ISSN No. 0976-5697

Volume 8, No. 5, May – June 2017

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

Review of Group Management Technique for Vehicular Ad-hoc Network (VANET)

Aditya K. Soni
Department of Computer Science and Engineering,
University Institute of Technology,
RGPV, Bhopal, India

Prof Raju Baraskar
Department of Computer Science and Engineering,
University Institute of Technology,
RGPV, Bhopal, India

Dr Rajeev Pandey
Department of Computer Science and Engineering,
University Institute of Technology,
RGPV, Bhopal, India

Abstract: Vehicular Ad-hoc Network (VANET) is emerging technology which is considered one of the key research area in security applications. This paper surveys advancements made in group based Vehicular Ad-hoc Network security technologies for future directions in group management technologies (GMT) and also various secure message transmission (SMT) amongst the groups. This paper also presents a review of architecture, related technologies, trends, applications in VANET technologies with major focus security Ad here once tools. Although offering significant services and devices, VANET based healthcare still faces major challenges and open research issues which are discusses in the paper as well.

Keywords: Vehicular Ad-hoc Network, SMT, Group management technology, Security technology, VANET

I. INTRODUCTION

A. Background

VANET is categorized as an ad-hoc networks that allows communication between nearby vehicles and between vehicles and fixed interface usually called as RSU (road side unit). The main goal of VANETs is to provide more security and comfort to the passengers. Accordingly, a spatial purpose electronic device is installed in each vehicle that allows connection to the other vehicles called as OBU (one board unit). Therefore, each vehicle equipped with the device acts as a node in the environment of ad hoc network and is also able to receive or send others messages through the network. These messages can be a text message, multimedia message or a security message, accident alert, entertainment, traffic observation, announcement of road sign, paying parking expenses, etc. These messages are helpful for the driver to select an appropriate route. In addition, multimedia and internet are embedded for passenger's facility. Paying tolls and parking expenses are other services of these networks. Today, various vehicle manufacturing companies have initiated different projects regarding such types of technologies and equipping their vehicles with VANET capabilities. VANET have currently attracted considerable research interest regarding wireless networking and vehicle industries. Relatively high flexibility, communication amongst the nodes (devices are considered as a node in some scenarios) in VANET enables an environment without an underlying structure and a highly dynamic network topology constantly change these networks .It can be considered as a component of intelligent transportation systems (ITSs).

As discussed, highly dynamic nodes and servers without a central station cause collisions in wireless VANET communications and packages are mostly lost or delayed. In such scenarios, simultaneous communication easily may fail.

VANETs involves different wireless technologies, including DSRC, which is a type of Wi-Fi, as well as WIMAX and cellular technology. Other short band wireless protocols, e.g., IEEE802.11, Bluetooth, and CALM could also be used in these networks.

B. Present Scenario:-

C. Caballero-Gil, *et al* defined group as "A group in a VANET is a set of vehicles that are located in a close geographic area whose formation is determined by the mobility pattern of vehicles. The group needs a minimum of vehicles and is managed by a given node called 'leader of the group'" [19]. Groups are proposed as a solution to decrease the number and size of packets exchanged among vehicles because by using groups, VANETs can be split in small sub-VANETs that allow to avoid sending the same information through different paths. In this way, we can improves the efficiency and safety of communications through a hybrid model that combines symmetric and asymmetric cryptography. There are many studies regarding grouping in VANETs.

GAP protocol based grouping and authentication is proposed to reduce the delay and lost messages. The node clustering methods are introduced, in which the node at the center of the group is considered as the leader node. These two methods do not specify the practical processes that nodes perform to manage the group and the collected information is not sufficiently reliable..

The usual way to provide an access control mechanism for the secure group communication is to employ a symmetric key, known as a group key, shared only by group members. Messages, encrypted by a member having a group key, can be decrypted by other group members having the same group key, which can guarantee secure group communication. Although this mechanism, using the shared group key, is an efficient way to guarantee security, it causes some difficulties

in maintaining an efficient key management system since the group key must be updated according to membership changes such as the user leaving or joining, which is referred to as rekeying. To reduce the key management overhead from the rekeying, a tree-based group key management (GKM) scheme has been extensively studied in the literature [3], [4],

II. VEHICULAR AD-HOC NETWORK:-

There are several types of vehicular network infrastructure are categorized in various categories but major categories are describes in [18] are described below:-

• Vehicle-to-Vehicle (V2V) ad hoc network: allows the linked vehicular communication that does not rely upon a fixed centralize infrastructure support. This type of VANET can be mainly used for enforcement of security, preserving safety and dissemination applications:-
• Vehicle-to-Infrastructure (V2I) network: allows a vehicle to establish link between road side infrastructure for information and data gathering applications.
• Hybrid architecture: This is the combination of both Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I). In such fashion RSU communicate in various fashion such as Single hoped network or multi-hope, i.e., if it can or not access directly the roadside unit. It also provides long distance connection to the Internet or to vehicles that are far away.

III. VANET CHARACTERISTICS

Both MANET and VANET have some common characteristic, self-organization, low bandwidth, self-management, no centralization node. But above that VANET has its own distinct characteristics that makes it more challenging then MANET, such as frequent disconnected network, highly dynamic, traffic density, mobility pattern of traffic flow etc. Here some of them are discussed.
High Mobility: The vehicle nodes in VANET move usually in high speed. Therefore it makes difficult to predict a node's position and protection of node privacy.
Mobility Prediction: VANET differs from other types of mobile ad hoc networks in which nodes move in a random way. Future position of vehicles can be predicted based on speed and street map.
Rapid Changing Network Topology: Due to high node mobility and random speed of vehicles, position of node changes frequently therefore network topology changes frequently.
Frequent Exchange of Information: Network collect information from other vehicles and RSUs because of its ad-hoc nature. Therefore information is frequently exchanged among nodes.
No Power Constraints: The power in VANET is not a critical challenge, because vehicles have the ability to provide continuous power to the OBU via the long life battery.
Time Crucial: The information in VANET must be delivered to the nodes with in time limit so that a decision can be made by node and perform accordingly.
High Computational Ability: Vehicles in VANET are equipped with sensors, processors, GPS, large memory capacity etc. which increases computation capacity of node which helps reliable wireless communication.

IV. APPLICATION:-

V2V and V2I communications allow the development of a large number of applications and can provide a wide range of information to drivers and travellers. Some of them are following:

- Warning about violating traffic signal
- Intersection collision warning
- Warning about blind merge detection
- Approaching emergency vehicle warning
- Post-crash warning
- Low parking structure and bridge warning
- Cooperative forward collision warning
- Emergency electronic brake lights (EEBL)
- Lane change warning.

V. LITERATURE REVIEW:-

Objective of my research is to classified VANET vehicles into the groups and manage with efficient group key generation algorithm that helps to reduce the key generation and management.

A group in a VANET is defined as a set of vehicles that are located in a close geographic area whose formation is determined by the mobility pattern of vehicles. The group needs a minimum of vehicles and is managed by a given node called "leader of the group". All vehicles forming part of a group have a direct wireless connection with the leader of such a group and share a secret key.

There are various approaches which defines the classification of the nodes, such as the clustering there are various issues related clustering and other grouping techniques.
Various authors recommends the use of groups or clusters, which are the same in VANETs [1] presents a theoretical analysis of a directional stability based clustering algorithm [2] Describes clusters where the leader is the node in the middle with the lowest identifier [3] Proposes clusters to maximize the advance of the relayed information and to avoid interferences, but the cluster head must know the exact positions of nodes in the cluster.

Importance of grouping is as much as the management of groups. No work is done or any process is define in detail that nodes have to complete for group management and do not show any of implemented scheme to demonstrate the reliability of obtained data . Groups will be used only when the conditions of the routes require it. Examples are dense traffic, traffic jams or congested highways, where the density of vehicles in a geographic zone causes that the number of communications is huge. But groups are formed before the number of nodes begins to degrade the network. Without any mechanism to minimize the number of communications, a simple broadcast will be launched from every vehicle generating a lot of unnecessary redundancy. The number of packets generated depends on the number of nodes in the network and interconnection among them. Therefore, it will be generated n packets for each data communications where n is the number of vehicles with On Board Unit (OBU) in the network (in the scope of interest). This number of connections is not extremely large, and perhaps would not need to taking steps to reduce that number, but some studies like [4] showing that many vehicles duplicate data packets

causing collisions in the information that is sent, which degrades communication quality.

Distinguish among several stages in group management, corresponding to different situations of vehicles, depending on the route and on their status in each moment. The stages are: Detection, Election, Creation, Membership and Life of a group [5, pp. 26-29].

There are various key management techniques are proposed for key management such as in terms of integrity-checking and authentication, well known and well accepted digital signature in conventional *public key infrastructure (PKI)* [6] is the choice. However, two problems as mentioned in [7] for vehicle to verify the signatures of other vehicles by itself. First, the OBU does neither have that much computational power nor it is strong enough to handle all verifications in a short time, especially in places where the traffic density is high. Second, message verification from an unknown vehicle involves the transmission of a public key certificate which causes heavy message overhead. Therefore, the general approach is to let the nearby RSU to help a vehicle to verify the message of another. The volume of signatures to be verified can be very huge (every vehicle is expected to broadcast a safety message every few hundred mili-sec [8]).

We need an efficient method for verifying a batch of signatures within a short period of time. Related problems have been addressed in some recent works [7, pp. 5-15]. In [9], the IBV protocol was proposed for vehicle-to-RSU communications. The RSU can able verify a large number of signatures in a forms batch with the help of just three pairing operation. However, such protocol have some limitations. First, this protocol majorly relies on a tamper-proof hardware device, installed in each vehicle, which preloads the system-wide secret key. If these devices are hacked, security of the whole system will be compromised. Second, anyone can trace the identity of sender, thus the privacy requirement is compromised. Third, the protocol has a flaw such that an anti-traceability attack and impersonation attack. Forth, if there exists any erroneous signatures, the whole batch is dropped. Conclusively, this protocol is not effective for V2V communication.

In a more recent work [7], the RAISE protocol was proposed for vehicle-to-vehicle communications. This protocol is software-based which allows a vehicle to check the signature of another with the help of a nearby RSU. However, drawback of this protocol is that the RSU has to verify signatures one by one it does not provide the batch verification. On the other hand, to notify other vehicles regarding the authenticity of a message (from a certain vehicle is authentic), 128 bytes hash value needs to be broadcasted. There can be millions of signatures within a short period of time, which induces a heavy message overhead. Although VANET allows unknown vehicles to broadcast safety message to one another, like other ad hoc network applications, there are scenarios (e.g. car racing, police patrolling, and tour travelling) which should allow a group of known vehicles to communicate securely among themselves. Wasef and Shen [10] considers such a secure group communications scenario but they only focus on how the group key can be updated.

How vehicles can form a group and how the initial group key can be established are not considered at all other recent efforts for making authentication in VANETs more efficient include. In [11], the authors propose to use the physical property of a transmitting signal to discriminate one transmitter from others because physical measurement is more efficient than software computation.

Wasef and Shen [12], on the other hand, aims at enhancing the efficiency of any certificate-based authentication scheme. The authors propose a HMAC-based solution to replace the time-consuming and traditional certificate revocation list checking process. Regarding conditional privacy preserving, some recent works [13] [14] propose to achieve the goal by using group signature schemes. That is, each vehicle in the system is assigned a group private key. When a vehicle wants to broadcast a message, it signs the message using its group private key. Verifiers such as RSUs can then verify its signature using a common group public key. In this way, a signature can be properly verified but at the same time, the real identity of the signer can be hidden. Only if necessary, a trusted party can use a private key to reveal the real identity of the signer. Though conditional privacy preserving can be achieved, we argue that such group signature schemes are complicated and inefficient. In terms of secure VANET applications, [15, 16] are two representatives. Lu et al. [15] proposes a secure navigation scheme for locating parking lots in a car park while Popa et al [16] proposes a secure and privacy preserving road toll calculation scheme under the principle of multi-party computation.

T.W. Chim et al described two Secure and Privacy Enhancing Communications Schemes are proposed for vehicular sensor networks (SPECS) [17]. This scheme can handle both types of communication ad-hoc messages and message sharing between the nodes of pre-formed group. Major advantages of this scheme are. First, scheme based on software that means it does not rely on any kind of special hardware. This scheme is also based on bilinear pairing as in [7]. Which helps to reduce the number of operations in the verification phase that's how it enhance the efficiency. Second, by sharing secrets with RSU and TA on the handshaking phase, a vehicle is permitted to use a different pseudo identity for each session (or message) to protect its privacy while only TA can trace the real identity of the vehicle. Third, this scheme uses the techniques of binary search in RSU message verification phase. To reduce the message overhead substantially they used bloom filter, which replaces hash values in notification messages that is how it enhance the effectiveness of the verification phase.

VI. ACKNOWLEDGMENT

As mentioned, one of the main challenges of VANETs is the optimal propagation of information. This paper is given a survey for particle swarm optimization based grouping and group key management; grouping reduces the number of communications, particularly in heavy traffic conditions, thus increasing the communication quality. In this paper, grouping is optimized using particle swarm optimization and using the proposed automatic management, it is predicted that the number of communications is considerably reduced and the communication quality is improved and Group key management technology also reduces the overhead of RSUs and simplifies the process of key generation and distribution.

VII. REFERENCES

[1] A. B. L. V. A. C. V. A. A. F. L. Felipe Domingos da Cunha, "Data Communication in VANETs: A Survey, Challenges," 15 Sep 2015.

[2] P. S. a. P. C. N. P. Fan, "Theoretical analysis of a directional stability-based clustering algorithm for vanets.," in Vehicular Ad Hoc Networks, 2008.

[3] B. W. a. H. P. G. Y. Gunter, "Medium Access Concept for VANETs Based on Clustering," in VTC Fall, 2008.

[4] Z. Y. Rawashdeh and S. M. Mahmud, "Media Access Technique for Cluster-Based Vehicular Ad Hoc Networks," in VTC Fall , 2008.

[5] C. C.-G. J. M.-G. a. C. H.-G. P. Caballero-Gil, "Flexible Authentication in Vehicular Ad hoc Networks,," in Proceedings of APCC IEEE Asia Pacific Conference , 2009.

[6] W. F. W. P. D. S. R. Housley, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile," in IETF RFC2459, 1999..

[7] R. L. X. L. P. H. X. S. C. Zhang, "An efficient identity-based batch verification scheme for vehicular sensor networks," in IEEE INFOCOM '08, April 2008.

[8] "Vehicle Safety Communications Project Report," National Highway Traffic Safety Administration US Department of Transportation, April 2006.

[9] X. L. R. L. P. H. C. Zhang, "RAISE: an efficient RSU-aided message authentication scheme in vehicular communication networks, in:," IEEE ICC , vol. 08, p. 1451–1457, May 2008.

[10] X. S. A. Wasef, "PPGCV: Privacy Preserving Group Communications Protocol for vehicular ad hoc networks," in IEEE ICC, May 2008.

[11] P. H. G. G. H. Wen, "A novel framework for message authentication in vehicular communication network," in IEEE GLOBECOM '09, December 2009.

[12] X. S. A. Wasef, "MAAC: message authentication acceleration protocol for vehicular ad hoc networks," in IEEE GLOBECOM '09, December 2009.

[13] S. V. S. B. B.K. Chaurasia, "Message broadcast in VANETs using group signature," in IEEE WCSN '09, December 2008.

[14] E. S. F. B. A. P. A. Studer, " TACKing together efficient authentication, revocation, and privacy in VANETs," in IEEE SECON '09, June 2009.

[15] X. L. H. Z. X. S. R. Lu, " SPARK: a new VANET-based smart parking scheme for large parking lots," in INFOCOM '09, April 2009.

[16] H. B. A. B. R.A. Popa, "VPriv: protecting privacy in location-based vehicular services," in USENIX Security Symposium, September 2009..

[17] S. Y. L. C. H. V. O. L. T.W. Chim, "SPECS: Secure and privacy enhancing communications schemes for VANETs," ELSEVIER-Ad Hoc Networks, vol. 9, pp. 189-203, 2011.

[18] A. B. L. V. A. C. V. A. A. F. L. Felipe Domingos da Cunha, "Data Communication in VANETs: A Survey, Challenges and Applications," hal-00981126v4, INRIA. 2014

[19] P. C.-G. J. M.-G. C. Caballero-Gil, "Using Groups to Reduce Communication Overhead in VANETs," in The Second International Conference on Advances in P2P Systems, 2010.

