International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 10, October- 2014

A Secure Alert Messaging for Vehicular Ad hoc Networks - Survey

Shikha Saju
Computer Science and Engineering
Sree Narayana Gurukulam College of Engineering
Kerala, India

Smitha Suresh
Associate Professor, CSE Dept.
Sree Narayana Gurukulam College of Engineering
Kerala, India

***Abstract*—Safety applications provided by Vehicular Ad Hoc Network is very crucial. The vehicles in the road form a network enabling the passengers with infotainment and security. Emergency messages can be disseminated in the VANET scenario for securing the lives of people by avoiding the situations like chain collisions. The main aim of such messages is to provide safety. So these messages should be genuine one and propagated to all the vehicles in the scenario without any delay. In this paper, clustering technique is used along with the trust relationship to disseminate emergency messages in the network to secure the vehicles from hazardous conditions.**

Keywords—Emergency messaging, cluster, trust, chain collision, intruder.

I. INTRODUCTION

Vehicular ad hoc Network (VANET) is an emerging area with various applications. It is a subset of Mobile ad hoc Network (MANET) consisting of various moving nodes (vehicles) as its members. Vehicles in the network communicate with each other sharing different types of information. The vehicles move at varying speed depending on the nature of the drivers. Vehicles disseminate messages for entertainment and security. Various messages regarding the road conditions, weather, traffic etc can be propagated in the network. Emergency messages play an important role in VANET and hence must be disseminated with great care. The emergency messages are disseminated when critical situations are occurred in the road like accidents, emergency brake or any other hazards. These emergency messages are helpful for the drivers to take necessary steps for avoiding dangerous situations in the road or highway.

Every vehicle in the VANET are provided with on board units (OBU) containing various sensors for sensing different network conditions. Since these sensors are of low cost, they can be deployed in the VANET scenario for providing more security for the vehicles in the network and for the lives of passengers in the vehicles. The different on board units communicates with each other sharing much relevant and crucial information helping the drivers to take necessary actions.

The network consists of a large number of moving nodes with high speed sharing their information regularly without the help of any road side units (RSU). So the main requirement of the VANET is that safety related messages must be reached to all the member vehicles in the network without any delay. So a major concern should be given to the dissemination of emergency messages (Figure 1) and the assurance of the reception by all the vehicles. Then only the application of security can be completely implemented in the network assuring lives of the passengers more secured.

Along with the assurance of the reception in the messages, the factor of trust must also be considered. Trust relationship must be maintained in the network with all the vehicles and road side units. The main aim of trust management in VANETs is to increase the security, reliability of message or information dissemination, reduction of traffic congestions and to ensure the safety of passengers in the network. The trust establishments in the scenario will help to detect any false or wrong information propagated among the members and also to find out the malicious or selfish users. These trustful messages will help the drivers to take appropriate actions during hazards or critical conditions in the road.

The main aim in the deployment of vehicular ad hoc network is to enrich the security of vehicles in the network. So the trust relationships must be evaluated in the real scenario to take accurate decisions during the emergency situations in the highway. The model can manage different vehicles dynamically with the dynamic topology change of network ensuring the security. The untruthful or selfish nodes can be detected easily in the trust evaluation restricting such nodes from further communication inside the network. Thus trust establishment provides more security for the lives of passengers and vehicles in the network.

The lives of the passengers are very important and hence it must be protected. The vehicles in the lane are moving at varying speeds and trust is build there.

In this paper, the vehicles in the VANET scenario are notified about the emergency event through clustering technique. Also the trust relationship is build to protect from the malicious vehicles. Here privacy of the user is assured with distributed trust establishment. The fake location and time stamp sent by the intruders are detected for more security of the network.

II. RELATED WORK

A. *ROUTING IN VANET*

Pei et al. [1] discussed about a table driven or proactive routing protocol in which the information regarding every nodes are collected from the neighboring nodes. Routing table is maintained increasing the storage complexity with the increased network size. Only a partial information is routed for updating, reducing the routing overhead.

Perkins et al. [2] discussed the reactive routing protocol which establishes the route on need. This routing protocol is having the sequence number of the destination and hence providing an up to date path to the destination. Excessive memory requirements are not needed and can be used in large scale networks. But the problem is that initial connection setup and communication requires more time. Extra bandwidth is also consumed due to periodic hello messages.

Karp et al. [3] proposed greedy perimeter stateless routing which only selects the closest node in the final destination to send the messages. To forward the packet, the node has to remember only one hop neighbor location and these forwarding decisions are made dynamically. The protocol mainly uses the greedy forwarding and perimeter forwarding to disseminate the packets. The information regarding the destination node is never been updated in the packet header of the intermediate node.

Santos [4] introduced the cluster based location routing to support the inter vehicle and intra vehicle communications. The clustering scheme used is location specific. The location of the node is very important when the cluster is formed. The route discovery time, end to end delay and number of retransmissions are evaluated. In the case of vehicle to roadside communication the average packet received reduces with the increase in the speed of vehicle. Also the end to end delay, route discovery time and maximum throughput varied very less with the speed of the vehicle.

B. *TRUST MODELS IN VANET*

Riaz et al. [5] proposed a robust method to detect false location and time information. The malicious nodes are detected through their messages based on their trust value. The trust value for the genuine nodes will always be greater than the intruders. It achieves security and robustness against the intruders. The problem is that this method will work accurately only if the message is received from the intruder directly.

Huang et al. [6] addresses limitations of information cascading and oversampling. This can be avoided by giving weights to the nodes. It means that the nodes who have observed the events are given weight 1 and the intermediary nodes with less weight. So the messages can be received made trustful and be used.

Chen et al. [7] designed a framework to support the information sent by the neighboring nodes and to effectively control the false or malicious information reception in the network. The quality of the message is evaluated in a distributed fashion. The malicious users are prevented from intruding into the network through clustering of the nodes. But the problem is that privacy and robustness are not given much importance in the work.

Minhas et al. [8] introduced an approach for modeling trust in VANET environments to restrict the number of reports that are received from other agents. An aggregated feedback mechanism is used which depends on the reliability of the estimated experience-based trust of each other. The confidence value will be calculated and the maximum error rate for the aggregated feedback is noted. The higher rate of confidence states that the message can be trusted in the network. The trust model is aimed to be decentralized, location or time specific, event or task specific and able to support the system level security. The robustness is not all considered in the method which causes problem in the network.

Sushmita Ruj et al. [9] proposed method to detect the false alert messages and the misbehaving nodes in the network after observing the actions. Here each node has the ability to decide whether the information received is true or false. And this decision is mainly depending on the reliability of recent messages and new alerts with estimated vehicle positions. The method does not rely on any voting schemes and group associations. Along with the false alert message detection, the false location information can also be detected.

Gurung et al. [10] proposed the trust model that directly evaluates the authenticity of the messages received from the vehicles. The content of the message is very important during the verification. The road side units or the central servers are not engaged in the checking of trustworthiness of the message. The message classification and information oriented trust model are the two main components of the framework. The two level clustering mechanisms are used to identify the conflict among the information obtained. The trustworthiness of the message received will be calculated in the next component.

Merrihan et al. [11] presented a decentralized trust management and evaluation scheme for the different vehicles in the VANET scenario. A combined trust based scheme is

used joining the role based and experience based trust. The node is assigned with a category level based on its trust value and the confidence measurement is done based on the degree of trustworthiness of a node's generated reports. A penalty system is introduced to monitor the intruders and trace their actions. It is an efficient message verification mechanism for vehicular communications. It only considers the trust opinions generated from the trusted nodes and discards from the non trusted ones.

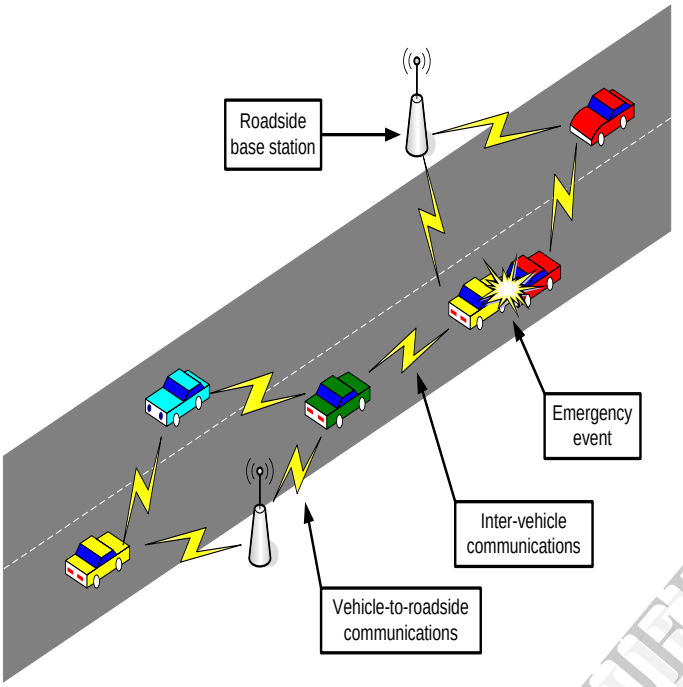

Figure 1. Occurrence of Emergency Event

III. CONCLUSION AND FUTURE WORK

In Vehicular ad hoc Networks, the vehicles are in contact with each other. Each vehicle communicates in regular periods by sending beacon messages. The main difference between other ad hoc networks is that VANET topology changes frequently. Traffic accidents or other emergency situations can occur in the network and the members in the VANET scenario must be notified about the event. So such emergency messages must be reached to all the nodes (vehicles) without any delay.

This survey is mainly on the routing techniques that can be used in the vehicular ad hoc networks during the critical conditions and the various trust models used for secure messaging. Different routing methods are analyzed with the secure emergency messaging techniques in the networks.

REFERENCES

[1] Pei G., Gerla M. and Chen, T.-W (2000), "Fisheye State Routing: A Routing Scheme for Ad Hoc Wireless Networks", Proc. ICC 2000, New Orleans, LA, June 2000.

[2] Perkins C., Belding-Royer E., Das S. (July 2003) "Ad Hoc On-Demand Distance Vector (AODV) Routing".

[3] Karp B. and Kung H. T. (2000), "GPSR: Greedy Perimeter Stateless Routing for Wireless Networks" in Mobile Computing and Networking, pages 243-254, 2000.

[4] R. A. Santos "Supporting Inter-Vehicular and Vehicle-Roadside Communications over a Cluster-Based Wireless Ad Hoc Routing Algorithm".

[5] Riaz Ahmed Shaikh, Ahmed Saeed Alzahrani, "Intrusion-aware trust model for vehicular ad hoc networks." Published in Wiley Online Library in Security and Communication Networks (Aug 2013).

[6] Zhen Huang, Sushmitha Ruj, Marcos Cavenaghi, Amiya Nayak. "Limitations of Trust Management Schemes in VANET and Countermeasures", In IEEE 22nd International Symposium on Personal Indoor and Mobile Radio Communications (2011).

[7] Jie Zhang, Chen Chen, Robin Cohen, "Trust Modeling for message Relay Control action decision making in VANETs". Published in Securiy and Communication Networks, volume 6 (2013).

[8] Minhas U. F., Zhang J., Tran T., Cohen R. "Intelligent Agents in Mobile Vehicular Ad Hoc Networks: Leverging Trust Modeling Based on Direct Incentives for Honesty." In proceedings of the IEEE/WIC/ACM International Conference on Intelligent Agent Technology, Toronto, Canada, vol.2, pp. 243-247 (2010).

[9] Sushmita Ruj, Macros A. Cavenaghi, Zhen Huang, Amiya Nayak and Ivan Stojmenovic. "On Data-Centric Misbehavior Detection in VANETs". Published in Vehicular Technology Conference (VTC Fall), 2011 IEEE, 5-8(2011).

[10] Sashi Gurung, Dan Lin, Anna Aquicciarini, and Elisa Bertino, "Information- oriented Trustworthiness Evaluation in Vehicular Ad-hoc Networks". Published in the 7th International Conference on Network and System Security (2013).

[11] Merrihan Monir, Ayman Abdel-Hamid and Mohammed Abd El Aziz. "A Categorized Trust-Based Message Reporting Scheme for VANETs". Advances in Security of Information and Communication Networks in Computer and Information Science vol. 381, Springer Link (2013).