Routing and Security in Vehicular Networking

Di Yan, diyan at go.wustl.edu (A paper written under the guidance of Prof. Raj Jain)

Download

Abstract

Vehicular Networking (VANETs) is a promising networking technology which allows road safety, traffic management and information dissemination for drivers and passengers. For VANETs, an efficient routing protocol is important for information transmission in VANETs due to the rapidly and constantly changes of network topology. The security issue is also important since some of the applications are safety-related. This paper will introduce the recent development of the routing protocol and security of VANETs. These recently proposed mechanisms have been designed to best fit the characteristics of VANETs which leads to a more complete network platform for the application of VANETs.

Keywords

VAENTs; VANETs routing protocols; SD-AOMDV; improved GPSR; VANETs security; DMGTA; certificate revocation.

Table of Contents

- 1. Introduction
- 2. VANETs Routing Protocol
  - 2.1 General Routing Protocols
  - 2.2 SD-AOMDV
  - 2.3 An Improved GPSR Routing Strategy
- 3. Security in VANETs
  - 3.1 A Defensive Mechanism for VANETs in Game Theoretic Approach
  - 3.2 A New Certificate Revocation Mechanism for VANETs
- 4. Summary
- 5. List of Acronyms
- 6. Reference

1. Introduction

Wireless and mobile communications has been developed rapidly in recent years. The concept of Mobile Ad Hoc Networks (MANETs) has become very popular in networking. MANETs are a type of ad hoc network where the nodes are mobile. The network topology can change over time. A Vehicular Ad Hoc Network (VANET) is an important application of MANET which uses cars as mobile nodes to create mobile networks. Every car within a VANET acts as a wireless router or node which allows cars to connect to each other as well as connect to road facilities to exchange information. This network gives the platform to provide Intelligent Transportation System (ITS) which includes applications that are aimed for traffic control, safety management and provide convenience services for the driver and passengers such as near-by services information, real-time detour routes computation. Because of the improvement VANETs bring to the current traffic system management, many researchers have been focusing on improving different aspects of VANETs [Gerla11].

In VANETs, there are 3 ways of communications: Inter-vehicle communication, vehicle-to-roadside communication, and routing-based communication. In inter-vehicle communication, there are two types of message forwarding mechanism: naive broadcasting - where vehicles periodically broadcast messages and ignore the message from behind. It ensures all the vehicles moving in forward direction can receive the broadcast message. Intelligent broadcasting where the number of message broadcast for an event is limited. If the event-detecting vehicles receives same messages from the vehicles from behind, it is assumed that at least 1 vehicle from behind received the message and stop broadcasting. The vehicle from behind is responsible for moving the message forward. Vehicle-to-roadside communication is the communication between the road-side unit and the vehicles. The roadside unit will periodically broadcast certain information such as speed limit to all the vehicles within its range. This communication must provide large bandwidth between the vehicle and roadside unit. Routing-based communication is a unicast communication from the source to the destination. This kind of communication will be explained in detail in this paper.

In this paper, we introduce recent advances inVANETs routing protocols and security mechanisms. The existing routing protocols still haven't taken the best advantage of the VANETs characteristics. In the second section of the paper we are going to introduce two recently proposed VANETs routing protocol which are more suitable for VANETs characteristics. VANETs security is also an important research area because VANETs affects the safety of the drivers and passengers. The third section of the paper is going to introduce two recently proposed security mechanisms for enhancing the security of VANETs.

2.VANETs Routing Protocol

Message transmission is important in VANETs. An effective routing protocol can directly affect the efficiency of the packet transmission in VANETs. Through all these years' development, there are many routing protocols for VANETs; some of these routing protocols are widely used. Although there are plenty of existing routing protocols for VANETs, as the applications based on VANETs become more and more popular and some of the applications have been applied to critical area like traffic safety management, people start to notice that the quality of the data transmission in VANETs deeply affects the performance of the network as well as the performance of the application that is built on top of the network. In recent years, many new routing protocols have been proposed. Most of them are improvement of the current work. In this section, we introduce general routing protocols and two recently developed routing protocols for VANETs.

2.1 General Routing Protocols

As an application of MANETs, VANETs is a self-organized network where there's no centralized authority or server to control the communication in the network and every node in the network acts as a terminal as well as a router. The communication between two nodes can be done directly without the help of other devices. VANETs share some same characteristics as MANETs: the nodes in network are rapidly moving and the topology of the network keeps changing. However, the general MANETs routing protocol is not efficient enough for VANETs, for VANETs have their own issues [Paul11]: 1. Frequent Disconnected network 2. Mobility Modeling 3. Battery Power and Storage Capacity 4. Communication Environment 5. Interaction with onboard Sensors.

Based on these characteristics, VANETs have developed several routing protocol that can optimize and avoid the pros and cons of these characteristics. The routing protocol can be basically divided into two categories: topology-based and position-based routing protocols. Topology-based routing protocols inherit the characteristics of a traditional MANETs routing protocol which send the data packets based on the links information where the routing table is stored. It is categorized into 3 subclasses: Proactive which update the routing table periodicity, reactive which maintain the routes only when needed and hybrid routing protocols which combine proactive and reactive protocols. Position-based touting Protocols determine routes on the positional information of the nodes. A source sends the packets using the geographic position rather than network addresses. This is a more stable routing protocol for VANET. There are 3 subclasses for Position-based routing protocol: Delay tolerant network protocol (DTN) where other nodes will help to finish the forwarding of data packets if one node cannot contact others, non-delay tolerant network (Non DTN) which always assumes that the communications are successful and hybrid position-based routing protocol which combines the characteristics of both DTN and Non DTN. Topology-based routing protocol and position-based routing protocol are the two basic categories of VANETs. Each category has its own subclasses and underlying protocols. Figure 1 shows a general classification of the VANETs routing protocols. [Altayeb13]

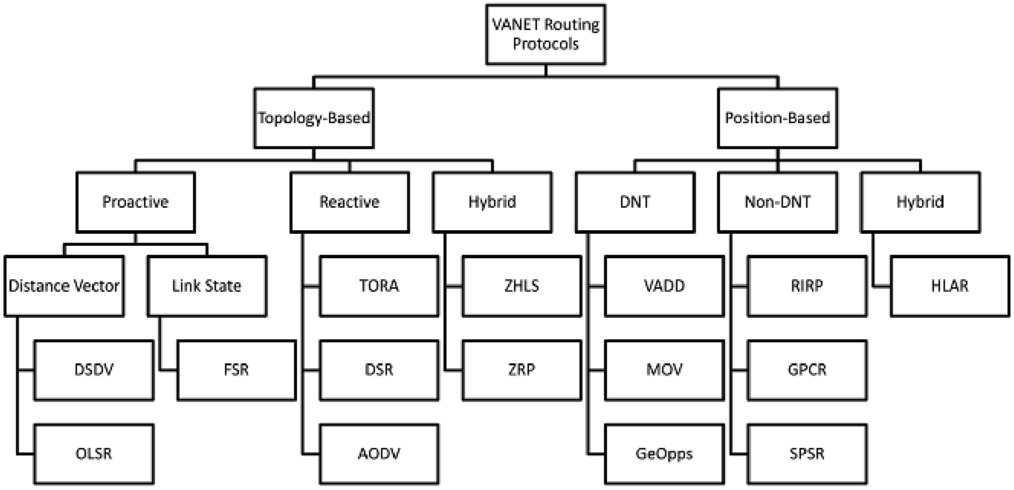

Figure 1: a general classification of the VANETs routing protocols

2.2 SD-AOMDV [Maowad12]

For the two general categories of the VANETs routing protocols, position-based routing protocols may provide more convenience, however they are hard to apply. An easy way to apply routing protocols to VANETs is to improve the existing MANETs routing protocols making them suitable for VANETs environment. AODV is one of the important MANETs routing protocols. AOMDV is the extension of AODV which can find multiple paths in a single route discovery process so if one path fails, there's no need to find a new one. SD-AOMDV is an improved protocol proposed in 2012 based on AOMDV. It is more suitable for the VANETs environment.

SD-AOMDV adds two new parameters: speed and direction to the hop count field of the AOMDV routing metrics. The intermediate nodes are selected based on these two parameters of the source node and destination node. The route in VANETs is unstable, because nodes are constantly moving at a fast speed. The entire concept is to maintain the stability of the route. For each disjoint path, the maximum difference between each node's speed and the average speed of source and destination are defined as speed metric. The path with minimum speed metric will be selected to act as optimal path. To further explain the nodes selection strategy: If two nodes that are trying to communicate are moving in the same direction, only nodes that are moving in the same direction can be selected as intermediate nodes. On the other hand, if two nodes are heading to different directions, the node that is moving in the same direction either as the source or as the destination can be selected as intermediate nodes; also the protocol uses speed parameter to select nodes at a speed that has minimum difference to the average speed between source and destination. Then by the time the node receives a message, it will not go out of the transmission range of the network and it results in an optimal path with other nodes in the path by the time it receives the packet.

In the SD-AOMDV mobility model, vehicles have 4 different directions based on the x, y coordinates. To determine the vehicle direction, we check the value of the x, y coordinates. If x,y coordinates are positive, the vehicle is considered to have a direction 1. If x is negative y is positive, then the vehicle have a direction 2. If x,y are both negative, the vehicle have a direction 3. If x is positive and y is negative, the vehicle has a direction 4. The direction model is shown as Figure 2.

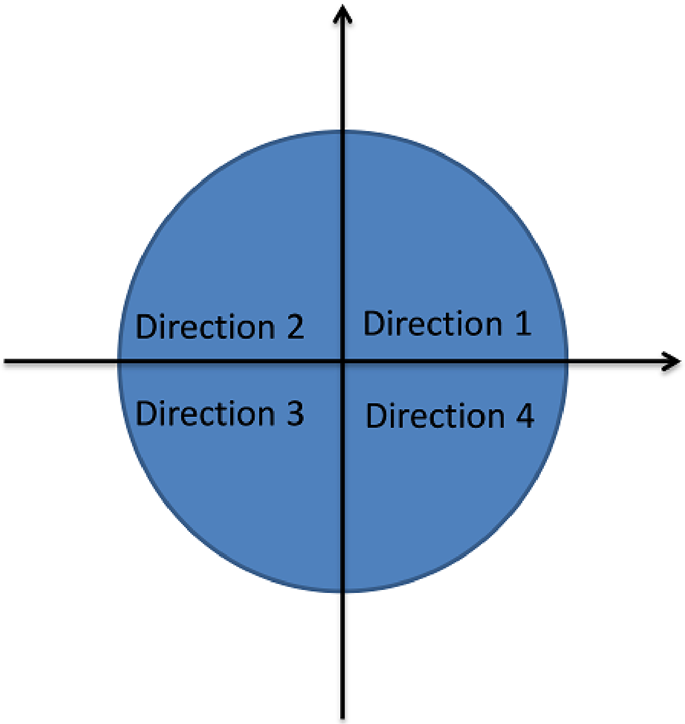

Figure 2: Direction Model.

Just as AOMDV, SD-AOMDV also uses RREQ and RREP messages for route discovery except that SD-AOMDV adds three new fields to the AOMDV's RREQ packet structure: SrcDir, SrcSpeed and SpeedMetric and adds 4 new fields to the AOMDV's RREP message: SrcDir, AvgSpeed, SpeedMetric and DestDir. Table 1 shows the RREQ packet of SD-AOMDV. Table 2 shows the RREP packet of SD-AOMDV.

Table 1: SD-AOMDV RREQ message

Source sequence number	SrcDir
Hop Count	SrcSpeed
Destination Sequence number	SpeedMetric

Table 2: SD-AOMDV RREP message

Source IP addressr	Hop Count
Destination IP address	SrcDir
Destination Sequence Number	AvgSpeed
Last_hop	SpeedMetric
First_hop	DestDir

For the routing table entry three new fields are added: AdvertisedSmetric, DestSpeed and DestDir. In the route list where list of paths for each destination is stored, SD-AOMDV adds Speedmetric field to the original list.

SD-AOMDV is an on-demand routing protocol which means a route discovery process will only be done when it is required. In the discovery process, source node broadcasts the RREQ packet. Initially, the SpeedMetric field is set to 0 and SrcDir and SrcSpeed is set to the current direction and speed of the source.

If a node that is not the destination node receives the RREQ package, it will implement a reverse path from the node to source and checking the routing table to find an available path from the node to the destination node. If the path exists, the node will then check if it has the same direction as the source and/or destination to see whether it can be an intermediate node. If it can, it will create an RREP packet and calculate the speed metric for the selected forward path and average speed of the source node as well as the destination node and update the SpeedMetric field and AvgSpeed field in the RREP message. Then the node will send the RREP message back to the source using the reverse path it established. If there's no route between an intermediate node and the destination node, the intermediate node will rebroadcast the RREQ packet after update the SpeedMetric field.

When the destination node gets the RREQ packet, it then also establishes a reverse path from the node to the source and sends back a RREP packet with the SpeedMetric field equals to 0. When a RREP packet is reaches an intermediate node, the node will first check whether it is heading to the same direction as the source and/or destination. If it does not, it will drop the packet. Otherwise, the node will compare the SpeedMetric field value in the RREP package to the difference between the speed of its own and the SpeedMetric field value in the RREP package and create a new RREP packet with the SpeedMetric field to the larger value. If different link-disjoint paths share the same node, the node will check whether there are any unused reverse paths to the source. If there are, the node will forward the RREP packet along one of such path. If there are not, the node will discard the packet. When a source node receives an RREP packet, S will select a forward path according to the SpeedMetric field and hop count value.

By introducing the new parameter, SD-AOMDV is more suitable for the rapidly changing VANETs topology. By several experiment researchers conducted, SD-AOMDV has a higher performance than AOMDV under different scenario.

2.3 An Improved GPSR Routing Strategy [Hu12]

GPSR is one of the most popular position-based protocols for VANETs. The protocol selects the intermediate nodes to forward the packet by the greedy algorithm that each time select the nodes that are nearer to the destination as intermediate nodes. If there's no node that is close to the destination, the protocol uses perimeter forwarding to route packets. GPSR protocol assumes that the vehicle geographical information can be obtained by GPS devices. GPSR is a stateless protocol. It only needs to keep the information of its 1 hop neighbors. The greedy scheme of GPSR to select the route is based on the position information of the neighbors. However, in VANETs nodes are rapidly moving and the position information is constantly changed. A selected intermediate node may be out of the transmission range after a short period and the routing process would fail. And also holding the out of date position information will not guarantee that appropriate intermediate node to be found.

An improved strategy for GPSR has been proposed recently. It aims at keeping the position information more up to date. In GPSR, a node will constantly sending a Hello packet to its neighbors to exchange the location to them. In the improved scheme, Hello packets are also sent constantly, however the packet format is different. The Hello packet format for the improved GPSR is shown in Table 3.

Table 3: Hello packet format for improved GPSR

PF	ID	x0	y0	Vx	Vy	VD	p	TS

PF is the priority flag with value 0 or 1. ID is the identity. X0 and Y0 is x, y coordinate of the current node. Vx and Vy is the velocity of the node in x, y coordinate when the packet is generated. VD is the vehicle direction and p is the number of the neighbor nodes. TS is the time flag indicating the time this message is generated. When a node receives the Hello message, it can use this information to calculate the current position of the source node. Suppose the current coordinate of the position of a node is (Xc, Yc), then:

$$X_t = X_0 + (t - t_0) * V_x$$

$$Y_t = Y_0 + (t - t_0) * V_y$$

If a neighbor's current position is out of the transmission range, it will not be a neighboring node. In the routing decision process, more up to date position information can be used. When packet is forwarded, if a node in the selected path is moving in the opposite direction towards destination node, the transmission may fail due to the node is soon out of the transmission range causing packet loss. In the improved GPSR scheme, a more refined next hop selection strategy is applied. That is where the priority flag come into used. The node forwarding the packet will set priorities to its one-hop neighbors based on their location information, speeds and directions. A one-hop neighbor will have the priority of 1 if it is heading towards the destination node and the relative speed between the neighbor and the current node is no more than 10m/s. Otherwise, it will have a priority of 0. The next-hop probability of the nodes is calculated as follow:

$$prob_{dist} = abs \frac{|D - S| - |S - M|}{|D - S|}$$

$$prob_{speed} = abs \frac{speed_{max} - speed_{|S-M|}}{speed_{max}}$$

where S is the position of the source node, M is the position of the potential next-hop node, D is the position of the destination node. The node with the highest probability will be chosen as the next-hop node. If there is no node with priority of 1, the nodes will have an equal possibility of being chosen as the next-hop node.

If the greedy scheme above fails, instead of using perimeter scheme, the improved GPSR uses a technique where the packets will be stored at the moving nodes and wait for the opportunities to be forwarded. When the node is unable to find the suitable intermediate node the packet will be sent to a selected subset of nodes which keeps track of all the nodes. The packets will be stored until an appropriate next hop node is found or time-to-live gets expire.

This improved GPSR scheme have a higher packet delivery ratio and less routing overhead comparing to the traditional GPSR and AODV routing scheme.

As we can see, both SD-AOMDV and the improved GPSR routing protocol modify the parameters in the old version adding new parameters to more precisely represent the state of the vehicle. This is due to the VANETs characteristics: the instability of the network topology and variety of the network environment. Any routing protocol that is designed for better routing scheme for VANETs should be suitable for these characteristics. As we can see from the recent study that trends for the recently proposed routing protocol for VANETs is try to more fit in the VANETs environment thus developing more efficient routing strategy. However, for a network, during the transmission of data, we have to guarantee the integrity and accuracy of the data. Especially for a network like VANETs, some of the data is about life and death. The security of VANETs is also a very big topic in the VANETs researching area. In the next section, we are going to introduce the recent advances for the security of VANETs.

3 Security in VANETs

The security issues in VANETs are very important aspect of the VANETs research. Some of the application based on VANETs is safety-related, it concerns with driver's safety. Other application is comfort-related which aims at providing convenience and comfort to the driver and passenger on the road. No matter what type of the application is, correctness and reliability of the information must be guaranteed, especially for safety-related applications. Due to the nature of the VANETs, there are several attacks that can be encountered [Kim13]: Sybil attack where 1 node sends several messages to other nodes with forged identity. It aims at causing a traffic jam in 1 route and causing the driver to take another route; denial of service attack where it attack the communication medium so that it causes channel jam and preventing the vehicles in the network from accessing the network service. This kind of attack is very severe in VANETs, especially in safety-related application where life critical information must reach the destination on time; the privacy attack where it tries to obtain the sensitive information about the driver and vehicles in the network such as the identity of the driver and location of the vehicles; data trust attack where it alters the original data and makes it inaccurate; replay attack where it retransmit some earlier information. This kind of attack may confuse the authorities and hide the id of the vehicles under certain situation such as hit-and-run incidents. There are other types of attacks that can happen in VANETs however the solutions for strengthen the security of VANETs to avoid certain attacks have been proposed constantly. In this section, we are going to introduce to recently proposed solution to eliminate VANETs security issues.

3.1 A Defensive Mechanism for VANETs in Game Theoretic Approach [M. 13]

The general VANETs security strategy is certificate authority mechanism as shown in figure 3 where CA is certificate authority which is responsible for registration of the vehicle and issuing keys and vehicular node registers with CA to get its ID and key. Game theory has been used for the VANETs for sensing the attack action. However it is not enough for the VANETs security requirements. This recently proposed mechanism is aimed at generating an appropriate security framework with support of defensive mechanism to for VANETs to enhance VANETs security.

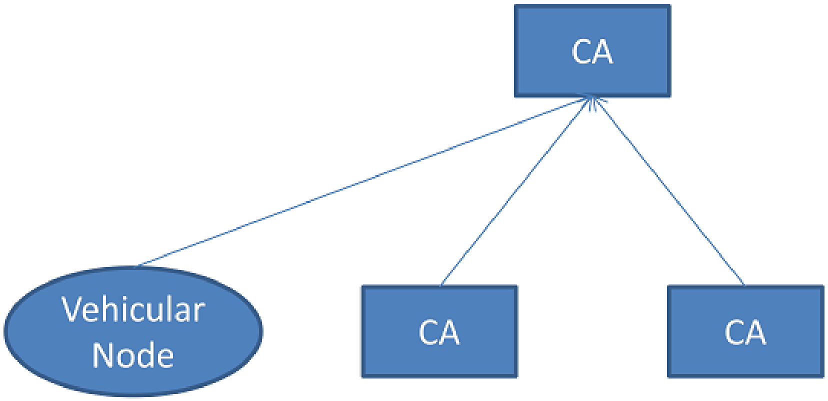

Figure 3 certificate authority mechanisms

In this defensive mechanism in game theoretic approach using heuristic based ant colony optimization (DMGTA), there are 3 processes: 1. identify the known and unknown opponents using heuristic based ant colony optimization. Known opponents are identified based on the information in the road network path and unknown opponents are identified by exploring the new road path with traversal of ants. 2. Involves Nash Equilibrium to identify the equilibrium state of all the players to determine the appropriate model for a given security problem. 3. Apply the defensive mechanism in game theoretic model if there's any suspicious procedure of optimal exploitation. Figure 4 shows the architecture of the DMGTA. In figure 5, multiple players are identified using heuristic ant colony optimization. Then the equilibrium state of all the players is specified by NE. Then the defensive mechanism is applied.

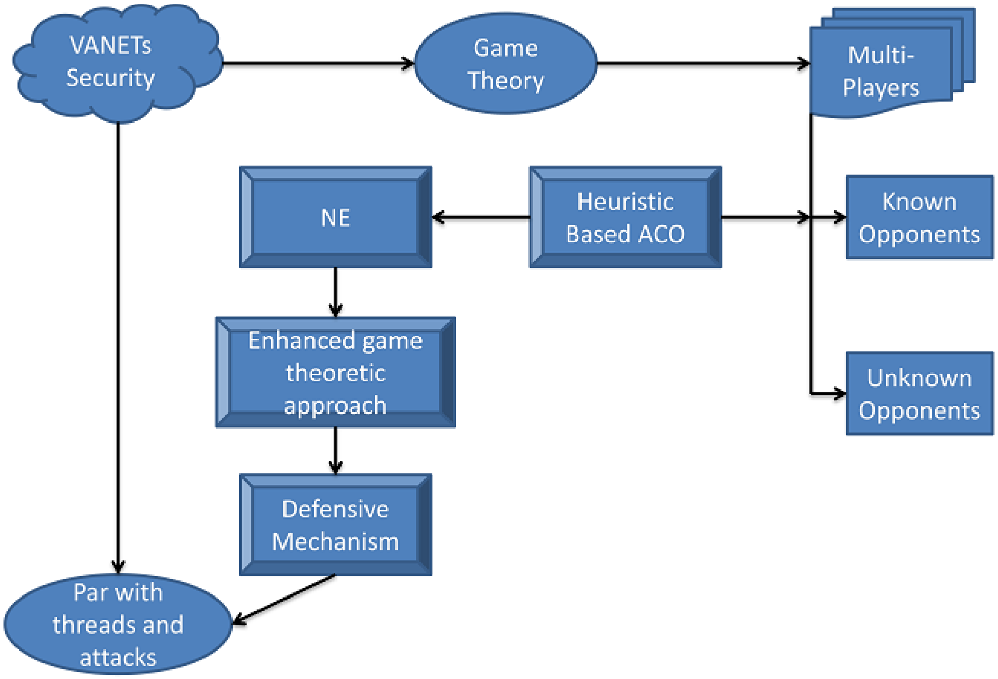

Figure 4 the architecture of DMGTA

In the first process, the game matrix is defined by the centrality measures and the permanent scalar indicating the risk or penalty of capture for the attacker. The centrality measures are done by mapping the vehicular networks to the underlying road topology, for road network is fixed and does not change. In the heuristic based ACO, vehicular nodes drive out ants to drop the information regarding the offensiveness of other nodes. Then after a pheromone principle process 1 node may extend the legitimacy of another node thus all the information available to the network can captivate a learned choice in an optimized way. When a node becomes part of a VANET it examines the information of other nodes. Then it sends the examined information back to certificate authority. The CA based on this information may conduct non-repudiation and banishing some nodes from the network. Ants can also be transmitted out to allocate the information for a particular node. Then all the nodes relying on these ants will make the decision of that node.

In the second process, nash equilibrium is established. A NE is a collection of strategies of the game where if each player in the game has chosen a strategy, there's no beneficial if only one player change its strategy while other players' strategies remain unchanged. It is useful for enhancing VANETs security where multiple players participate in the game. The game model derived after identifying equilibrium states can effectively enhanced the security of the VANETs.

After the 2 process, a defensive mechanism can be applied for further ensuring the security of the VANETs. There are 3 common classes of attacks. One class is to jam or interrupts the transmission of a region. This kind of attack can be monitored untimely by users or other defensive forces. Attackers can be recognized by triangulation techniques. Another class of attacks involves transmission of forge message. This kind of attack can also be effectively prevented using existed defense systems. The third class is the attackers sending message under forged identities. Deploying suitable local defensive system can also assist in monitoring the attacks and recognize the attackers.

By the experiment conducted by the researchers, DMGTA derives the game model that is more effectively ensure the security of the VANETs by any other existed security model.

3.2 A New Certificate Revocation Mechanism for VANETs [Samara12]]

Certificate revocation happens when a problematic certificate is found. It revokes the certificate which avoiding other vehicles receiving the message from these problematic certificates. Currently, Road Side Unit (RSU) is responsible for tracking the vehicle and revoking of the certificates by broadcasting Certificate Revocation List (CRL). However, the current strategy will cause high overhead on RSU and CRL will cause control channel consumption. In 2012, there's a new proposed mechanism is designed for better and fast revoking certificates strategy.

In the new certificate revocation method, when a vehicle receives a message, it will check the sender's certificate validity. If the sender does not have a valid certificate (VC), the message will be ignored. Moreover, if the sender does not even hold a certificate, the receiver will report the sender to RSU. RSU will check the correctness of the message. If it is correct, RSU will assign a VC to the sender. Otherwise, RSU will give an invalid certificate (IC) to the node, and register the vehicle's id to the CRL. Figure 5 shows the message checking process. In figure 5, 1 shows car 1 discovers car 2 has an IC by receiving a packet from car 2. 2 indicate that car 1 then broadcast a warning to the neighboring cars as well as the nearest RSU. Process 3 shows RSU then informed other RSUs. 4 shows the process that other RSUs then broadcast the warning to the cars that is within its range.

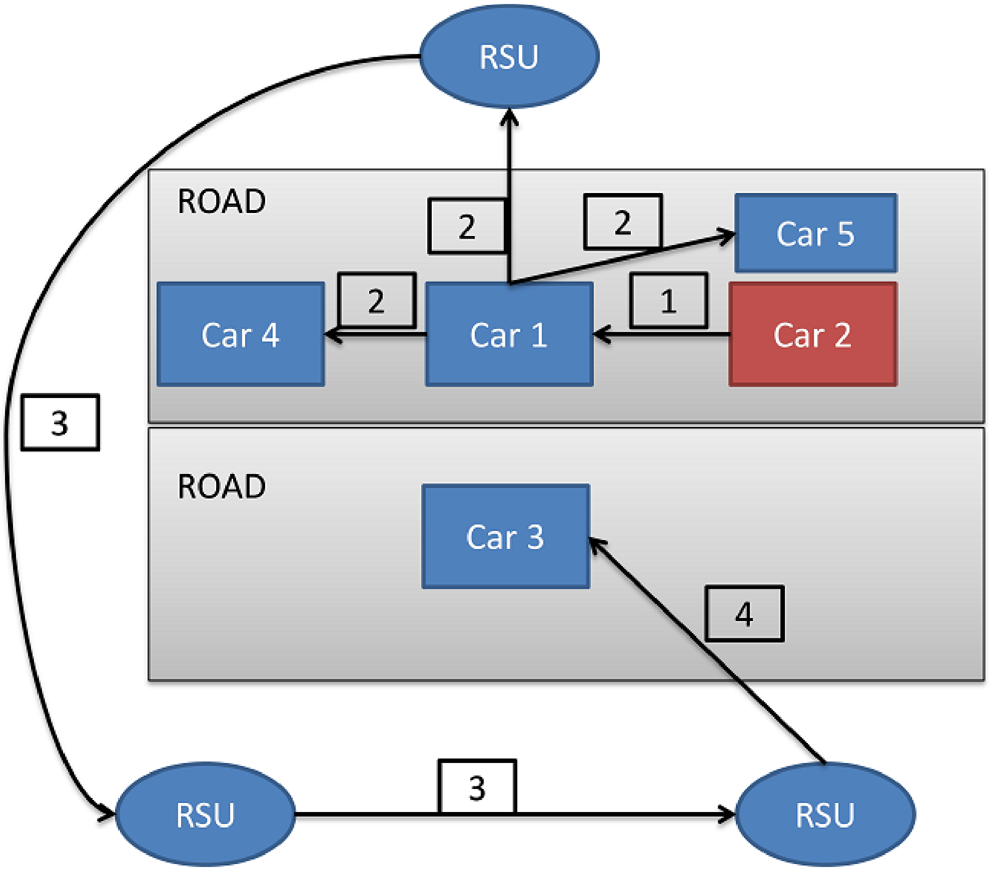

Figure 5 message checking process

The certificate revocation happens when a vehicle having VC behaves inappropriate. RSU will then replace the VC with IC. The certificate revocation will be taken place when more than 1 vehicle report to the RSU that a VC issued vehicle sending the incorrect data. Figure 6 shows the certificate revocation procedure. In figure 6: 1. Car A, B, C suspect of car V. 2. Car C, A, B sends the accusation message to RSU 3. RSU send the accusation message to CA 4. CA orders RSU to remove the certificate 5. RSU removes the certificate and assign an IC.

The process of revocation is as follows: When a receiver receives a message from an untrusted vehicle, the receiver then sends a message to RSU to obtain Session Key (SKA). RSU then reply the receiver with the SK Reply (SKR) which includes the SK to the current connection. SK is to prevent forging messages between the two communicating vehicles. Then the receiver sends a Validity Message which will inquiry the RSU whether the suspected vehicle has VC. RSU then replies to the receiver the sender whether has a VC.

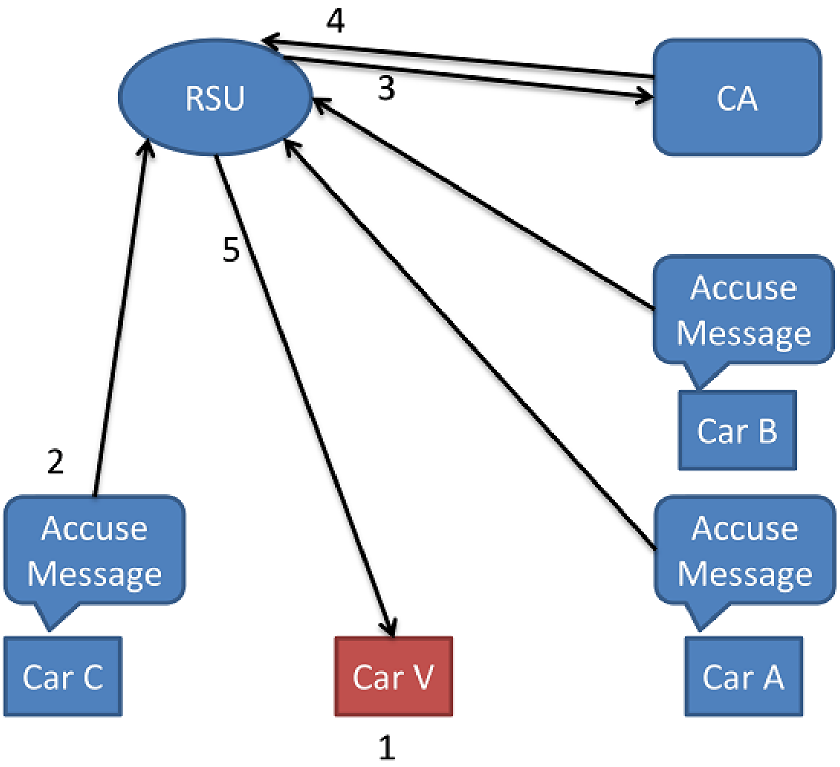

Figure 6 certificate revocation procedures

Every message is classified into categories; every category has a unique code. For example, the intersection collision warning has a code 001. When a vehicle received a data with the same code with other message but has a different data, this message will be viewed as a bogus message. Receiver receiving such message will sends an Abuse Report (AR) to RSU. The AR contains the sender's id, message code and the receiving time. RSU will forward the AR to CA, if more than 1 vehicle in the same area sends the AR about the same vehicle. If half the vehicles in the same range send an AR about the same vehicle, RSU will make a Revocation Request (RR) to revoke VC of the sender. CA will ask RSU for revocation after checking the RR and updating the CRL. RSU then revokes VC of the sender by assigning an IC.

In the common mechanism, each vehicle has to store approximately 25000 certificates. Each certificate is about 100 bytes. Total 2.5 mb is required to for 1 vehicle. The CRL size will be very big. In the proposed mechanism, the adversary vehicles will have a VC or IC to indicate whether it is a trusted node and the size of CRL will be reduced by 90%. This mechanism provides faster and more efficient distribution and adversary recognition for VANET.

Security issue for VANETs is a very important topic, for some of the VANETs application is safety-related. The accuracy and integrity of the information have to be guaranteed. This section we introduced 2 recently proposed mechanism for improving VANETs security. DMGTA uses the game theory and heuristic based ant colony optimization to generate more secured security framework with the support of defensive mechanism. The security framework generated by DMGTA approach is more specific to the situation of the current network and will detect the suspicious action more efficiently. In the second propose, the current certificate revocation mechanism has been improved to reduce the size of the data making it a more efficient security mechanism for VANETs.

4 Summary

VANETs have been very popular during recent year. It provides all kinds of possibility for road service application. Due to VANETs unique characteristics, it has to develop its own protocol and mechanism to support the network. VANETs routing protocol has been developed over years, and there are many routing protocols for VANETs that have already been widely used in the industry. However, the existed routing protocols are not really suitable for the characteristic of VANETs. There are still many new routing protocols have been proposed in the recent years. SD-AOMDV is an improved version of AOMDV introducing the speed and direction parameters. When calculating the routes, these parameters can help to acquire the more precise state of each node in the network thus providing the more efficient routes. In the improved version of GPSR, it introduces a new version of hello packet with priority flag, direction, speed and traffic density, so every node can predict the future movement of other nodes. The route selection is based on the priority flag of each node and also buffers the packet and reforward later if greedy approach failed. This approach also gets the more precise information of each node thus a more appropriate route is calculated. In fact, many recently proposed routing protocols for VANETs are a modification version of the existing ones. By introducing more parameters, the routing protocol can predict the network topology changes over times. VANETs cannot use only one routing protocols by the different traffic environment. Each area should use the routing protocol that is the most suitable for its traffic condition. The vehicles can have a negotiation process to determine what kind of protocol is using currently.

The security of VANETs is also a big issue, because VANETs application affects the safety of the driver and the passengers. There are many kinds of attacks that can happen in VANETs. To guarantee the security for VANETs is a big challenge. DMGTA is a newly proposed mechanism using game theory to identify the suspicious action in the network. Nash Equilibrium model is applied for identify the most suitable security model for the current network and also a defensive mechanism is supported. DMGTA generates the security framework for VANETs that is more secured than the existing security framework. Also in the recent research, the common mechanism certificate revocation in VANETs has been improved, instead of each vehicle stores thousands of certificates; it identifies other vehicle by valid certificate or invalid certificate. The broadcast of CRL is more efficient, thus allowing efficiency and security. VANETs security has been so important, however many proposed security solutions cannot effectively solved the security issues. A security frame work of VANETs not only should prevent the potential attacks but cannot add too much overhead to the transmission packets affecting the transmission efficiency. More standard should be proposed regarding to the VANETs security for the development trend of VANETs is to merge with cloud computing where security is even more important.

VANETs now are one of the important topic In MANETs areas. The development of VANETs has never been stopped over recent years. As the VANETs have become more and more complete, it will then been widely used for the road services in the future.

5 List of Acronyms

ACO	ant colony optimization
AODV	Ad hoc On-Demand Distance Vector Routing
AOMDV	Ad hoc on-demand multipath distance vector routing
AR	Abuse Request
CRL	Certificate Revocation List
DMGTA	defensive mechanism in game theoretic approach using heuristic based ant colony optimization
DTN	Delay tolerant network protocol
GPSR	Greedy Perimeter Stateless Routing
IC	Invalid Certificate
MANETs	mobile ad-hoc networks
RR	Revocation Request
RSU	Road Side Unit
VANETs	Vehicular ad-hoc networks
VC	Valid Certificate

6 Reference

1. [Maowad12] Hafez Maowad, Eman Shaaban, "Enhancing AOMDV routing protocol for V2V communication", In Proceedings of the 6th international conference on Communications and Information Technology, World Scientific and Engineering Academy and Society (WSEAS), 2012, P 20-27, http://dl.acm.org/citation.cfm?id=2209535.2209538
2. [Hu12] Hu, Lili; Ding, Zhizhong ; Shi, Huijing; "An Improved GPSR Routing Strategy in VANET", Wireless Communications, Networking and Mobile Computing (WiCOM), 2012, P1-4, http://ieeexplore.ieee.org/xpl/abstractReferences.jsp?arnumber=6478416
3. [Altayeb13] Marwa Altayeb, Imad Mahgoub, "A Survey of Vehicular Ad hoc Networks Routing Protocols" International Journal of Innovation and Applied Studies, 2013, P 829-846, http://www.issr-journals.org/xplore/ijias/IJIAS-13-122-09.pdf
4. [Paul11] Bijan Paul, Md. Ibrahim, Md. Abu Naser Bikas, "VANET Routing Protocols: Pros and Cons", 2011, P28-34, http://arxiv.org/ftp/arxiv/papers/1204/1204.1201.pdf
5. [M. 13] PRABHAKAR M., Dr. J.N. SINGH, Dr. MAHADEVAN G., "DEFENSIVE MECHANISM FOR VANET SECURITY IN GAME THEORETIC APPROACH USING HEURISTIC BASED ANT COLONY OPTIMIZATION", 2013, P1-7, http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6466118
6. [Samara12] Ghassan Samara, Wafaa A.H. Ali Alsalihy, "A New Security Mechanism for Vehicular Communication Networks", International Conference on Cyber Security, CyberWarfare and Digital Forensic, 2012, P18-22, http://arxiv.org/ftp/arxiv/papers/1207/1207.0967.pdf
7. [Kim13]Yeongkwun Kim, Injoo Kim, "Security Issues in Vehicular Networks", Information Networking (ICOIN), 2013,P468-427 http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6496424
8. [Khan13] Khan, Amjad; "Minimization of Denial of services attacks in Vehicular Adhoc networking by applying different constraints". International Journal of Academic Research in Business and Social Sciences, 2013, P662-684 http://hrmars.com/hrmars_papers/Minimization_of_Denial_of_services_attacks_in_Vehicular_Adhoc_networking_by_applying_different_constraints1.pdf
9. [Gerla11] M. Gerla, L. Kleinrock, "Vehicular networks and the future of the mobile internet". Computer Networks ,2011, P457-469, http://www.sciencedirect.com/science/article/pii/S1389128610003324

Last Modified: December 10, 2013
This and other papers on latest advances in computer networking are available on line at http://www.cse.wustl.edu/~jain/cse570-13/index.html
Back to Raj Jain's Home Page