Security and Performance issues in VANET

Bharathi M, Preethi
Department of Computer Science & Engineering, SJCIT
E-mail: bharathigowda1@gmail.com, preethisrivathsa@gmail.com

***Abstract*- A Vehicular Ad-Hoc Network or VANET is a form of Mobile Ad-Hoc Network or MANET which provides communication between vehicles and between vehicles and road-side base stations. A vehicle in VANET is considered to be an intelligent mobile node capable of communicating with its neighbors and other vehicles in the network. In order to achieve a good performance of safety-related protocols, we propose to limit the load sent to the channel using a strict fairness criterion among the nodes. Bandwidth issues arise in this type of networks due to the potential large number of nodes. Data aggregation addresses these issues avoiding the dissemination of similar messages in the network.**

Keywords:
VANET, Wireless sensors, data aggregation, security of VANETs

1. Introduction:

Vehicular Ad-Hoc Network, or **VANET**, is a form of Mobile ad-hoc network, to provide communications among nearby vehicles and between vehicles and nearby fixed equipment, usually described as roadside equipment. *In VANET*, or Intelligent Vehicular Ad-Hoc Networking, defines an intelligent way of using Vehicular Networking. *In* VANET integrates on multiple ad-hoc networking technologies such as WiFi IEEE 802.11 b/g, WiMAX IEEE 802.16,Bluetooth, IRA, ZigBee for easy, accurate, effective and simple communication between vehicles on dynamic mobility. VANET is mainly designed to provide safety related information, traffic management, and infotainment services. Safety and traffic management require real time information and this conveyed information can affect life or death decisions. Simple and effective security mechanism is the major problem of deploying VANET in public. Without security, a Vehicular Ad Hoc Network (VANET) system is wide open to a number of attacks such as propagation of false warning messages as well as suppression of actual warning messages, thereby causing accidents. This makes security a factor of major concern in building such networks. VANET are of prime importance, as they are likely to be amongst the first commercial application of ad hoc network technology. Vehicles are the majority of all the nodes, which are capable of forming self organizing networks with no prior knowledge of each other, whose security level is very low and they are the most vulnerable part of the network which can be attacked easily. Figure 1 shows the basic units of VANET[21].

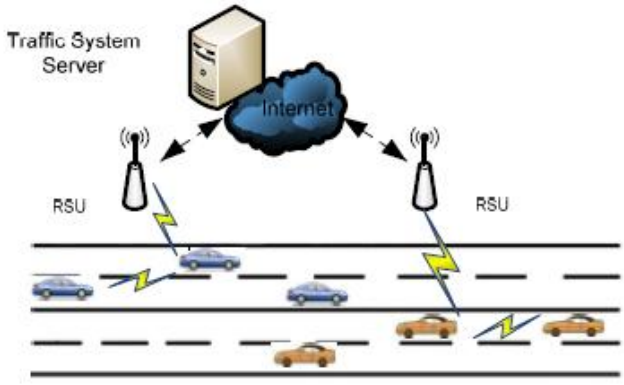

Fig 1: Basic units of VANET

2. Related work

The networks that interconnect vehicles on road are called Vehicular Ad hoc Networks (VANETs) [2], [3], [4], [14]. "A mobile ad hoc network (MANET) consists of mobile nodes that connect themselves in a decentralized, self-organizing manner and may also establish multi-hop routes. If mobile nodes are cars this is called vehicular ad hoc network" [15].

"The main target of research in VANETs is the improvements of vehicle safety by means of inter vehicular communication (IVC)" [3]. Several different applications are emerging in VANETs. These applications include safety applications to make driving much safer, mobile commerce, and other information services that will inform drivers about any type of congestion, driving hazards, accidents , traffic jams [2], [4], [9], [10], [16]. VANETs have several different aspects compared to MANETs, in that the nodes move with high velocity because of which the topology changes rapidly [2], [3], [9], [11], [12], [13]. VANETs are also prone to several different attacks. Therefore, the security is of VANETs is indispensable. VANETs pose many challenges on technology, protocols, security which increase the need for research in this field [17].

In the past years, in-network aggregation schemes for vehicular networks received increasing research attention. The research area is related to aggregation mechanisms for wireless sensor networks (WSNs), but due to differing requirements, like high node mobility in VANETS, WSN aggregation mechanisms cannot be easily adopted [2]. Most VANET aggregation mechanisms are targeted towards one specific use case, often dissemination of average speeds on road segments, while mentioning applicability to other use cases, as well. Similarly, generic modeling schemes for network data have been proposed in different research

domains. These models are usually crafted towards centralized systems and used as a data structure to support algorithms working on the contained data.

3. VANET Security Architecture

Although handling security issues in VANET is very tough, because handling security issues will increase the overhead cost and also the functional cost. VANET will be executed when cost management and security handling issues, both will be reduced or compromised so that the system becomes effective from both the point of views. While going through all the papers each and every paper gave us certain information. VANET follows a simple security architecture which is underlined below [1, 3].

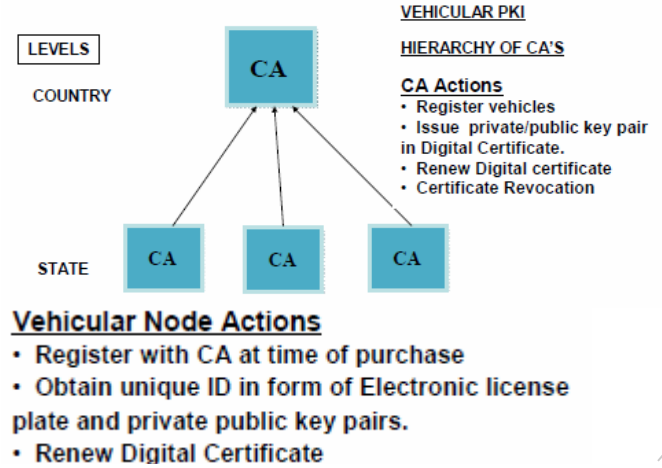

Fig 2: VANET Security Architecture

The basic architecture consists of Network nodes which can be either Vehicles or Road Side Infrastructure and existing Registration Authorities for vehicle registration and record maintenance.

These nodes will be installed with required sensors for gaining information, processing units for processing the collected or received information and communication system for disseminating information to and receiving information from other nodes. A secure system, besides the basic network nodes, will consist of a Vehicular Public Key infrastructure (PKI), a Secure Computing platform and various security mechanisms. Secure mechanisms comprise identity management using Electronic License Plates with certified public and private keys attached to the owner, Authentication and Integrity using Digital Signatures, Privacy using Pseudonyms, Pseudonym handling and Certification Revocation mechanisms.

A Vehicular PKI will consist of the national and state level registration authorities acting as Certification Authorities

(CAs) which will issue certified public/private key pairs to vehicles. A Secure Computing platform on a vehicle will consist of tamper resistant hardware and firmware. Its job is to store cryptographic material (private keys) and a trusted (tamper proof) clock.

The proposed solution is based on transferring authenticated messages with the help of base stations, monitoring center and road side situated camera. The message authentication is monitored by the Central Authority (CA), i.e. monitoring center and at the same time, spreading proper messages to all the vehicle is also monitored by CA. There are certain assumptions which are considered beforehand, i.e. deploying the whole proposed system. It will be discussed through out, while describing the system.Tamper-proof device (TPD) will take care of storing all the cryptographic material and performing cryptographic operations, especially signing and verifying safety messages.

4. Data Aggregation in Vehicular Networks

Data aggregation is used to combine correlated information
from different nodes before redistributing the information into the network. The aim is to decrease the number of disseminated messages which in systems with a continuously update of information (e.g. traffic systems that keeps informs the drivers with the traffic conditions) will result in a dramatically decrease of the overhead.

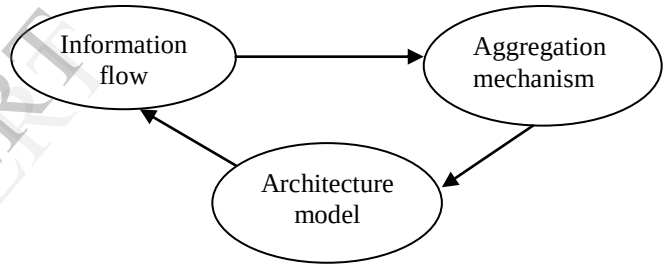

Fig 3: Aggregation modeling

Information flow: The goal of the information flow model is to visualize aggregated information and its origins from the viewpoint of one particular vehicle after a given aggregation scheme has run a certain amount of time. To model the information flow, we start with a one-dimensional street, on which a number of vehicles are positioned at regular intervals.[5][6] All vehicle positions are assumed to be static. Introducing vehicle mobility to the information flow would complicate the resulting graph without providing additional information.

Aggregation mechanism: Information originating from one or more cars about an interval in time and/or space. Examples for aggregated information are “there are 50 free parking spots in the harbor district”, “the average speed on the motorway M1 between kilometer 20 and 25 is 50 kph”, or “on Main Street, at kilometer 6.2, there is an icy road interval

of 500m length".[10] A survey of the data aggregation solutions in VANETs reveals that there are two high level approaches for making use of data aggregation schemes in VANETs. Data is then analyzed to see whether there is any correlation between atomic data items. If it is decided that there is data correlation, then data is fused. Data, aggregated or not depending on the correlation, is further disseminated in the network.

Architecture Model: The following four tasks fully describe a generic aggregation scheme:
(1) Decide whether data items can be aggregated
(2) Fuse several data items together
(3) Manage the information available to a node in a world model, and
(4) Disseminate parts of the information to other nodes.

5. Applications

Some of the application where the security- related and improvements of performance play important roles is listed below:

Collision Avoidance

V-V and V-I Communications can save many lives and prevent injuries. In this application, if a vehicle reduces its speed significantly after observing an accident or experiencing an accident, it will broadcast its location to its neighbor vehicles. And other receivers will try to relay the message further and the vehicle in question will emit some kind of alarm to its drivers and other drivers behind. In this way, more drivers far behind will get an alarm signal before they see the accident and can take any decision for his betterment.

Cooperative Driving

The drivers play the leading part in this application. Like violation warning, turn conflict warning, curve warning, lane merging warning etc. These services may greatly reduce the life-endangering accidents. In fact, many of the accidents come from the lack of cooperation between drivers. Given more information about the possible conflicts, we can prevent many accidents.

Traffic Optimization

In this application the vehicles could serve as data collectors and transmit the traffic condition information for the vehicular network. To be more specific, in this application, vehicles could detect if the number of neighboring vehicles is too many and or the speed of vehicles is too slow, and then relay this information to vehicles approaching the location. To make it work better, the information can be relayed by vehicles traveling in the other direction so that it may be propagated faster to the vehicles toward the congestion location. In this way, the vehicles approaching the congestion location will have enough time to choose alternate routes.

Payment Services

This application is very suitable for toll collection without even decelerating the car or waiting in line.

Location-based Services

Finding the closest fuel station, restaurant, lodge etc can be done effectively using location based service. Although, GPS systems have such kinds of services already present in it but it can also be achieved using VANET.

6. CONCLUSION

In this paper we proposed a system that can be used for authentication of messages,. Firstly we discussed the overview of the network, applications and system requirements of VANET security. Later we discussed the aggregation mechanism in detail. Then we discussed about some of the applications which uses the security-related and performance improvements in VANET application. Still there is a lots of scope and challenge in VANET security and performance related concepts.

REFERENCES

[1]. Al Sakib Khan Pathan: A book: where a chapter is Security in VANET- YEet to yet be published.
[2]. Fay Hui: A survey on the characterization of Vehicular Ad Hoc Networks routing solutions ECS 257 Winter 2005 Date: 01/28/2005
[3].Antonios,Stampoulis(antonios.stampoulis@yale.edu),Zheng Chai: A Survey of Security in Vehicular Networks
[4]. Haojin Zhu, Xiaodong Lin, Rongxing Lu, Pin-Han Ho, Xuemin (Sherman) Shen: AEMA: An Aggregated Emergency Message Authentication Scheme for Enhancing the Security of Vehicular Ad Hoc Networks
[5]. Zheng: Challenges in vehicular networks
[6]. Maen M. Artimy, William Robertson, and William J. Phillips: CONNECTIVITY IN INTER-VEHICLE AD HOC NETWORKS
[7]. Jijun Yin Tamer ElBatt Gavin Yeung Bo Ryu: Performance Evaluation of Safety Applications over DSRC Vehicular Ad Hoc Networks
[8]. S.Y. Wang: Predicting the Lifetime of Repairable Unicast Routing Paths in Vehicle-Formed Mobile Ad Hoc Networks on Highways
[9].Linda Briesemeister Role-Based Multicast in Highly Mobile but Sparsely Connected Ad Hoc Networks
[10]. Yong Hao, Yu Cheng, and Kui Ren Distributed Key Management with Protection Against RSU Compromise in

Group Signature Based VANETs
[11]. Wenmao Liu, Hongli Zhang and Weizhe Zhang An autonomous road side infrastructure based system in secure VANETs
[12]. Une Thoing Rosi and Chowdhury Sayeed Hyder A Novel Approach for Infrastructure Deployment for VANET
[13] B. Yu, J. Gong and C.-Z. Xu, "Catch-up: a data aggregation scheme for vanets", *VANET'08: ACM Int. Workshop on VehiculAr Inter-NETworking,* pp. 49-57, NewYork, NY, SA, ACM, 2008.
[14] K. Ibrahim and M.C. Weigle, "CASCADE: Cluster-Based Accurate Syntactic Compression of Aggregated Data in VANETs", *GLOBECOM Workshops*, pp. 1-10, 2008.
[15] M. Caliskan, D. Graupner and M. Mauve, "Decentralized Discovery of Free Parking Places", *ACM VANET '06*, New York, USA 2006, pp. 30–39.
[16] S. Dietzel, E. Schoch, B. Konings, M. Weber and F. Kargl, "Resilient Secure Aggregation for Vehicular Networks", *IEEE Network*, pp. 26-31,2010.
[17] F. Picconi, N. Ravi, M. Gruteser, L. Iftode, "Probabilistic Validation of Aggregated Data in Vehicular Ad-Hoc Networks," *ACM Int. Workshop on Vehicular Ad Hoc Networks*, New York, USA, 2006, pp. 76–85.
[18] S. Buchegger, J. Mundinger and J. Le Boudec, "Reputation Systems for Self-Organized Networks: Lessons Learned," *IEEE Technology and Society Magazine*, vol. 27, no. 1, pp. 41–47, 2008.
[19] M. Raya, A. Aziz and J. Hubaux, "Efficient Secure Aggregation inVANETs," ACM Int. Wksp. Vehicular Ad Hoc Networks, New York,USA, 2006, pp. 67–75.
[20] B. Scheuermann, , "A Fundamental Scalability Criterion for Data Aggregation in VANETs," *ACM Int. Conf. on Mobile Computing and Networking*, New York, USA, 2009, pp. 285–96
[21] S. Dietzel, F. Kargl, G. Heijenk and F. Schaub, "Modeling in-network aggregation in VANETs," in *Communications Magazine, IEEE* , vol.49,no.11, pp.142-148, 2011.