IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 11, November 2015

A survey on Security based data dissemination for VANETs

C. Kiruthika[1], Ms. N. Gugha Priya[2]

PG Scholar, Department of Computer Science and Engineering, KIT-Kalaignar Karunanidhi Institute of Technology, Coimbatore, India[1]

Assistant Professor, Department of Information Technology, KIT-Kalaignar Karunanidhi Institute of Technology, Coimbatore, India[2]

Abstract: Vehicular Ad hoc Networks (VANETs) are the hopeful approach to offer safety and other applications to the drivers and customers. A lot of works have been completed towards it but security in VANET is still challenging. Data dissemination is the basic process in vehicular ad hoc networks (VANETs). Data dissemination is used to improve the quality of driving in terms of time, distance and safety. That is, after an accident or jamming is identified by the corresponding sensors build up on the vehicles, an alert message should be quickly disseminated to the vehicles moving towards the affected areas. The limited characteristics of VANETs are high mobility of vehicles, alternating connectivity, and dynamic topology. These following characteristics make data propagation tricky. In this paper, a survey on trust based data dissemination for VANETs is presented. This paper provides a detailed idea about how to securely disseminate the message between vehicles within a time.

Keywords: Vehicular ad hoc networks, Data dissemination, Epidemic routing, VADD.

I. INTRODUCTION

Nowadays, to assist enhanced road protection and console driving, to a greater extent vehicles are prepared with wireless devices and different types of sensors. Vehicular networks are the source for various applications presented in intelligent transportation system; Enchanting gain of this application, arriving vehicles will be knowledgeable in progress of accidents and the drivers may geta new path or suitable measures. Approximately 1.2 million public were took life every year on the road accidents. Road traffic protection has been the difficult issue in travel management. A potential approach is to present the traffic information to the vehicles so that they can use them to analyze the traffic environment. It can be attained by exchanging the information of traffic situation with vehicles. All the vehicles are movable in natural history; hence a portable network is required which can be self organized and able to working with no infrastructure support. With the development of microelectronic technology, it becomes feasible to incorporate node and network mechanism into distinct unit and wireless interconnection, i.e. ad hoc network. The communication between vehicles is unplanned where communications are done between various infrastructure and cars. Today's vehicles are become a smart car with assistance from wireless communication technology. Smart cars are fully prohibited software devices. As shown in Fig. 1, In a classic VANET vehicles are set with three different devices namely On Board Unit (OBU), Sensors, Tamper proof device (TPD). On board unit is a one device which is built-in the car. This OBU is able to communicating with additional vehicles and road side infrastructure. Sensors are used for sensing principle and to compute their status of the car. TPD is a security mechanism locates in the vehicle. It consists of much information of the vehicles such as battery life, timepiece synchronization. It obtains on only by the creative owner. Road side units organized near by the roads. Road side unit and on board unit are endlessly communicating with each other via communication protocols.

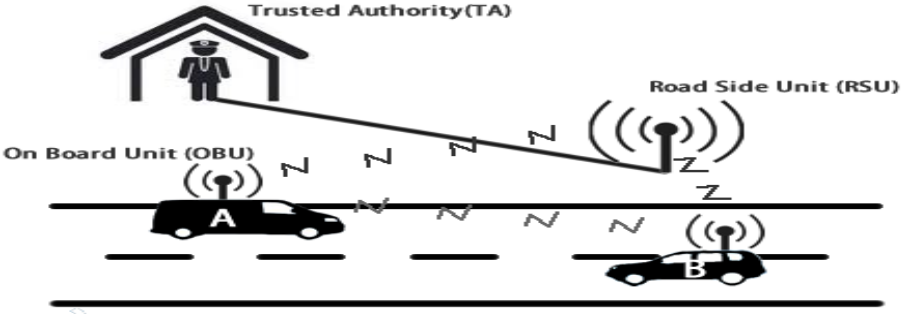

Fig.1. Components of VANETs

DOI 10.17148/IJARCCE.2015.41159

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 11, November 2015

During the registration of each and every vehicle trusted authority (TA) allocates a valid identity and tamper proof device launch password also offer a license plate number to all vehicles. When vehicle initiates the driver enters the valid identity and password into tamperproof device to activate it. If the identity andpassword are faulty the tamperproof device declines to do additional action.

VANETs are formed by applying the principles of MANETs, in which all node i.e. vehicles can pursues traffic law with high speed. VANETs support two types of communication: vehicle - to- vehicle (V2V) and vehicle-to-infrastructure (V2I).V2V can provide a data exchange platform for the drivers to share information and warning messages, so as to extend driver assistance. V2I is another useful research field in VANETs. V2I communication enables real-time traffic or weather updates for drivers and provides environmental sensing and monitoring. By using these technologies, stakeholders envision many eSafety applications that will enhance traffic safety. Vehicle-to-broadband cloud communication also available in VANETs, it means that vehicles can communicate via wireless broadband systems such as 4G/3G.

Several protocols have been developed in VANETs specially for clustering such as Predictive clustering, Back-bone based clustering, MAC based clustering, Traditional clustering, Hybrid clustering, Secure clustering. In this paper, we discussed about the different techniques and existing routing protocols for data dissemination in VANETs.

II. LITERATURE REVIEW

A. FACT framework

Karim Rostamzadeh, Hasen Nicanfar, Narjes Torabi, Sathish Gopalakrishnan, and Victor C. M. Leung [1] described about a routing, security and trust mechanisms. They have proposed a trust-based framework for secure and trustworthy data dissemination in VANETs. The framework consists of two modules. One applies the three safety checks to build sure the message is trusted. The security measures are, i) originated from a trusted region and traversed a trusted path; ii) It was not under attack on its path; and iii) It has a valid content.Second looks for a not dangerous path. Technique used was FACT framework, is based on carry-and-forward data diffusion. The solution provided was, FACT gives network designers a complete package which delivers honest messages through a harmless path with elevated trustworthiness and in a little quantity of occasion.

B. Epidemic routing protocol

A. Vahdat and D. Becker [2] described about the techniques to deliver messages in the case where there is nevera connected path from source to destination or when a network partition exists at the time a message is originated. They have proposed a Epidemic Routing protocol relies upon the transitive distribution of messages through ad hoc networks, with messages eventually reaching their destination, where random pair-wise exchanges of messages among mobile hosts ensure eventual message delivery. The goals of Epidemic Routing are to: i) Maximize message delivery rate, ii) Minimize message latency, and iii) Minimize the total resources consumed in message delivery.

Epidemic Routing delivers 100% of messages with reasonable aggregate resource consumption for scenarios where existing ad hoc routing protocols are unable to deliver any messages because no end-to-end routes are available.

C. Vehicle-Assisted Data Delivery protocols

Jing Zhao and Guohong Cao [3] described about the problem of proficient data delivery in VANETs. They have proposed a vehicle-assisted data delivery (VADD), which is based in the scheme of caching techniques and carry and forward, where nodes carry the packet when routes do not be present and forward the packet to the latest recipient that moves into its locality. There are many protocols being proposed, the Hybrid probe (H-VADD) protocol is the best between those protocols. The proposed VADD protocols give best performance in terms of data packet delay, protocol overhead and packet delivery ratio. And also effortless solutions can be based on the conventional vehicle mobility.

D. Data-Centric trust establishment framework

Maxiumraya, Panospapadimitratratos, Virgil D. Gligor and Jean-pierreHubaux [4] described about the challenges of extending the conventional view of confidence to data-centric.They have proposed a data-centric trust Establishment framework. Using that framework, trust value of each individual portion of information is evaluated and interconnected but may be differing information are combined. Then their legitimacy is contingent by a decision component based on the Dempster-shafer theory. The Dempster-shafer theory is used to estimate information reports with related trust levels. This theory enhances both data-centric and ephemeral.

E. Trust-based On-demand Multipath routing

X.Li, Z.Jia, P.Zhang, R.Zhang, and H.Wang [5] described about the packet forwarding ratio to evaluate a node trust and a sustained result of node trusts to estimate a path trust. They have proposed a protocols of, AODV, AOMDV and AOTDV, these protocols were capable of determine multiple loop-free paths as nominees in one route detection. Compared these three protocols, AOTDV improves packet delivery ratio and it is against multiple attacks from malicious nodes, including black-hole attack, modification attack, fabrication attack and impersonation attack. This protocol provides a feasible and flexible approach to decide a shortest path in a all path nominees.

F. Trusted Multi-hop Broadcasting Protocol

D. Tian, Y. Wang, H. Liu, and X. Zhang [6] described about authenticated, integrated, non-repudiated vehicular connections. They have proposed a multi-hop dissemination protocol called PMBP, PKI-based multi-hop dissemination protocol. That protocol presents the ECDCA-based key administration, message signing and verifying process and multi-hop dissemination system. And ECDCA (Elliptic curve discrete logarithm) applies

the public key size of 160 bits, the lesser key size suggests qualities of quicker computational efficiency with memory, energy and bandwidthinvestments. Two ID's were used namely, Electronic License Plate issue by a government or an alternatively an Electronic Chassis Number (ECN) issued by the automobile company. And it compares the waiting time of free space, shadowing and two-ray ground radio dissemination models.

G. Trust-extended authentication mechanism (TEAM)
M.-C. Chuang and J.-F. Lee [7] described about the verification method to guard legal clients from cruel attack They have proposed a decentralized trivial verification method called "TEAM".TEAM approves the idea of transitive trust relationships to progress the presentation of the verification process. TEAM assures the following safety necessities anonymity, location privacy, mutual authentication to guard spoofing attacks, forgery attacks, modification attacks and replay attacks as well as no clock synchronization problem, no verification table, fast error detection and session key agreement. Especially computation is fewer than in presented schemes because it only exercises an XOR function and a hash function.

S.NO	AUTHOR	DISADVANTAGES	ADVANTAGES	TECHNIQUES USED
1	KarimRostamz adeh et al.	Cost of technique and query traffic is high.	Low complexity, high scalability and efficiency.	FACT framework
2	A. Vahdat and D. Becker	It gives optimum delivery delay only when the data rate is very low.	Entire messages delivered using end to end routes.	Epidemic routing protocol
3	Jing Zhao and Guohong Cao	Multi-hop data delivery is difficult due to high mobility.	The protocol forwards the packet to the best road with the lowest data delivery delay.	Vehicle assisted data delivery protocols(L-VADD, D-VADD and H-VADD)
4	Maxiumraya et al.	Trust values are established in very specific way and cannot be generalized.	DST is highly data-centric and ephemeral.	DST, Bayesian inference and weighted routing.
5	X.Li, Z.Jia, P. Zhang,R.Zhang , and H. Wang	AOTDV does not provide tokens for the trusted third party.	Flexible and feasible approach to choose the shortest path.	Trust-based On-demand routing protocols (AODV, AOMDV and AOTDV)
6	D. Tian, Y. Wang, H. Liu, and X. Zhang	It is very simple for attackers to damage the system or cause accidents.	It provides authenticated, integrated, non-repudiated vehicular communications.	ECDSA(Elliptic Curve Digital Signature Algorithm)
7	M.-C. Chuang and J.-F. Lee	Asymmetric cryptography is not suitable.	Lightweight authentication scheme adopts the concept of transitive trust relationships to improve the authentication scheme.	TEAM(Trust-Extended Authentication Scheme)

Table 1.Comparison of different data dissemination techniques in VANETs

III. ROUTING PROTOCOLS

A routing protocol administrates the method that two communication vehicles exchange information; it includes the process in founding a route, assessment in forwarding, and act in maintaining the route or recovering from routing breakdown. The most common types of routing protocols in VANETs are unicast routing protocol, multicast routing protocol and broadcast routing protocol. Some routing protocols are,

A. AODV
In Ad Hoc on Demand Distance Vector (AODV) routing, upon receipt of a broadcast query (RREQ), vehicles trace the address of the vehicle distributing the query in their routing table. This process of tracing its preceding hop is called backward learning. Upon arriving at the destination, a reply packet (RREP) is then sent through the entire path achieved from backward learning to the source. At every stop of the path, the vehicle would trace its preceding hop, thus establishing the forward path from the source. The flooding of query and sending of reply establish a full duplex path. After the path has been established, it is maintained as long as the source uses it. A link failure will be reported recursively to the source and will in turn trigger another query-response procedure to find a new route.

B. DSR
Dynamic Source Routing (DSR) uses source routing, that is, the source specifies in a data packet's the sequence of midway nodes on the routing path. In DSR, the query packet duplicates in its header the IDs of the midway nodes that it has traversed. The destination then retrieves the complete path from the query packet, and uses it to respond to the source. As a result, the source can create a path to the destination. If we permit the destination to send several route replies, the source node may obtain and store several routes from the destination. A route can be used when some link in the present route breaks. In a network with low mobility, this is beneficial over AODV since another route can be tried before DSR initiates another

flood for route detection. There are two key differences between AODV and DSR. First, is that in AODV data packets hold the destination address, while in DSR, data packets hold the full routing information. This means that DSR has potentially additional routing overheads than AODV. As well, the diameter of the network increases, the quantity of overhead in the data packet will continue to increase. Second, is that in AODV, route reply packets hold the destination address and the sequence number, but in DSR, route reply packets hold the address of every node along the route.

C. VADD

Vehicle-Assisted Data Delivery (VADD) is a vehicular routing policy intended at improving routing in detached vehicular networks by the plan of carry-and-forward based on the use of expected vehicle mobility. A vehicle makes a conclusion at acrossroads and selects the next forwarding trail with the minimum packet delivery delay. A path is merely a divided road from an intersection. The predictable packet delivery delay of a path can be modeled and articulated by parameters such as road density, average vehicle velocity, and the road detachment. The minimum delay can be solved by a set of linear system equations. VADD variations such as, L-VADD, D-VADD and H-VADD decides the next forwarding node after the next forwarding lane.

Location First Probe: Location First Probe (L-VADD) would pick a node nearby to the next forwarding path even though such a node is disappearing away from the forwarding path.

Direction First Probe: Direction First Probe (D-VADD) would pick a node which is going to the forwarding path even though such a node might be further from the forwarding path than other nodes.

Multi-Path Direction First Probe: Multi-Path Direction First Probe (MD-VADD) would choose multiple nodes going toward the forwarding path so as not to miss forwarding to a node that offer a shorter time to the destination. Lastly, Hybrid Probe (H-VADD) merges L-VADD and D-VADD so the extended packet delay from D-VADD is offset by L-VADD and routing loops from L-VADD are covered by D-VADD. Comparing with L-VADD and L-VADD, H-VADD has the best performance.

D. DSRC

Dedicated short range communications are both one-way and two-way short-range to medium-range communication channels specifically designed for automotive use. DSRC protocol works in 5.85 to 5.92GHz band with bandwidth of 75MHz. Its approximate range is 1000 meter. The network should support both private and public data communication, that means both road side to vehicle communication and vehicle to vehicle communication in VANETs but higher priority is given to public communications. DSRC provides several channels for communications. Standards divide the channels into two categories: 1) Control channels and

2) Service channels.

Control channel is reserved for broadcasting and coordinating communications which generally takes place in other channels. Although DSRC devices are allowed to switch to a service channel, they must continuously monitor the control channel. DSRC systems can also be used to monitor adverse weather and hazardous conditions.

IV. CONCLUSION

In recent years VANETs becomes broadly used dissemination technology. This survey paper provides characterization of some existing data dissemination techniques with its advantages and disadvantages. We congregate data about how individual participants in traffic use the capability to deceive when being able to communicate between each other. Data dissemination requirements (delay, reliability, coverage, etc.) may be different from one application to another. Secure data dissemination in VANETs is of vital importance in ITS. Without security, minimizing the delay and maximizing the reliability could not be attained. Intelligent transport applications aim at providing faster delivery of traffic information, and improving the accuracy and efficiency of traffic detection.

REFERENCES

[1] Karim Rostamzadeh, Hasen Nicanfar, Narjes Torabi, Sathish Gopala krishnan and Victor C.M. Leung, "A Context-Aware Trust-Based Information dissemination framework for vehicular networks," IEEE Trans. Veh. Technol., vol. 2, no. 2, pp. 3974–3982, April 2015.

[2] A. Vahdat and D. Becker, "Epidemic routing for partially connected ad hoc networks," Duke Univ., Durham, NC, USA, Tech. Rep. CS-200006, 2000.

[3] J. Zhao and G. Cao, "VADD: Vehicle-assisted data delivery in vehicular ad hoc networks," IEEE Trans. Veh. Technol., vol. 57, no. 3, pp. 1910– 1922, May 2008.

[4] M. Raya, P. Papadimitratos, V. Gligor, and J.-P.Hubaux, "On data-centric trust establishment in ephemeral ad hoc networks," in Proc. IEEE 27th Conf. Comput. Commun. (INFOCOM'08), 2008, pp. 1238–1246.

[5] X. Li, Z. Jia, P. Zhang, R. Zhang, and H. Wang, "Trust-based on-demand multipath routing in mobile ad hoc networks," IET Inf. Secur., vol. 4, no. 4, pp. 212–232, Dec. 2010.

[6] D. Tian, Y. Wang, H. Liu, and X. Zhang, "A trusted multi-hop broadcasting protocol for vehicular ad hoc networks," in Proc. Int. Conf. Connect.Veh.Expo. (ICCVE), 2012, pp. 18–22.

[7] M.-C. Chuang and J.-F. Lee, "TEAM: Trust-extended authentication mechanism for vehicular ad hoc networks," IEEE J. Syst. vol. 8, no. 3, pp. 749–758, Jan. 2013.

[8] T. Gazdar, A. Rachedi, A. Benslimane, and A. Belghith, "A distributed advanced analytical trust model for VANETs," in Proc. IEEE GlobalCommun. Conf. (GLOBECOM), 2012, pp. 201–206.

[9] N. Haddadou and A. Rachedi, "DTM2: Adapting job market signalling for distributed trust management in vehicular ad hoc networks," in Proc. IEEE Int. Conf. Commun. (ICC), 2013, pp. 1827–1832.

[10] C. Liao, J. Chang, I. Lee, and K. K. Venkatasubramanian, "A trust model for vehicular network-based incident reports," in Proc. IEEE 5th Int.Symp.Wireless Veh.Commun. (WiVeC), 2013, pp. 1–5.

[11] S. Buchegger and J.-Y. Le Boudec, "Performance analysis of the CONFIDANT protocol," in Proc. 3rd ACM Int. Symp. Mobile Ad Hoc Netw. Comput., 2002, pp. 226–236.

[12]A. Das and M. M. Islam, "Securedtrust: A dynamic trust computation model for secured communication in multiagent systems," IEEE Trans.Dependab. Secure Comput., vol. 9, no. 2, pp. 261–274, Mar./Apr. 2012.

[13] D. Dolev and A. Yao, "On the security of public key protocols," IEEE Trans. Inf. Theory, vol. 29, no. 2, pp. 198–208, Mar. 1983.

[14] N. Wisitpongphan, F. Bai, P. Mudalige, V. Sadekar, and O. Tonguz, "Routing in sparse vehicular ad hoc networks," IEEE J. Sel. Areas Commun., vol. 25, no. 8, pp. 1538-1556, Oct. 2007.