A Survey on Architecture, Protocols, Challenges and Solutions on Vehicular Networking

Muhammad Asif khan, Aytizaz Ahmed, Mujahid Shah, Muhammad Shahab khan,
Noor Gul, Nauman Qamar and Amir Shahzad
Gandhara University of Sciences, Peshawar, Pakistan

Abstract– **Vehicular networking has various prospects and opportunity to facilitate various functions connected with traffic safety, traffic Effectiveness system infotainment and on their improvement. In this paper we set up the essential overview, its application and related requirements, its architecture, protocol its challenges and its solutions.**

Keywords– Protocols, Networking, Vehicular, Challenges and Solution

I. INTRODUCTION

Vehicular network also known as VANETs are a foundation of the envision intelligent transport system (ITS). with allowing Vehicles to be in touch with each others through inter Vehicles communication (IVC) plus with roadside base station via roadside-to- Vehicles communication (RVC) , Vehicular network will add to safe and sound and more proficient roads by giving appropriate information to the concerned system. The attractive research paper of Vehicular network is where Ad-Hoc networks can carry to their full prospective.

A. Security of Vehicular Network

To be an actual expertise which warranty open security on roads, Vehicular network require an suitable safety structural design which defend them from diverse kind of protection hit. Leveraging on knowledge of LCA in the area of network and safety, we are discovering the diverse safety features of Vehicular network with:

1. Threat model
2. Authentication and key management
3. Privacy
4. Secure positioning

The concern application entails diverse sanctuary and seclusion constraints with revere to the fortification goals integrity, discretion and availability. Nevertheless, there is a familiar need for a security infrastructure establishing communal trust and enabling cryptography. Basically using digital signatures and a public key infrastructure (PKI) to defend message veracity is inadequate taking into account multilateral security and performance requirements. Consequently we developed security architecture for VANETs those weighing scale security requirements of all participants whilst keeping in mind the real-time requirements. We also acknowledged and if required developed viable mechanisms so as to fit in this architecture [1].

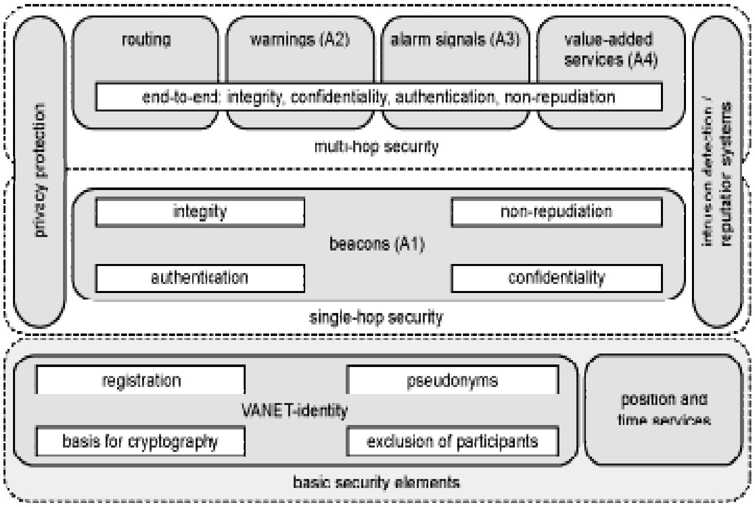

Fig. 1: VANET Security Model [1]

B. Architecture of Vehicular Networks

The VANETs are a subgroup of mobile ad-hoc networks (MANETs) with the distinctive possessions so as to the nodes are vehicles like trucks, cars, buses and motorcycles. So this involves that node progress is restricted by reasons/facts akin to road course, encircling traffic and traffic policies. For the reason that of the constrained node faction it is a practical postulation that the VANET will be propped up by some fixed infrastructure that gives a hand with some services and can endows with admittance to stationary networks. The rigid infrastructure will be employed at decisive locations approximating slip roads, service stations, dodgy crossroads or places well-known for perilous weather circumstances. Nodes are anticipated to correspond by means of North American DSRC standard that utilizes the IEEE 802.11p standard for wireless communication.

To permit communication with participants out of radio range, messages ought to be forwarded by other nodes (multi-hop communication). Vehicles are not subject matter to the stern energy, space and computing abilities restrictions generally espoused for MANETs. Further exigent are the potentially very high tempo/speed of the nodes (up to 250 km/h) and the hefty dimensions of the VANET. The principal VANET's objective is to augment road safety. To attain this, the vehicles proceed/acts as sensors and swap warnings or more commonly telematics information (like contemporary speed, location or ESP commotion) that facilitates the drivers to retorts untimely to anomalous and potentially dangerous situations like accidents, traffic jams or glaze. The information supplied by further vehicles and stationary infrastructure might also be used for driver subordinate systems like adaptive cruise control (ACC) or breaking assistants. Further more, authorized entities similar to police or firefighters ought to be able to send alarm signals and lessons e.g. to clear their way or impede other road users.

Moreover that, the VANET should augment reassure by means of value-added services similar to position based services or else the Internet on the thoroughfare/road.

II. VANET ROUTING PROTOCOLS OVERVIEW

As far as the VANET is concern, so the routing protocols are categorized into diverse classes: Routing protocol Topology based, Routing Protocol Position based, Routing protocol Cluster based, Routing protocol Geocast based & Broadcast based.

A. Topology Based Routing Protocols

Topology based routing protocols which discover the route and maintain routing information in a table before the Sender starts transmitting data. They are divided into Proactive, Reactive and hybrid protocols.

Proactive Protocols [2]: all the nodes of the networks in proactive protocol or table driven routing protocols periodically exchanging the knowledge of topology. The proactive protocols do not have initial route discovery delay but consumes lot of bandwidth for periodic updates of topology; e.g., fisheye state routing (FSR), Optimized Link State Routing Protocol (OLSR), and Topology Dissemination Based on Reverse-Path Forwarding (TBRPF) etc.

Reactive Protocols [2]: Reactive routing protocols or on-demand routing protocols periodically update the routing table, when some data is there to send. When use flooding process for route discovery, which causes more routing overhead and also suffer from the initial route discovery process, which make them unsuitable for safety applications in VANET; e.g., Ad hoc on demand distance vector (AODV), Dynamic Source Routing (DSR), and temporally-Ordered Routing Algorithm (TORA) etc.

Hybrid Protocols [2]: Hybrid routing protocols is combination of reactive routing protocols and proactive routing protocols which reduce the control overhead of proactive routing protocols and decrease the initial Route discovery delay in reactive routing protocols; e.g., Zone Routing protocol (ZRP), Hybrid Routing Protocol (HARP) etc.

B. Positions Based Routing Protocol

Routing protocol position based constitutes of class of routing Algorithm. Which is sharing the belongings of geographic spotted information in succession to go for the subsequently forwarding hops? The packet is launch/transmit devoid of any map acquaintance to the one hop neighbor, which is adjacent to destination. As far as the better performance of Position based routing is concern so for the reason that there is no necessitation for the creation and to maintain worldwide route from source node to destination node. We have two types of Position based routing: Position based greedy Vehicle-to-Vehicle protocols, Delay Tolerant Protocols etc.

Position Based Greedy Vehicle to Vehicle Protocols [3]: Within Greedy vehicle to vehicle routing Protocols policy and transitional node should infatuated position of itself, location of its neighbor and destination location in the route forward message to the farthest neighbor in the direction of the next destination. The core objective of these protocols is min holdup routing protocols to convey data packets to destination as soon as possible that different types of position based greedy Vehicle to Vehicle protocols likes GSR, GPSR, CAR, ASTAR, STBR, CBF etc.

Geographic Source Routing (GSR) [4]: GSR used in mobile ad hoc network to improve the performance because to use many application of MANET in vehicular ad hoc network VANET circumstances by slotting in to it greedy forwarding of messages in the direction of the destination. If at some or any leap/hop there are no nodes in the route of destination after that GPSR exploits a recuperation approach branded as perimeter mode having two components.

- Constructs confined renovation/conversion/translation of connectivity chart/table addicted to planar chart by removing superfluous edges which are called distributed planarization algorithm.
- Routing algorithm (Online) that maneuvers on planer charts. Within GPSR if some or any hindrance or emptiness transpires subsequently algorithm goes through perimeter mode and planner grid/chart/graph routing algorithm initiates function, engrosses transmitting the message to intermediate neighbor instead of sending to farthest node, but this method introduces long delays due to greater no. of hop counts.
- Due to fast movement of vehicles, routing loops are introduced which causes dissemination of messages to long path.
- GPSR uses static street map and location information about every node, since GPSR does not consider vehicle density of streets so it is not an efficient method for VANET.

C. Broadcast Based Protocols

Broadcast is based on hierarchal structure for highway network. In broadcast the highway is divided into virtual cells which move like vehicles. The nodes in the highway are organized into two level of hierarchy: the first Level hierarchy includes all the nodes in a cell, the second level hierarchy is represented by cell reflectors, which are few nodes located closed to geographical centre of cell. Some Cell reflected behaves for certain interval of time as cluster head and handles the emergency messages coming from same members of the cell or nearby neighbor. This protocol performs similar to flooding base routing protocols for message broadcasting and routing overhead.

Distributed vehicular broadcast protocol (DVCAST) [5], [6]: Each vehicle uses a flag variable to check whether the packet is redundant or not and It is uses local topology information by using the periodic hello messages for broadcasting the information. DVCAST protocol divides the vehicles into three types depending on the local connectivity as well connected, sparsely connected, totally disconnected neighborhood. In well connected neighborhood it uses persistence scheme weighted persistence, slotted 1and persistence. In sparsely connected neighborhood after receiving the broadcast message, vehicles can immediately rebroadcast with vehicles moving in the same direction. In totally disconnected neighborhood vehicles are used to store the broadcast message until another vehicle enters into transmission range, otherwise if the time expires it will discard the packet. DVCAST protocol causes high control overhead and delay in end to end data transfer.

Urban Multi-hop Broadcast Protocol (UMB) [7]: This protocol performs with much success at higher packet loads and vehicle traffic densities without any prior topology information to sender node tries to select the furthest node in the broadcast direction for forwarding and acknowledging the packet. It is designed to overcome the interference, packet collision and hidden node problems during message distribution in multi-hop broadcast [8].

III. VEHICULAR NETWORKING SOLUTIONS TO THE CHALLENGES

This section describes solutions to the challenges:

A. Addressing and Geographical Addressing

Packets transported within a vehicular network require particular addressing and routing features. In fixed infrastructure routing, packets are usually routed following topological prefixes and therefore cannot be adapted to follow geographical routing. The concern solutions of three families are expressed to incorporate the perception of corporeal/physical locality into the contemporary devise of Internet that relies on logical addressing. These families of solutions are:

- Application layer solutions
- GPS-Multicast solution
- The Unicast IP routing broaded/extensified to pact with the addresses of GPS – specifies how GPS positioning is used for destination addresses. A GPS address could be represented by using:

(i) The slammed/closed polygons, such as ring/circle (Radius center point), where, any node that lies within the defined geographic area could receive a message, (ii) site-name as a geographic access path, wherever a memo/message can be transmitted to a particular place by spotting/defining its location in provision of real-word names such as names of site, city, township, county, state, etc. (iii) Application layer solutions to addressing– the application layer solution uses an extended DNS scheme to find the geographical position.

DNS (Domain Name System) is extended by including a "geographic" data base, which contains the jam-packed index information downwards to the stage of IP addresses of each base station and its exposure area characterized as a polygon of coordinates. Four level domains are included. The first level represents the geographic information; the second one represents the states, the third one represents the counties and the fourth one represents polygons of geographical coordinates, or the so called points of interest. The concern geographic address is decided to be resolved in a same fashion as the typical domain address, by using IP addresses of base stations that cover the geographic area.

Two possibilities are distinguished. In the first one, a series of unicast messages is transmitted to the IP addresses returned by the DNS. These IP addresses correspond to the base stations located in the given geographic area. Each base station then forwards the messages to the nodes that are communicating with it, either using application layer filtering or network level filtering. In the second option, all the base stations located in the given geographic area have to join the impermanent multicast cluster intended for the geographic area identified in the message. All messages that have to be sent to that given geographic area will be sent on a multicast manner using that multicast address.

B. GPS-Multicast Solution to Addressing

The GPS Multicast solution uses the GPS Multicast Routing Scheme (GPSM). Here every detachment and fragment/atom is mapped to a multicast address. An atom represents the smallest geographic area that can have a geographic address. A partition is a larger geographic area that contains a number of atoms that can also encompasses a geographic address. A county, state, town could be represented by a partition. The main idea used by this protocol is to estimate the addressing polygon of the negligible partition, which is enclosed in this polygon and by employing the multicast address related to that partition as the IP address of the concern message. GPSM provides a flexible mix between application level filtering for the geographic address and multicast.

C. Unicast IP Routing Solution Extended to Deal with GPS Addresses

The solutions associated with this geographic addressing type are the following:

• ***Geometric Routing Scheme (GEO):*** This routing scheme exploits the polygonal geographic target/destination information in the GPS-cast header directly for routing. GEO routing uses a virtual network, comprised of GPS address routers, which applies GPS addresses for routing overlayed onto the current IP internetwork.

• ***Geographical Positioning Extension for IPv6 (GPIPv6) [9]:*** This protocol is defined for distribution of geographical positioning data within IPv6. GPIPv6 requires the specification of two new option types for IPv6. These options are GPIPv6 source and GPIPv6 destination, which consist of signaling the geographical positions of the source and destination, respectively. Using unicast-prefixes to target multicast group members [10].

In [11] an extension to IPv6 multicast architecture is described that allows for unicast-prefix-based allocation of multicast addresses. Using this specification unicast prefixes could be used to target multicast group members located within a geographic area.

IV. DISCUSSIONS

Three geographical addressing families can be identified: Application layer, GPS-multicast and Unicast IP routing enlarged to pact with GPS addresses. The most promising, but also the most complex one is the family that extends IP routing and IP addressing in order to cope with GPS addresses. While several solutions associated with this family have been proposed, more research and standardization activities are needed for a successful realization. B. Risk analysis and management Risk analysis in vehicular networks has not yet been studied extensively. One frequently cited paper on attacker capabilities in vehicular networks is [12], which describes the work accomplished in the German project Network on Wheels (NoW) [13]. The security model used in NoW is flexible, allowing integrating previously found attacks into the studied attack model. This model studies four major attack aspects:

- Attacks on the wireless interface
- Attacks on the hardware and software running on OBUs and RSUs
- Attacks on the sensor inputs to different processing units in vehicles
- Attacks on security infrastructure behind wireless access networks, such as vehicle manufacturers, certification authorities, traffic authorities, etc

In [14], [15], [16] two procedures are identified to enhance the overall security: 1) perform local plausibility checks, such as comparing the received information to internal sensor data and evaluating the received information from different sources about a single event; 2) Do regular checks on the nodes, most notably RSUs.

Thus, Risk analysis and management have been researched on a small scale. From the performed studies in this area it can be concluded that position forging attacks constitute a major vulnerability of the system [17]. More work is needed in the area of risk management in order to cope with this vulnerability.

In [18], security concepts that can be used to support the data trust and verification are categorized into proactive security and reactive security concepts.

The proactive security concepts can be currently, considered as the most promising candidates for traffic safety applications in vehicular networks [19].

V. CONCLUSIONS

This research paper is a study and survey, which commence and argue the possible uses and already implement cases, which might be maintained by Vehicular networking in the coming future. As Vehicular networking is the allowing skill, which sustain numerous functions changeable from Internet services and application up to road safety application. and discussed. As a final point the current major study challenges related with Vehicular networking are commence and a number of explanation and solutions for these research challenges are explain and described.

REFRENCES

[1] www-sec.uni-regensburg.de/vanet/ (Access on Jan 14, 2012)

[2] C.Siva Rammurty and B.S.Manoj[2011] ,"Ad hoc wireless networks architectures and protocols" ISBN 978-81-317-0688-6.

[3] Yu Wang and Fan Li, "Vehicular Ad Hoc Networks" in Guide to Wireless Ad HocNetworks, Computer communication and Networks, DOI 10.1007/978-1-84800, 328-6_20, 2000.

[4] B. Karp and H.T. Kung, "GPSR: Greedy perimeter stateless routing for wireless networks", in Proceedings of the ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom), 2000.

[5] Kevin, Uichin Lee, Mario Gerla, "Survey of Routing Protocols in Vehicular Ad Hoc Networks in Car2Car, 2010.

[6] Jagadeesh Kakarla, S Siva Sathya, "A Survey on Routing Protocols and its Issues in VANET" International Journal of Computer Applications, Vol. 28, No. 4, 2011.

[7] Sandhaya Kohli, Bandanjot Kaur, "A comparative study of Routing Protocols in VANET", Journal of Information Engineering and Applications, Vol. 1, No. 4, 2011

[8] [9] R. Baldessari, A. Festag, and J. Abeille, "NEMO meets VANET: A Deployability Analysis of Network Mobility in Vehicular Communication," in 7th International Conference on ITS Telecommunications (ITST '07), 2007.

[9] T. Imielinski and J. Navas, "GPS-Based Addressing and Routing," IETF RFC 2009, pp. 1–27, November 1996.

[10] J. Navas and T. Imielinski, "GeoCast Geographic Addressing and Routing," in Proc. ACM Mobicom97. ACM, 1997, pp. 66–76.

[11] J. Vare and J. Syrjarinne and K.-S. Virtanen, "Geographical positioning extension for IPv6," in Proc. International Conference on Networking (ICN 2004), 2004.

[12] B. Haberman and D. Thaler, "Unicast-Prefix-based IPv6 Multicast Addresses," IETF RFC 3306, August 2002.

[13] A. Aijaz, B. Bochow, F. Dotzer, A. Festag, M. Gerlach, R. Kroh, and T. Leinmuller, "Attacks on Inter Vehicle Communication Systems – an Analysis," in 3rd International Workshop on Intelligent Transportation (WIT 2006), 2006.

[14] NOW Website, "Network on Wheels," Website, May 2011, also available as http://www.network-on-wheels.de/about.html.

[15] B. Schneier, "Attack trees: Modeling security threats," Dr. Dobb's Journal, December 1999.

[16] T. Leinm¨uller and E. Schoch and C. Maih¨ofer, "Security Requirements and Solution Concepts in Vehicular Ad Hoc Networks," in Proceedings of 4th Annual Conference on Wireless On demand Network Systems and Services (WONS 2007), 2007.

[17] M. Raya and J. P. Hubaux, "The Security of Vehicular Ad Hoc

[18] Network," in Proc. 3rd ACM workshop on Security of ad h and sensor networks, (ACM SASN 2005), 2005.

[19] IEEE Communications Surveys & Tutorials, Vol. 13, No. 4, Fourth Quarter, 2011.