ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

An Innovative Method For Delay Reduction In VANETS

Veena.V.Gopal [*1], **S. Manikandan** [2]
Department of Electronics and communication, PSN College of Engineering and technology, India
veenavgopal90@gmail.com

Abstract

An Vehicular networks are used for vehicle to vehicle communication and vehicle to roadside equipment communication. Many developing countries are badly in need of VANET for vehicular safety. It is a growing area of research with a large number of applications. Vehicular Ad-hoc Networks (VANETs) can be considered as a subset of Mobile Ad hoc Networks (VANETs) with unique characteristics. The applications seen so far include safety applications, traffic efficiency enhancements, and infotainment services. All applications are matched with proper security mechanisms. Current proposals have its key focus on entity authorization using a public key infrastructure. It gives a proactive security mechanism that excludes non authorized entities from the network. However this method cannot eliminate insider attackers from the network. If informations are received from both honest and malicious vehicles, the attacks need to be detected. In this paper, we propose Ron Shamir Adleman algorithm (RSA) to increase the security and AODV to reduce the delay. The simulated result shows an increased security and reduced delay.

Keywords: Data consistency, Vehicular networks (VANET)

Introduction

VANET is a special class of MANET to provide communication among vehicles and between vehicles and nearby roadside equipments. It is based upon short range wireless communication between vehicles. In these networks, each vehicle is equipped with communication equipments, computing devices and GPS (Global Positioning Systems) receivers. GPS receiver provides all the information of a vehicle like speed, direction of movement of vehicle, time, location etc. Each vehicle stores the information about itself and other vehicles in a local database. The records of this database are periodically broadcasted to other vehicles and road side equipments. This record comprises some parameters like vehicle identification number, position(latitude and longitude), direction, speed of vehicle, time stamp of creation of record, time stamp of receiving updated record etc.

The applications of VANET include vehicle collision warnings, security distance warning, driver assistance, cooperative driving, dissemination of road information, internet access, map location, automatic parking, weather forecasting. When a vehicle is coming through the wrong lane or the vehicle is in over speed coming close to each other then the driver will get a vehicle collision warning. This will help the driver to take the necessary measures to avoid the accident. Security distance warnings are given when two vehicles come in an unsafe distance. Thus the chances of collision can be avoided. The vehicular networks will give alerts when an emergency vehicle is coming. It will disseminate the current traffic information to all the vehicles. The driver is provided enough internet access while travelling on road. It informs the driver about current parking space availability and also provide map updates. Most of the traffic problems can be solved by providing appropriate information to the driver or to the vehicle. Existing research on routing protocols, which exclusively focuses on routing efficiency, will not be ideal from a security perspective. More research is necessary on protocols that explore the tradeoff between increased security due to redundancy on the one hand and dissemination efficiency on the other hand. Existing system uses Advanced encryption standard (AES) algorithm. The existing system consist of a categorization of data consistency mechanisms into model-based, sensor-based, and dissemination-redundancy-based approaches and argue that redundant data forwarding paths are the most promising technique to enable consistency checks in multihop data dissemination protocols. The entity authorization eliminates the unauthorized users from the communication. Its key focus is on eliminating the attacker nodes. It does not have any focus on reducing the delay. Data dissemination and data consistency are the two mechanisms used in the existing research. It uses different dissemination patterns for the transfer of messages from the sender to the receiver.

This paper uses Ron Shamir Adleman (RSA) algorithm. This algorithm overcomes the security issues in the existing system. All data packets and control packets are unlinkable and unobservable. Unlinkability of two or more IOIs means these IOIs are no more or no less related from the attacker's view. Unobservability of an IOI is the state that whether it exists or not is indistinguishable to all unrelated subjects, and subjects related to this IOI are anonymous to all other related subjects. So this paper defined stronger privacy requirements regarding privacy-preserving routing in vehicular networks. Then we propose an unobservable secure routing scheme USOR to offer complete unlink ability and content unobservability for all types of packets. It also uses AODV to reduce the delay in communication. It always chooses the shortest path to the destination. This paper uses a public key infrastructure to ensure data security.

Materials and methods

Adhoc On Demand Distance Vector Routing (AODV)

It is a reactive routing protocol. It establishes a route to a destination only on demand. In contrast, the most common routing protocols of the Internet are proactive, meaning they find routing paths independently of the usage of the paths. AODV is, as the name indicates, a distance-vector routing protocol. AODV avoids the counting-to-infinity problem of other distance-vector protocols by using sequence numbers on route updates, a technique pioneered by DSDV. AODV is capable of both unicast and multicast routing**.**In AODV, the network is silent until a connection is needed. At that point the network node that needs a connection broadcasts a request for connection. Other AODV nodes forward this message, and record the node that they heard it from, creating an explosion of temporary routes back to the needy node. When a node receives such a message and already has a route to the desired node, it sends a message backwards through a temporary route to the requesting node. The needy node then begins using the route that has the least number of hops through other nodes. Unused entries in the routing tables are recycled after a time. When a link fails, a routing error is passed back to a transmitting node, and the process repeats. Much of the complexity of the protocol is to lower the number of messages to conserve the capacity of the network. For example, each request for a route has a sequence number. Nodes use this sequence number so that they do not repeat route requests that they have already passed on. Another such feature is that the route requests have a "time to live" number that limits how many times they can be retransmitted. Another such feature is that if a route request fails, another route request may not be sent until twice as much time has passed as the timeout of the previous route request. The advantage of AODV is that it creates no extra traffic for communication along existing links. Also, distance vector routing is simple, and doesn't require much memory or calculation. However AODV requires more time to establish a connection, and the initial communication to establish a route is heavier than some other approaches.

The AODV Routing protocol uses an on-demand approach for finding routes, that is, a route is established only when it is required by a source node for transmitting data packets. It employs destination sequence numbers to identify the most recent path. The major difference between AODV and Dynamic Source Routing (DSR) stems out from the fact that DSR uses source routing in which a data packet carries the complete path to be traversed. However, in AODV, the source node and the intermediate nodes store the next-hop information corresponding to each flow for data packet transmission. In an on-demand routing protocol, the source node floods the Route Request packet in the network when a route is not available for the desired destination. It may obtain multiple routes to different destinations from a single Route Request. The major difference between AODV and other on-demand routing protocols is that it uses a destination sequence number (DestSeqNum) to determine an up-to-date path to the destination. A node updates its path information only if the DestSeqNum of the current packet received is greater than the last DestSeqNum stored at the node. A Route Request carries the source identifier (SrcID), the destination identifier (DestID), the source sequence number (SrcSeqNum), the destination sequence number (DestSeqNum), the broadcast identifier (BcastID), and the time to live (TTL) field. DestSeqNum indicates the freshness of the route that is accepted by the source. When an intermediate node receives a Route Request, it either forwards it or prepares a Route Reply if it has a valid route to the destination. The validity of a route at the intermediate node is determined by comparing the sequence number at the intermediate node with the destination sequence number in the Route Request packet. If a Route Request is received multiple times, which is indicated by the BcastID-SrcID pair, the duplicate copies are discarded. All intermediate nodes having valid routes to the destination, or the destination node itself, are allowed to send Route Reply packets to the source. Every intermediate node, while forwarding a Route Request, enters the previous node address and its BcastID. A timer is used to delete this entry in case a Route Reply is not received before the timer expires. This helps in storing an active path at the intermediate node as AODV does not employ source routing of data packets. When a node receives a Route Reply packet, information about the previous node from which the packet was received is also stored in order to forward the data packet to this next node as the next hop toward the destination. DSR includes source routes in packet headers. Resulting large headers can sometimes degrade performance-particularly when data contents of a packet are small; AODV attempts to improve on DSR by maintaining routing tables at the nodes, so that data packets do not have to contain routes. AODV retains the desirable feature of DSR that routes are maintained only between nodes which need to communicate. Route Requests (RREQ) are forwarded in a manner similar to DSR. Routing table entry uses a reverse path. Setting the routing table is very important. When a node re-broadcasts a Route Request, it sets up a reverse path pointing towards the source-AODV assumes symmetric (bi-directional) links. When the intended destination receives a Route Request, it replies by sending a Route Reply (RREP).Route Reply travels along the reverse path set-up when Route Request is forwarded. Route Request (RREQ) includes the last known sequence number for the destination. An intermediate node may also send a Route Reply (RREP) provided that it knows a more recent path than the one previously known to sender. Intermediate nodes that forward the RREP, also record the next hop to destination. A routing table entry maintaining a reverse path is purged after a timeout interval. A routing table entry maintaining a forward path is purged if not used for an active-route-timeout interval.

A neighbor of node X is considered active for a routing table entry if the neighbor sent a packet within active-route-timeout interval which was forwarded using that entry. Neighboring nodes periodically exchange hello message. When the next hop link in a routing table entry breaks, all active neighbors are informed. Link failures are propagated by means of Route Error (RERR) messages, which also update destination sequence numbers. When node X is unable to forward packet P (from node S to node D) on link (X,Y), it generates a RERR message. Node X increments the destination sequence number for D cached at node X. The incremented sequence number *N* is included in the RERR. When node S receives the RERR, it initiates a new route discovery for D using destination sequence number at least as large as N. When node D receives the route request with destination sequence number N, node D will set its sequence number to N, unless it is already larger than N. Routes need not be included in packet headers. Nodes maintain routing tables containing entries only for routes that are in active use. At most one next-hop per destination maintained at each node-DSR may maintain several routes for a single destination. Sequence numbers are used to avoid old/broken routes. Sequence numbers prevent

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

formation of routing loops. Unused routes expire even if topology does not change. One of the advantage of adhoc on demand distance vector routing is that routes are established on demand and destination sequence numbers are used to find the latest route to the destination. It have only a lower delay for connection setup. At first the suitable route to the destination is discovered. It is done by sending a route request (RREQ) from the source to the destination. Route discovery in AODV is shown in fig1

Figure:

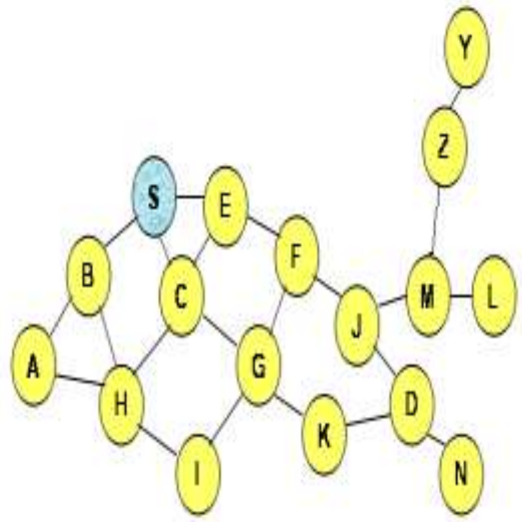

Fig1. Represent a node that has received RREQ for D from S.

The send route request is then transmitted to the destination through different paths. All nodes in the path between source and destination receives the route request and is send node to node. The request is transferred through different paths at the same time to reduce the delay in finding the shortest path. If the request is forwarded through a single path at a time it takes more time to find the shortest path as it forwards the request through another path only after cancelling one path. So the time to find the shortest path increase when the number of paths between the source and destination increase.The transmission of route request is shown in fig2

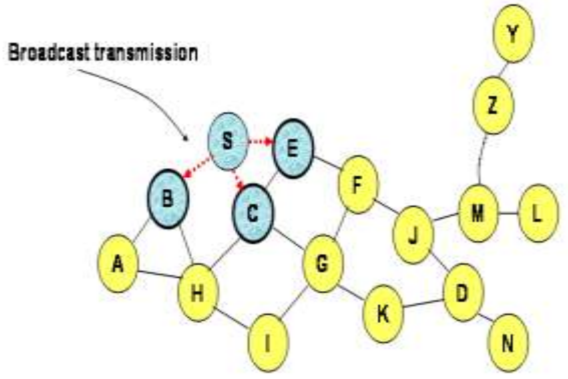

Fig2. Transmission of RREQ

Before setting the reverse path the reverse path inks are setup Node C receives RREQ from G and H, but does not forward it again, because node C has already forwarded RREQ once.. The links on the reverse path is shown in the fig3

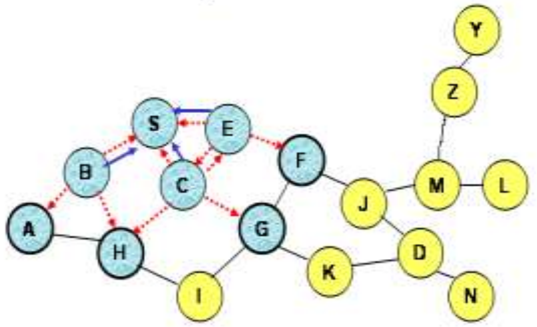

Fig3. Links on reverse paths.

Node D does not forward RREQ, because Node D is the intended target of RREQ. The request is transferred through different paths at the same time to reduce the delay in finding the shortest path Sequence numbers prevent formation of routing loops. Sequence numbers are used to avoid old/broken routes . The reverse path setup is shown in fig4.

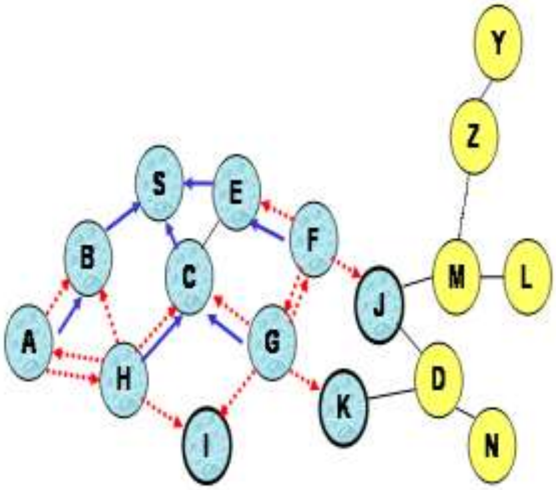

Fig4. Reverse path setup in AODV

Forward links are Set-Up when RREP travels along the reverse path. The forward path setup in AODV is shown in fig5. The curved arrow represents a link broken on the forward path

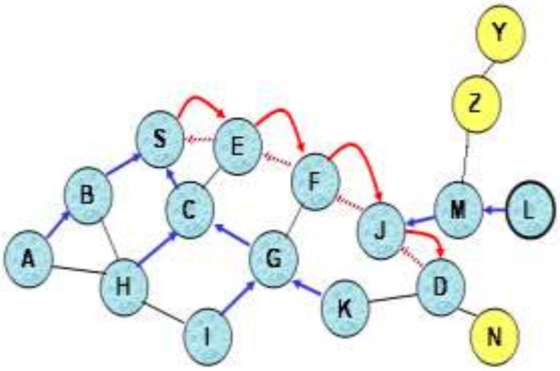

Fig5. Forward path set-up in AODV

Secure Data Transmission

The secured data transmission is provided by using encryption and decryption of messages. This paper uses a third party service to increase the security of transmitted data. A public key is widely distributed while the private key is known only to its propriator. The keys are related mathematically but the parameters are chosen so that calculating the private key from the public key is impossible.The public key is used to encrypt plain text and the private key is used to decrypt the cipher text.The trusted authority has a database consisting of all informations about each and every user in the network. It checks the authorization of all users involved in communication. It allows only the authorized users to communicate each other. The keys are issued by the trusted authority. The message can be decrypted only by using the key. Insider cannot modify the message as it is transmitted in the encrypted form.

The trusted authority issues certificates for only those authorized users during data transfer. These certificatesv carries some informations like the identity of the certified authority,owners identity, owners public key, the certificate expiry date etc. The recipient can verify the certificate to make sure that the certificate is valid. The use of key infrastructure provides better security than any other methods. It involves a sequence of exchanges. Here security is provided in the network and the transport layer. The network layer is confidential if all the data carried by IP datagram are in encrypted form. The encryption is done by using public key. The public keys are issued by the trusted authority after verifying the authorization of the user.

Results and discussion

The next generation of wireless communication systems, there will be a need for the rapid deployment of independent mobile users. Significant examples include establishing survivable, efficient, dynamic communication for emergency/rescue operations, disaster relief efforts, and military networks. A typical VANET consists of vehicles and access points along the road. Vehicles move on the roads sharing information between themselves and with the Internet through the access points. Vehicles often move at high speed but their mobility is rather regular and Predictable. High speed movement creates scenarios characterized by a very dynamic network topology. Vehicles can always rely on recharging batteries. An accurate estimate of vehicles position can be made available through GPS systems or on-board sensors. VANETs are used for short range, high-speed communication among nearby vehicles, and between vehicles and roadside infrastructure units.

The existing research in vehicular communication focused only in finding the attacker nodes. It does not provide any measures to reduce the delay and overhead.

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

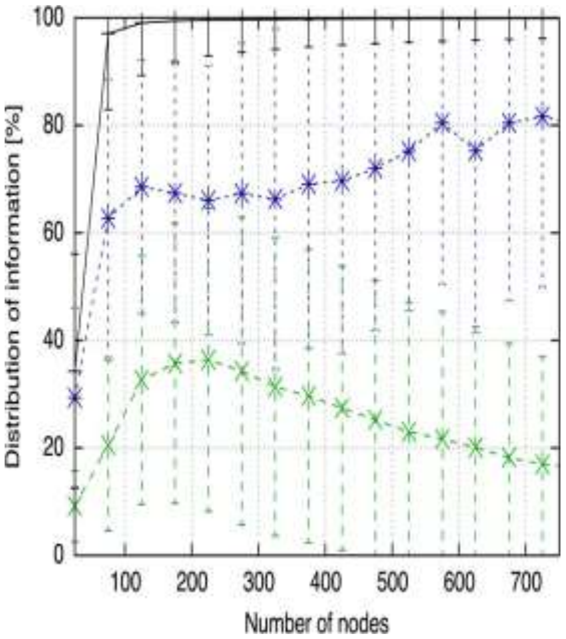

Fig6. Comparison of performance of existing systems in three different scenarios

The simulation results of the existing system is shown in fig6. The X-graph shows the performance of the vehicular networks in three different scenarios. The three scenarios are one with heavy traffic, one with medium traffic and one with light traffic. The graph is drawn between the number of nodes and the percentage of distribution of information. When the number of nodes increases more number of nodes are involved in the communication thus the percentage of distribution of information also increases. It is found that the performance is very poor in city scenario. City scenario is having a heavy traffic due to the increased number of nodes. As the number of nodes increases the need to trasfer more messages increases. Network congesion occur due to the overhelming of messages. The performance is degraded by the increased delay. This discreepency is overcomed in this paper.

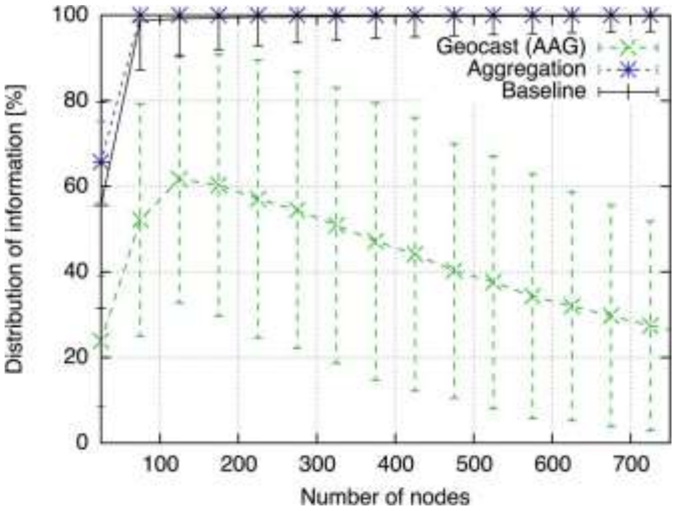

Fig7. Performance after implementing AODV

The performance of vehicular networks after implementing AODV is shown in fig7. The performance is improved by reducing the delay. The number of nodes involved in communication increased. The percentage of information transfer increased.

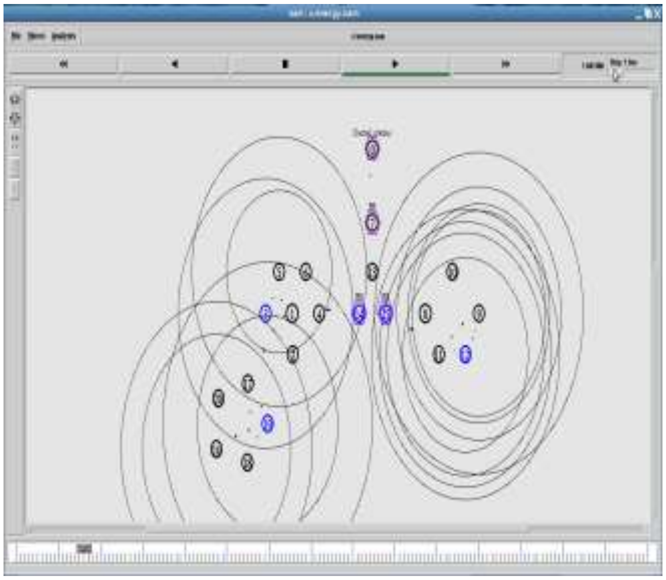

Fig8.screenshot of output

Conclusion

An unobservable routing protocol USOR based on group signature and ID-based cryptosystem for ad hoc networks is proposed. The design of USOR offers strong privacy protection completes unlinkability and content unobservability for adhoc networks. The security analysis demonstrates that

USOR not only provides strong privacy protection, it is also more resistant against attacks due to node compromise. We implemented the protocol on ns2 and examined performance of USOR, which shows that USOR has satisfactory performance in terms of packet delivery ratio, latency and normalized control bytes.

References

1. *E. Schoch, F. Kargl, M. Weber, and T. Leinmuller, "Communication patterns in VANETs," IEEE Commun. Mag., vol. 46, no. 11, pp. 119–125,Nov. 2008.*
2. *P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger,M. Raya, Z. Ma, F. Kargl, A. Kung, and J.-P. Hubaux, "Secure vehicular communication systems: Design and architecture," IEEE Commun. Mag.,vol. 46, no. 11, pp. 100–109, Nov. 2008*
3. *F. Kargl, P. Papadimitratos, L. Buttyan, M. Müter, E. Schoch,B. Wiedersheim, T.-V. Thong, G. Calandriello, A. Held, A. Kung, and J.-P. Hubaux, "Secure vehicular communication systems: Implementation, performance, and research challenges," IEEE Commun. Mag.,vol. 46, no. 11, pp. 110–118, Nov. 2008.F. Dressler, F. Kargl, J. Ott, O. K. Tonguz, and L. Wischhof ,"Executive summary—Inter-vehicular communication," in Proc. Dagstuhl Semin.10402—Inter-Veh. Commun., Wadern, Germany, Oct. 2010.*
4. *IEEE Trial-Use Standard for Wireless Access in Vehicular Environments-Security Services for Applications and Management Messages, IEEE Std.1609.2-2006.*
5. *M. Raya, P. Papadimitratos, V.D. Gligor, and J.-P. Hubaux, "On datacentric trust establishment in ephemeral ad hoc networks," in Proc. 27th Conf. IEEE INFOCOM, 2008, pp. 1238–1246.*
6. *P. Golle, D. Greene, and J. Staddon, "Detecting and correcting malicious data in VANETs," in Proc. 1st ACM Int. Workshop VANET, New York,2004, pp. 29–37.*
7. *T. Leinmüller, E. Schoch, F. Kargl, and C. Maihöfer, "Decentralized position verification in geographic ad hoc routing," Security Commun. Netw., vol. 3, no. 4, pp. 289–302, 2010.*
8. *J. Petit, M. Feiri, and F. Kargl, "Spoofed data detection in VANETs using dynamic thresholds," in Proc. IEEE VNC, Nov. 2011, pp. 25–32.*
9. *J. Petit and Z. Mammeri, "Dynamic consensus for secured vehicular adhoc networks," in Proc. IEEE 7th Int. Conf. WiMob, Oct. 2011, pp. 1–8.*
10. *S. Dietzel, J. Petit, F. Kargl, and G. Heijenk, "Analyzing dissemination redundancy to achieve data consistency in VANETs (short paper),"in Proc. 9th ACM Int. Workshop Veh. Inter-Netw., New York, 2012,pp. 131–134.*

Author Biblography

	Veena.V.Gopal ME Student at PSN College of engineering Email: veenavgopal90@gmail.com