provides communication between vehicle to vehicle, vehicles to server. A numerous number of new approaches are proposed such as smart cities, Intelligent Traffic System (ITS), Intelligent Light System (ILS) etc. It is difficult to control the urban traffic system by manual method. In this paper proposes an inter vehicular routing protocol using digital signature and hash chain. The inter vehicular communication using digital signature and hash function reduces this delay. Through its extensive simulation the traffic of a city environment may be controlled. The result shows that the data passing rate of inter vehicular communication decreases. As a result, each vehicle can communicate to others more quickly, which improve the road safety as well.

General Terms
Security, Networking, Vehicular Ad Hoc Networks

Keywords
VANET, ITS, ILS, Routing, cluster

1. INTRODUCTION
Mobile Ad-hoc networks (MANETs) have been investigated and applied to a lot of areas. Though vehicular Ad-hoc Networks is a subclass of Mobile Ad-hoc Network (MANETs) [1], the existing routing protocol of MANETs cannot be directly applied to VANETs. VANET mainly refers to the Inter Vehicular Communication (IVC). The Mobile ad-hoc networks can use for car to car communication. To support the development of the US Federal Communication Commission (FCC) has allocated 75 MHZ in the 5.9 GHZ band for licensed Dedicated Short Range Communication (DSRC) [2] and IEEE has defined a new standard for DSRC named 802.11p. VANET encourages a lot of companies such as BMW, Toyota to use this network for more road safety. Their several projects are Advance Driver Assistance System (ADASE2) [3] crash Avoidance Metrics Partnership (CAMP) [4], CarTatk 2000 [5], FleeNet [6] and DEMO 2000 by the Japan Automobile research Institute (JSK). Now a day several automobile companies use this type of technologies on their vehicles. In MANETs different zones are divided into different cluster.

The VANETs a lot amount of research focuses on optimal methods for clustering nodes in MANETs. The VANET proposes new challenges that the vehicles must follow each other. Vehicles must go into a queue, must follow well understood traffic movement patterns and must travel in the single direction pattern. There are many simulation models such as NS-2 [7], a micro simulation tools implementation. These tools have been designed for MANET implementation. For multi-hop communication [8] different routing protocol are used for data passing. As for different routing protocol ad-hoc on demand distance vector routing protocol (AODV) [9]

implements the route discovery mechanism for VANET network. All models and simulation tools wants to reach the same goal that the data pass rate will increase and the time delay decrease.

The rest of the paper is organized as follows. Section 2, a summary of background knowledge and related works are presented. The Section 3 provides the research method of the research is presented and in section 4 discusses the design and implementation of these experiments. Section 5 discusses the result and analysis about the research. Section 6 poses a set of conclusion and some direction for the future works.

2. RELATED WORK
For the route discovery, routing protocol different method is used. All the methods face the broadcast problem. These problems influence us to work for the high speed data pass and at the same time provide the security for the passing data.

The position-based routing becomes more popular and low cost technique of Global Positioning System (GPS) and Geo-Location Services. In geographic routing data are routed to vehicles based on their geographic location. For example position-based routing algorithms are face-2 [2], GPSR [10] and DREAM [11]. Among them GPSR (which is algorithmically identical to face-2) is seems to more suitable for the network. In GPSR, greedy forwarding is used to send data which are closest to the destination. However, there are some reasons for which data packet reaches maximum. Another study [12] also is a method to improve AODV. To deal with the challenges of city scenarios, Lochert et al. [13] proposed GSR which provides a greedy forwarding method that selects the shortest path. MDDV [14] and VADD are two multi-hop routing protocols; the idea is that the message can be delivered by carry and forward approach, to the destination. When a network is disconnected the node carry the packet and pass the packet to the nearest neighbor nodes.

The data are passed between vehicle to vehicle through the wireless technology uses the GPS based navigation system or some other digital road maps. By using these systems, the data pass loss increases and the passing data provide no security. These path losses influence the study to provide a light attachment of security code with the passing data. The main goal of this paper is to reduce the path loss. To do that, send the security code with the passes data that provide the system faster and more secure.

3. RESEARCH METHOD

The proposed system is to improve the AODV routing protocol for route discovery mechanism. When a vehicle travels on the road, it gets data from the server. The data are served by the road side network such as 4G network, Wi-Fi etc. The Vehicle must reply the server request. Each vehicle, then gets an instruction to move or not. This vehicle to vehicle and vehicle to server communication should be faster that less than a second. The research is divided into three parts to implement: 1) Collecting sample data 2) Encrypt the data 3) Implement the decryption process and analyze the data for server instruction.

Firstly, to analyze the data, traffic traces the vehicle by different network: school Wi-Fi network, home Wi-Fi networks or mobile networks. After the tracing process data pass through the encryption and decryption process.

Secondly, the server sends a signed data packet to the destination. The data packet is signed by the digital signature. A certificate is attached to the data packet so that the directed receiver can receive this signed data. The vehicles receive the data packet, but only those receivers can decrypt the message whose certificate match to the sender's certificate. Then those receivers decrypt the signed data packet and get instruction to move.

Finally, after the encryption and decryption process data passes to the remote server. Analyzing the get data a proper decision is gathered for the vehicle movement.

4. DESIGN AND IMPLEMENTATION

In VANET the fast moving nodes, frequent topology changed data packet passes as early as possible to the moving nodes. A light weight data packet with digital signature helps the data packet for moving fast.

4.1 Data encryption and decryption

A digital signature signs the data at the sender nodes by its public key cryptosystem. An attachment of hash code with binary value passes with the encrypted data. These data packets pass through the wireless technology. When the receiver node receives the same hash code, then decrypt the data.

Pseudo code:

1. Input the binary value data
2. Data is encrypted with D_{sign} and produce a hash message Ds_{hash}
3. Receiver receives Dr_{hash} data
4. If $Ds_{hash} = Dr_{hash}$, then decrypt Dr_{hash} data
5. After decryption Dr_{hash} data the original D_{sign} data will find

These shows when the data packet signatures of two node matches, then the signed data packet decrypts the data and get the message.

4.2 Data encryption process

Each vehicle of a small cluster gets the message, but the decrypt process executes when the matched certificate is found

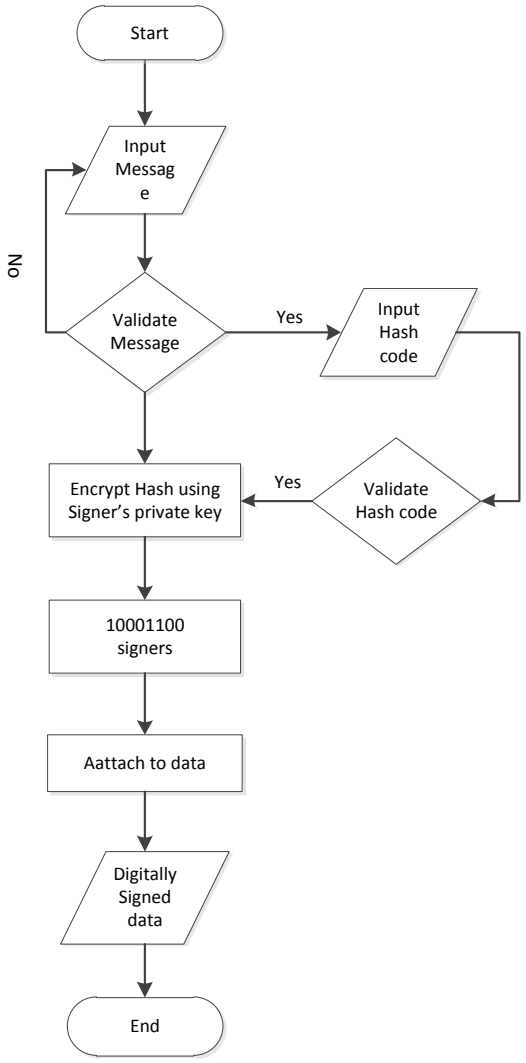

Fig 1: Data encryption process

Figure 1 shows data encryption process. A valid hash code encrypts the data packet with the user private key. This valid hash code attaches with the original data and produce digitally signed data.

4.3 Data decryption process

The signed data, then send to the receiver for decryption.

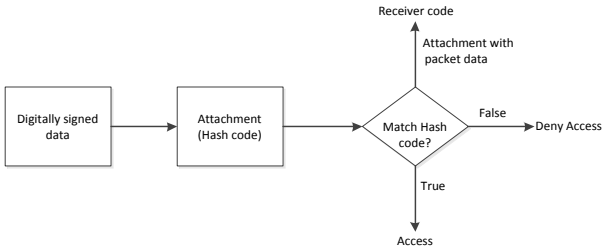

Fig 2: Data decryption process

The digital signed data decrypt at the receiver end. When two hash code matches, then the original data is found. In this way every vehicle passes data among themselves and to the server. The input of the attachment is a binary value that causes the data pass rate is lower than any other mathematical value.

At the end, data is analyzed by the server and sends the instruction to the vehicles as they can make the proper decision for passing, overtaking, breaking and so on. Proper maintenance of the instruction and the drivers driving skill make the journey safer.

5. RESULT AND ANALYSIS

This section provides a detailed description about the results and analysis of the obtained data. For data transmission each vehicle transmits a Route Request Packet (RREQ) to its neighbor nodes. Each node when receives the request, then send a Route Reply (RREP) message that it receives those messages. When it receives the message, then establishes a link and transmits data. Each vehicle sends data to their neighbor nodes, until the source reached to the location. Route maintenance maintains the routes that are active. When the link is not available it sends a Route Error Message, this will continue until it gets secure link and provides a HELLO message to detect the link breakage. The failure of reception of three consecutive HELLO message from a neighbor is handled as link error.

When data pass from one node to another node, every node signs the data so that the receiver node can get the message by this same signature. The sender node signs the information by its public key and encrypts the data. The encrypted data passes to the neighboring node. Here, hash chain is used in such a suitable system so that the data pass rate of the digital remains high. Suppose the signed data is D_{sign}. This data passes through the encryption process and produce a hash code like D_{Hash}. These D_{Hash} codes are attached to the main data.

Data at the receiver node the D_{Hash} data are decrypted by the decryption process. The decryption process the signature data D_{sign} is found at the receiver node. Therefore, every node uses digital signatures to sign the whole message and that any neighbor that receives verifies the signature.

The sender sends routing request packets and at a time get the routing reply packet, then the total data stored in a temporary file. This increases the delay and make the collisions. Because of sending repeat requests and at the same time of the data packet, there establish a link and also reduce the delay.

The VANET process is a super fast technology. When the process faces the time delay, there may cause a great harm for the system. Then, instead of road safety it will be the road risk technology. The lighter of the attachment of data, the more speed of data passing rate. As we use the binary value of the attachment transmitting data, the time delay decreases than any other value.

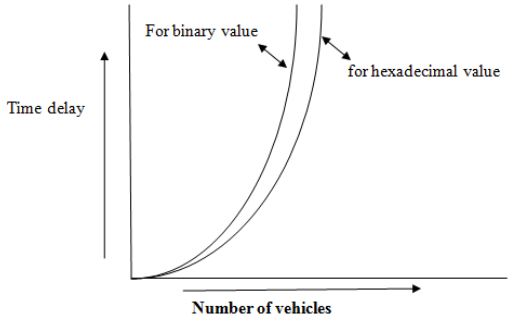

Fig 3: Time delay compares with hexadecimal and binary value

The graph shows that for binary and hexadecimal value time delay increases with more rapidly in binary value than hexadecimal value. For larger number of vehicles this delay time increases more and more than binary value. For data passing vehicle to vehicle using a binary value decreases the time delay. This research provides the AODV routing protocol using light attachment hash code.

6. CONCLUSION

In this paper is presented a set of observation with regards to a light attachment with the digital signature. This light weight attachment with the digital signature can be called the simplification of digital signature. Firstly, the data passing this digital signature provides an extra security for data authentication. Secondly, the light attachment of hash code data provides an extra feature for fast data passing with the condition of matching two hash codes. All the process is done for car to car fast communication. Finally, light attachment of data reduces the time between car to car and car to server communication.

Future work can be address as focus on various collisions warning message when two cars overtake each other. Furthermore, it would be interesting to study the use of co-operative collision warning, Electric brake warning and more.

7. REFERENCES

[1] Jerbi, M., Senouci, S. M., Meraihi, R., & Ghamri-Doudane, Y. (2007, June). An improved vehicular ad hoc routing protocol for city environments. In *IEEE International Conference on Communications, 2007. ICC'07*. (pp. 3972-3979). IEEE.

[2] Abedi, O., Berangi, R., & Azgomi, M. A. (2009, June). Improving route stability and overhead on AODV routing protocol and make it usable for VANET. In *29th IEEE International Conference* on *Distributed Computing Systems Workshops, 2009. ICDCS Workshops' 09*. (pp. 464-467). IEEE.

[3] Shulman, M., & Deering, R. K. (2005). *Third Annual Report of the Crash Avoidance Metrics Partnership, April 2003-March 2004* (No. HS-809 837).

[4] Andreone, L., & Ricerche, C. (2005). Activities and applications of the vehicle to vehicle and vehicle to infrastructure communication to enhance road safety.*Proc. 5th Eur. Congr. Exhib. ITS, Hannover, Germany*.

[5] Krüger, R., Füßler, H., Torrent-Moreno, M., Transier, M., Hartenstein, H., & Effelsberg, W. (2005). Statistical analysis of the FleetNet highway movement patterns.

[6] Sivavakeesar, S., & Pavlou, G. (2002, September). A prediction-based clustering algorithm to achieve quality of service in mulithop ad hoc networks. In *Proc. of the London Communications Symposium (LCS)* (pp. 157-160).

[7] Project, V. The network simulator NS-2 http://www.isi.edu/nsnam/ns/ [Online; Accessed: 28-July-2014]

[8] Perkins, C. E., & Royer, E. M. (1999, February). Ad-hoc on-demand distance vector routing. In *Second IEEE Workshop on Mobile Computing Systems and Applications, 1999. Proceedings. WMCSA'99.* (pp. 90-100). IEEE.

[9] Johnson, D. B., & Maltz, D. A. (1996). Dynamic source routing in ad hoc wireless networks. In *Mobile computing* (pp. 153-181). Springer US.

[10] Bose, P., Morin, P., Stojmenović, I., & Urrutia, J. (2001). Routing with guaranteed delivery in ad hoc wireless networks. *Wireless networks*, *7*(6), 609-616.

[11] Karp, B., & Kung, H. T. (2000, August). GPSR: Greedy perimeter stateless routing for wireless networks. In *Proceedings of the 6th annual international conference on Mobile computing and networking* (pp. 243-254). ACM.

[12] Basagni, S., Chlamtac, I., Syrotiuk, V. R., & Woodward, B. A. (1998, October). A distance routing effect algorithm for mobility (DREAM). In *Proceedings of the 4th annual ACM/IEEE international conference on Mobile computing and networking* (pp. 76-84). ACM.

[13] Lochert, C., Hartenstein, H., Tian, J., Fussler, H., Hermann, D., & Mauve, M. (2003, June). A routing strategy for vehicular ad hoc networks in city environments. In *Intelligent Vehicles Symposium, 2003. Proceedings. IEEE* (pp. 156-161). IEEE.

[14] Zhao, J., & Cao, G. (2008). VADD: Vehicle-assisted data delivery in vehicular ad hoc networks. *IEEE Transactions on Vehicular Technology*, *57*(3), 1910-1922.