Data Transmission in VANETS: A Review, Applications, Routing Protocols

Samiksha
PG Student
Chandigarh Engineering College
Landran , Punjab , India

Anit Kaur
Asstt. Prof., Department of CSE
Chandigarh Engineering College
Landran , Punjab , India

ABSTRACT
A novel kind of ad hoc network is defeating the roads: Vehicular Ad Hoc Networks. In these networks, vehicles communicate with each other and perhaps with a roadside infrastructure to provide a long list of requests varying from transit safety to driver support and Internet access. Security is a vital concern for many Vehicular Ad-hoc Network applications. One specific serious attack, known as Sybil attack, against ad hoc networks involves an attacker illegally claiming multiple identities. In these networks, information of the real-time position of nodes is a supposition made by most protocols, algorithms, and requests. This is a very reasonable assumption, since GPS receivers can be fitted easily in vehicles, a number of which already comes with this technology. In this method, each Road Side Unit calculates and stores different parameter values (Signal Strength, distance) after receiving the inspiration packets from nearby vehicles.

Keywords
Security, Roadside Units, GPS and Application of Vehicular Ad-hoc Network.

1. INTRODUCTION
In current years, Vehicular Ad-hoc Networks have attracted a lot of kindness from the research community. The main reason of research in VANET is to improve vehicle safety by Vehicle to Vehicle and Vehicle to RSU communication. For example, in the case of an accident, a VANET should be able to warn all imminent vehicles. Nodes share information using the wireless channel in VANET [1]. VANETs can be exploited for a broad range of safety and non-safety applications, allow for value additional services such as vehicle safety, automatic toll payment, traffic [11,12] management, improved navigation, location based services such as conclusion the closest fuel station, eatery or travel lodge and infotainment applications such as long as access to the Internet.

For instance, in the case of a coincidence, a VANET should be able to warn all approaching vehicles [13]. Nodes share information using the wireless channel in VANET. Malicious nodes take benefit of wireless communication environment for realizing the spoofing attacks. In such a condition, an attacker fakes its identity to deception as another node. Sybil attack is a spoofing attack in which an attacker can produce multiple identities either by forging, stealing or by using any other resources. Attackers use some or all of these identities [2] to fabricate information about traffic and/or event. An attacker can create an impression of traffic congestion to mislead neighbouring nodes. It can also insert false information in the network by using the identities of non-existing nodes.

2. OVERVIEW OF VANET
Vehicular networks permit [14] cars to communicate with each other and with a distinct infrastructure on the road. Infrastructures can be purely ad hoc between cars or facilitated by making use of an infrastructure. The organization typically consists of a set of so called roadside units that are connected to each other or even to the Internet [3].

VANET uses three systems: (1) Intelligent transportation systems (2) Vehicle-to-roadside communication and (3) Routing-based communication

Intelligent transportation systems*:* The inter-vehicle communication conformation Figure no: 1 uses multi-hop multicast or programme to transmit traffic correlated information over multiple hops to a group of receivers. In intellectual transportation systems, vehicles need only be concerned with activity on the road forward and not behind.

Fig1 intelligent transportation systems

Vehicle-to-roadside communication: The vehicle-to-roadside communication formation Figure no: 2 characterizes a single hop transmission where the roadside unit sends a broadcast message to all prepared vehicles in the vicinity. Vehicle-to-roadside communication formation provides a high bandwidth link between automobiles and roadside units. The roadside units may be placed every kilometre or less, succeeding high data rates to be continued in heavy traffic [4].

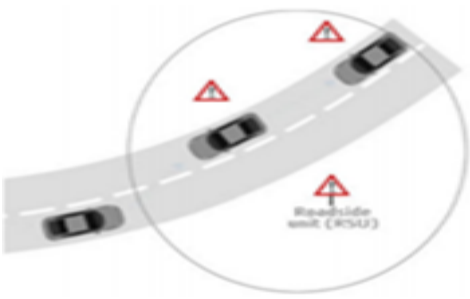

Fig: 2 Vehicle-to-roadside

Routing-based communication: The routing based communication arrangement Figure no: 3 is a multi-hop unicast where a message is broadcasted in a multi Figure no. 3 Routing based announcement hop fashion until the vehicle carrying the anticipated data is reached. When the request is received by a vehicle preserving the desired piece of information, the application at that vehicle instantly sends a unicast message containing the information to the vehicle it established the request from, which is then exciting with the task of forwarding it towards the query source.

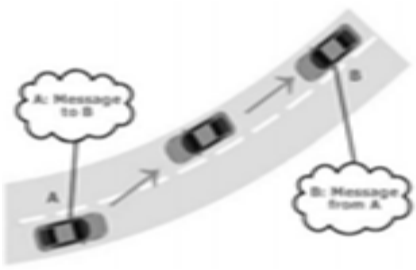

Fig 3 Routing Based Communication

A numerous of applications are intended for these systems, some of which are already probable in some recently designed vehicles Figure no: 4

- Vehicle collision cautioning
- Safety distance warning
- Motorist assistance [15]
- Co-operative driving
- Co-operative cruise control
- Distribution of road information
- Internet access
- Map location
- Instinctive parking
- Driverless vehicles [5]

Fig: 4 Various VANET applications [16]

3. OVERVIEW OF PRIOR WORK

Agung B et al. proposed a protocol for secure vehicular communication. Each vehicle is preloaded with a large quantity of private keys, as well as their corresponding anonymous certificates (perhaps approximately 43 800) [6]. The sending automobile then randomly chooses one of the anonymous certificates, using its corresponding isolated key to digitally sign mails to be sent. To confirm the integrity of the message received, other vehicles use the sender's public key related with this signature. Each unsigned certificate has only a short lifespan to meet the driver's privacy requirements.

V.K. Remya et al. exposed the fact that the unique characteristics of group signature, which is an important cryptographic original, impeccably match the security and privacy requirements in VANETs [7]. By taking diverse security and privacy necessities of two types of VANET infrastructures into account, namely, vehicle-to-infrastructure and vehicle-to-vehicle communications, they suggest a novel secure and privacy preserving protocol for vehicular communication, based on a combination of group signature and identity based mark techniques.

Joaqu´ın F S´anchez. et al. proposed an efficient authentication protocol for [8] vehicular communication, using an effective cryptographic primitive, which is called a batch signature. It allows an RSU to concurrently verify multiple signatures, suggestively reducing the message verification overhead of the RSU as a result.

Ling Fu Xie et al. described as, the classes of uses for vehicular networks range from time serious safety applications to delay accepting internet connectivity applications. In this paper, they take the location that VANETs would indeed turn out to be the networking stand that would support the prospect vehicular applications [9].

4. TOPOLOGY BASED PROTOCOLS

These protocols determine the route and maintain it in a table previously the sender starts communicating data [17]. They are advance divided into Proactive, Reactive and crossbreed protocols.

Pro-active Protocol: The proactive protocol is also recognised [18] as table driven routing protocol. The proactive protocols do not have initial route discovery delay but ingests lot of bandwidth for periodic updates of topology.

Re-active Protocol: These protocols are called as on-demand routing protocols as they[10] periodically update the routing table, when some data is there to send. But these protocols use overflowing process for route discovery, which causes more routing overhead and also suffer from the initial route detection process, which make them inappropriate for safety applications in VANET.

Hybrid Protocol: The hybrid protocols are presented to reduce the control overhead of proactive routing protocols and decrease the initial route discovery delay in reactive routing protocols [19, 20].

5. CONCLUSION

Routing is a significant component in vehicle-to-vehicle and infrastructure to Vehicle statement. This paper converses various routing protocols of VANET. Scheming an efficient routing protocol for all VANET requests is very hard. Hence a review of different VANET protocols, comparing the attacks is absolutely essential to originated up with new proposals for VANET. Therefore this paper has come up with a complete survey and comparison of different classes of VANET routing protocols. From the review it is clear that situation based, geo-cast and cluster based protocols are more dependable for most of the applications in VANET.

6. REFERENCES

[1] Zeadally, Sherali, et al. "Vehicular ad hoc networks (VANETS): status, results, and challenges." Telecommunication Systems 50.4 (2012): 217-241.

[2] Bitam, Salim, Abdelhamid Mellouk, and Sherali Zeadally. "VANET-cloud: a generic cloud computing model for vehicular Ad Hoc networks." *Wireless Communications, IEEE* 22.1 (2015): 96-102.

[3] Balmahoon, R., and R. Peplow. "Vehicular Ad-Hoc Networks: An Introduction to Privacy." Southern African Telecommunication Networks and Applications Conference (SATNAC) will be held from. Vol. 2.

[4] De Castro, Cristina, Carla Raffaelli, and Oreste Andrisano. "A dynamic hierarchical VANET architecture for Named Data Networking applications."*Communications (ICC), 2015 IEEE International Conference on*. IEEE, 2015.

[5] Chaima, Bensaid, Farouvan Kamel Mohame, and Bouki Hacene Sofiane. "Cluster based key management in VANET networks." *Programming and Systems (ISPS), 2015 12th International Symposium on*. IEEE, 2015.

[6] Prasetijo, Agung B., Sami S. Alwakeel, and Hesham A. Altwaijry. "Effects of VANET's attributes on network performance." *Information Technology, Computer and Electrical Engineering (ICITACEE), 2014 1st International Conference on*. IEEE, 2014.

[7] Remya, V. K., and Tanya Singh. "A heterogeneous wireless network integrating smartphones, WLANs and VANET to enhance on-road surveillance and security." *Reliability, Infocom Technologies and Optimization (ICRITO)(Trends and Future Directions), 2015 4th International Conference on*. IEEE, 2015.

[8] Sanchez, J. F., and Luis Armando Cobo. "Theoretical model of congestion control in VANET networks." *Communications and Computing (COLCOM), 2014 IEEE Colombian Conference on*. IEEE, 2014.

[9] Xie, Ling Fu, et al. "Mitigating Doppler effects on physical-layer network coding in VANET." *Personal, Indoor, and Mobile Radio Communications (PIMRC), 2015 IEEE 26th Annual International Symposium on*. IEEE, 2015.

[10] Kumar, Rakesh, and Mayank Dave. "A comparative study of Various Routing Protocols in VANET." arXiv preprint arXiv:1108.2094 (2011).

[11] Yi, Shanqiang, et al. "A context-aware MAC protocol in VANET based on Bayesian Networks." *Communications and Networking in China (CHINACOM), 2014 9th International Conference on*. IEEE, 2014.

[12] Pandey, Pratibha. "Effect of Selfish Behavior on Network Performance in VANET." *Communication Systems and Network Technologies (CSNT), 2015 Fifth International Conference on*. IEEE, 2015.

[13] Knorr, Florian, et al. "Reducing traffic jams via VANETs." *Vehicular Technology, IEEE Transactions on* 61.8 (2012): 3490-3498.

[14] Liu, Kai, et al. "Cooperative Data Scheduling in Hybrid Vehicular Ad Hoc Networks: VANET as a Software Defined Network." (2015).

[15] Martinez, Francisco J., et al. "A survey and comparative study of simulators for vehicular ad hoc networks (VANETs)." *Wireless Communications and Mobile Computing* 11.7 (2011): 813-828.

[16] Singh, Ajit, et al. "A relative study of MANET and VANET: its applications, broadcasting approaches and challenging issues." *Advances in Networks and Communications*. Springer Berlin Heidelberg, 2011. 627-632.

[17] Chen, Xianbo, Hazem H. Refai, and Xiaomin Ma. "On the enhancements to IEEE 802.11 MAC and their suitability for safety-critical applications in VANET." *Wireless Communications and Mobile Computing* 10.9 (2010): 1253-1269.

[18] Liu, Bingyi, et al. "Cloud-Assisted Safety Message Dissemination in VANET-Cellular Heterogeneous Wireless Network." (2015).

[19] Lin, Chun-Cheng, and Der-Jiunn Deng. "Optimal two-lane placement for hybrid VANET-sensor networks." *Industrial Electronics, IEEE Transactions on* 62.12 (2015): 7883-7891.

[20] El Khatib, Amjad, et al. "A Cooperative Detection Model Based on Artificial Neural Network for VANET QoS-OLSR Protocol." *Ubiquitous Wireless Broadband (ICUWB), 2015 IEEE International Conference on*. IEEE, 2015.