Communication and Network Architectures of Intelligent Transport System: A Review

Savitha Sivalingam
Research Scholar, Computer Science Engineering and Technology, CMR University, India
E-mail: Savithas.15phd@cmr.edu.in

Abstract- Intelligent Transport Systems (ITS) are required to support the economy of the country and to address the issue of congestion management in the country. ITS is an umbrella term that covers the latest technologies and operational methods adopted for highways and transit. The use of ITS technologies has the potential to yield a new wave of road safety and other potential benefits for India. ITS is expected to play an important role in delivering safer transportation environment by introducing autonomous vehicles. The present paper addresses the various networking technologies and communication developments introduced in the field of ITS and their impact on providing transportation solutions for the future. The available literature on ITS technologies deployed for managing and assisting transportation were reviewed. Versatile systems and technologies that enhance the safety and efficiency of transportation with the help of communication platforms and sensing capabilities were reviewed.

Keywords- Intelligent Transport Systems, Traffic Management, Communication, Vehicular networks, Road safety, Inter-vehicle, Public road transport, Autonomous vehicles, Driving, Traffic information systems, Traffic control.

1. INTRODUCTION

The increasing number of vehicles over the decade has resulted in a saturation of the infrastructure architecture (Jalali, El-Khatib & McGregor, 2015). The current situation has an adverse impact on the lives of the people who live in urban areas. Traffic congestion, delay in transportation, and vehicular pollution are some of the major issues owing to increase in the number of vehicles. Several solutions such as wearing safety belts, constructing better roads have been introduced to address these issues. However, these solutions have a considerable amount of impact on the environment and face the limitation of space in urban areas (Figueiredo et al., 2001). Nonetheless, improving the transport infrastructure of the country is critical for the economic development of the country. Therefore, a critical need for implementing a compromise solution has been felt in the recent years. The ITS proponents foresee a substantial future for new ITS technologies in transportation applications that can revolutionize the manner in which transport systems are designed and built.

The deployment of intelligent transportation systems technologies is expected to provide safety, and efficiency of the road-vehicle systems (Figueiredo et al., 2001). ITS applications for traffic management aids in intersection control, incident detection, vehicle classification, monitoring, revenue collection, and historical traffic data. Similarly, ITS also assists the commuters on-road with the following: congestion maps and travel time estimates, public transport and information about its arrival, individual vehicle management, and emergency accident handling.

Research in the field of ITS has been carried out in different domains such as signal processing, communication technologies, robotics, electronics, control systems, and information systems (Papadimitratos et al., 2009). The multi-disciplinary nature of ITS enhances the complexity of the problem under study as it requires knowledge transfer from different research areas. The present review records the various architectures deployed for ITS. For this purpose, the paper is organized as follows: Section 2 describes the various network and communication architectures deployed in vehicular communication systems; and Section 3 discusses the possible directions for future research in the ITS field in the light of observations made during the review.

2. METHODOLOGY

In this review, the main focus of the researcher was on vehicular networks and how they impact on ITS. Accordingly, studies that discuss vehicular network architecture in the field of ITS have been reviewed. The identified articles were screened with the help of inclusion and exclusion criteria and the required information was retrieved from the chosen studies. Published research articles that discuss vehicular networks and empirical studies that capture all the empirical evidence were considered. Studies that clearly define the vehicular communication architecture and the various nodes in the network were considered for the review. Further, publications between 2008 and 2018 by relevant scientific sources (IEEE, Springer, ACM, and Elsevier) were included. However, systematic reviews, surveys and meta-analyses were omitted. Studies with incomplete data and poorly defined architecture were also excluded. Also, studies that did not have full text availability were not used in the review.

After the initial screening with the help of inclusion and exclusion criteria, the abstract and the concepts discussed in the paper were read, based on which the selected papers were clustered to form categories for the mapping of studies. The categories were updated periodically if the papers revealed a new architecture. The categories identified by the researcher are as follows: Hybrid, WSN, Software-Defined Networking (SDN), Vehicular cloud, Heterogeneous network architecture, and Cooperative network architecture. The research methodology is shown in Figure 1.

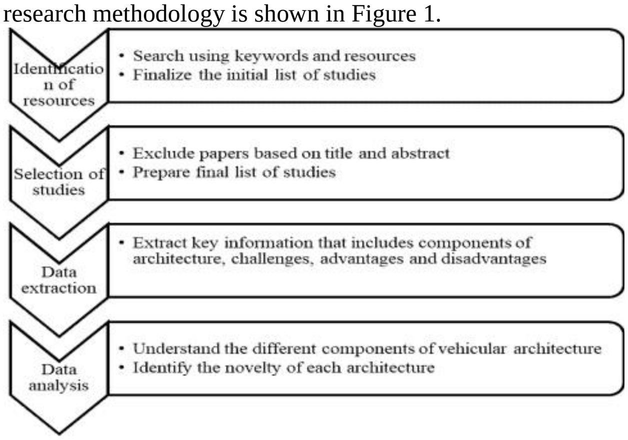

Fig.1.1 Study methodology

3. REVIEW OF VEHICULAR NETWORK AND COMMUNICATION ARCHITECTURES FOR ITS

ITS is a technology that fuses vehicles and the communication among the vehicles; thereby, assist the drivers and the passengers a comfortable and safe traveling environment. Inter-Vehicle communication (I-VC) and Road-Vehicle Communication (R-VC) are the two important communication systems that play an important role in for assisting safe driving and supporting automatic driving (Fujise et al., 2002). In the inter-vehicle communication, the communication between the vehicles is not dependent on the roadside infrastructure, unlike the road-vehicle communication. The present section describes the various architectures adopted for vehicular communication in ITS by different studies.

A mobile ad hoc network built upon IPv6 proxy-based architecture that selects the optimal mode of communication and provides dynamic switching between vehicle-to-vehicle and Vehicle-to-Roadside communication mode was proposed by Baldessari et al. (2006). The architecture used position-based routing for communication in the vehicular ad hoc networks and includes the following distinct domains: in-vehicle, ad hoc and infrastructure domain. The in-vehicle domain consists of the On-Board Units (OBUs) and other Application Units (AUs); whereas the ad hoc domain consists of vehicles with OBUs and Road Side Units (RSUs). The architecture was developed to support three modes of communication, namely, Direct In-Vehicle, Vehicle-to-Vehicle, and Vehicle-to-Roadside communication. Al-Sultan et al. (2014), in their comprehensive review on VANETs, described the network architecture in detail. Vehicle-Vehicle and Vehicle-RSU communication is established through a wireless medium known as WAVE. The service application is hosted by the RSU and the OBU is a peer device that utilizes the services. The OBU is a wave device that is mounted on-board a vehicle. It has a network device for short range wireless communication. The AU helps the vehicle to avail the services offered by the service provider by means of the communication capabilities of OBU. The AU connects with the network only through the OBU, which is responsible for the networking operations and mobility of devices. RSUs are fixed along the sides of the roads and are equipped with a network device based on IEEE 802.11p.

The important security aspects of the vehicular communication system have been described with different views such as functional view, component view, reference model view and information centric view by Gerlach et al. (2007) while implementing a vehicular communication system that integrates the security concepts into its stack of protocols. According to the functional view of the system, as shown in Figure 2, the lowest layer is concerned with the registration of nodes (OBUs and RSUs), the test and certification layer is concerned with the assessment of the operation of nodes, the pseudonym layer is concerned with providing anonymity to the nodes, the revocation layer is concerned with removing the nodes from the system, and the top data assessment and intrusion handling layer is concerned with assessing, auditing, detecting and handling any misbehavior of the nodes. The organizational view of the system depicts the following components of the system that are part of its security infrastructure: vehicle manufacturer and registration authority, inspection site, escrow entity, and the communication security infrastructure. The distribution of functions over different authorities is explained using the organizational view of the system. The reference model view of the system is enhanced by the following components: core security application, confidence filter, and network security components.

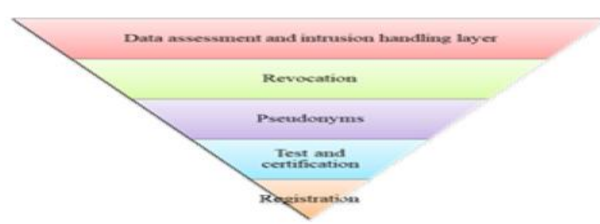

Fig1.2 Functional layer of security architecture

Security architecture for vehicular communication that provides identity and cryptographic key management, and integrates various privacy enhancing technologies was proposed by Papadimitratos et al. (2007). The main components of the architecture include Certification Authorities (CAs) that issue certificates to all nodes upon registration and expiration of the certificate, Privacy Enhancing Mechanism known as Pseudonym provider that provides each node with a distinct certified public key without any additional information, pseudonym authority that infers the mapping of a vehicle's long-term identity with its pseudonym, Secure communication patterns such as beaconing, restricted flooding, and position-based routing, and Trusted Components (TCs) such as event data recorders that store cryptographic information and perform cryptographic operations. In the simplest architecture, a CA was considered to be the Pseudonym provider as well as the resolution authority.

In order to make a Vehicular Communication (VC) system adaptable, extensible and flexible for incorporating security requirements in the future, component-based security architecture, where the components can be added or deleted, has been proposed by the SeVeCom project. According to Kargl et al. (2008), the baseline architecture for VC system includes various modules that address the security issues and contains components that implement a part of the system functionality, to achieve the required flexibility. Some of the modules include Identity Management, Cryptographic Support Module and Secure Communication Module. The Secure Communication Module ensures secure communication by implementing protocols, and consists of several components that implement a single protocol each. The Security Manager is considered to be at the center of the architecture which configures the security modules and establishes connection with the Cryptographic Support Module. With the help of hooking architecture at the interface between every layer of VC system, event-callback mechanism has been implemented to introduce new security measures without modifying the entire communication system. The communication system has been implemented as a layered stack in which Inter Layer Proxies (ILP) have been inserted at several points. The Hardware Security Module (HSM) secures the private keys and the execution of cryptographic operations. Tamper resistance of HSM was provided by implementing HSM as an Application-Specific Integrated Circuit. In the absence of an appropriate HSM hardware, the same can also be implemented in the form of a software library. Finally, the in-vehicle security module protects the interface between the in-car networks and wireless communication systems. It consists of two components, namely, firewall that controls the flow of data from other applications to the vehicle and vice versa, and an Intrusion Detection System (IDS) that monitors the in-car systems and detects real-time attacks.

A. Hybrid architecture

A hybrid architecture that combines the architectures of vehicle-to-vehicle (V2V) and vehicle to infrastructure (V2I) known as vehicle-to-vehicle-to-infrastructure (V2V2I) architecture was proposed by Miller (2008). The hybrid architecture combines the benefits of fast queries and responses from the V2I architecture and a distributed architecture without a single point of failure from the V2V architecture. The new hybrid architecture (shown in Figure 3) splits the transportation network into zones and assigns a vehicle as a 'Super Vehicle'. Super Vehicles have the privilege of communicating with the central architecture and with other super vehicles. Also, all the other vehicles can only communicate with the Super Vehicle that is responsible for the particular zone in which the vehicle is traversing currently. A 'Super Vehicle Detection' algorithm has been designed and implemented for assigning the Super Vehicle and describing how the other vehicles can identify a Super Vehicle. All the vehicles traversing in a zone will send their location and speed information to the Super Vehicle of the zone over a wireless link. The Super Vehicle is responsible for aggregating the vehicle information and sending it to the central server.

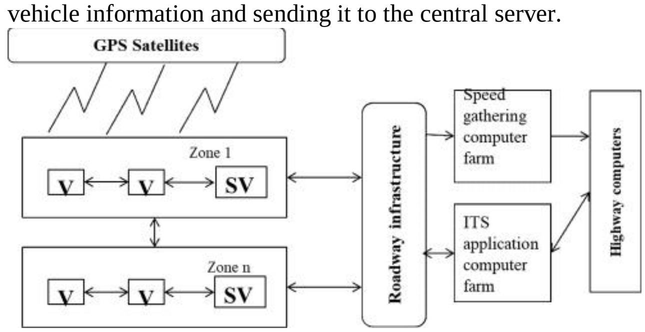

Fig.1.3 V2V2I Architecture

Santa, Gómez-Skarmeta and Sánchez-Artigas (2008) realizing the VC to be the cornerstone of future vehicle equipment, studied the unified architecture of V2V and V2I communication systems based on cellular networks. Recent developments in cellular networks have enabled the cellular networks to deal with not only V2I solutions, but also with the V2V communications. A novel communication paradigm that unifies both V2V and V2I communication systems has been developed. The communication infrastructure has been created with the help of peer to peer network technology that enables the vehicles to exchange information among them and with the roadside units. A software platform for implementing on-board services has been extended with a middleware service to provide a high level communication interface for exchanging messages in both V2V and V2I systems. In the present architecture, the traffic network is split into coverage zones, each consisting of a specific communication group. Geometry information about each area is stored in the Group Server. Local events within the communication group are handled by the Environment Server. The vehicles move from one coverage area to the other through a roaming process. The information about the coverage area is stored in the group server, which transmits the area geometry to the vehicle, and the vehicle connects to the Group Server when it has been detected to be out of the coverage area; thereby, saving communication resources. In case of events such as repairs or traffic jam, the vehicles use a special safety device to notify the event to the environment server, which in turn broadcasts the event; thereby, enhancing the warning mechanism.

Most of the existing studies on V2V communication and Device to Device (D2D) fail to discuss the issue of 'hole to next hop' and the resultant 'dead-ends' issue. Abd-

Elrahman et al. (2015) proposed a hybrid model that extends the V2V inter-VC model with D2D architecture. The unified architecture improves the 'dead-ends' failure recovery delays with the help of LTE-based D2D mechanisms. In case of a dead-end, the ITS protocol stack of the last V2V transmitting node performs a channel sensing followed by a handover to the D2D mechanism. In a D2D communication network, the devices are within a particular range and connected to the same base station (eNB); thereby, enabling the D2D devices to identify each other easily. The coverage area of the V2V communication system is thus enhanced with the help of LTE-enabled D2D mechanism. The chances of a message packet to reach the next hop (belonging to the next set of connected vehicles) in the direction of final destination have been improved.

B. Wireless sensor network architecture

In order to provide support for both accident prevention and post-accident investigation, Bohli et al. (2008) proposed WSN Roadside architecture. The architecture was purely based on software security solutions and hence does not need RSUs and tamper resistant modules for the sensor nodes. The communication between the vehicle and roadside units are based on wireless sensor networks. In order to prevent road accidents, the sensor units along the road measure the road conditions at several positions and communicate the aggregated information to the passing vehicle, which generates and distributes the warning message using geocast. The cost of WSN islands can be reduced by equipping each vehicle with an OBU with two RFs (IEEE 802.11p and IEEE 802.15.4), which in turn eliminates the need for RSUs other than the WSNs. Further, post-accident investigation is also supported by the sensor nodes that continuously store the information about the road condition. Though this information may be of little interest for the forensic team, it can be of interest for a specified group of people (like the insurance companies). Authorized queries to the roadside WSN units can be passed with the help of an IEEE 802.15.4 enabled reader device.

Parallel control and management system has been proposed as a new mechanism for intelligent transportation systems as it is a data-driven approach that considers both the engineering and social complexities for making decisions. Wang (2010) described the architecture of Parallel Transport Management System (PtMS) that was observed to be effective to be implemented in a complex networked traffic system. The Artificial societies, Computational experiments and Parallel execution (ACP) approach for ITS embeds both cyber physical systems (CPS) and cloud computing along with cyber physical-social systems (CPSS). The parallelism offered by this approach supports a wide-range of new application scenarios. The architecture of ACP-based PtMS has five major components, namely, the actual transportation system, ATS (Artificial Transportation System), OTSt (traffic operator and administrator training systems), DynaCAS (dynamic network assignment based on Complex Adaptive Systems), and aDAPTS (agent-based Distributed and Adaptive Platforms for Transportation Systems). OTSt is responsible for the learning and training of administrators and traffic operators. DynaCAS is responsible for designing and evaluating transportation experiments, traffic patterns and support the adoption of advanced traveler information systems. aDAPTS provides the supporting environment for developing, managing and managing the agent functions for various traffic tasks, with the help of a Global Traffic Operating Center and other Regional Traffic Operating Centers that can be either virtual or real.

Wireless sensor-based hybrid architecture was proposed by Qureshi, Abdullah and Anwar (2014). The vehicles communicate with the help of OBUs, and various routing applications, through wireless networks. There are two types of sensors deployed, sink and source nodes. While the source nodes measure the traffic conditions, the sink nodes have a processing capability. Both the sensors can communicate with both the vehicle nodes and base station. The base station gathers information from the sensors and vehicles, which is used by the data center for traffic management and forecast.

Safety and comfort of the passengers can be enabled by quicker distribution of data. Ratnani, Vaghela and Shah (2015) presented a novel architecture for controlling vehicular traffic and enabling quicker distribution of data. The architecture is based on Vehicular Sensor Networks and utilizes the maximum available bandwidth for message transmission and realizes low latency levels for the distribution of messages. In the present architecture, vehicles can automatically detect their transmission range; thereby, effectively broadcast the message with minimum hops. The messages generated by the applications are broadcasted several times. Vehicles fitted with OBUs process the message packets at different layers (MAC, network and transport layer). A priority scheme was adopted to select the next hop forwarder and the message is rebroadcasted based on the distance from the previous sender. The transmission range is calculated dynamically and is used for transmitting the message with as few hops as possible.

C. Software-defined network architecture

The VANET architectures were not found to be flexible enough to deploy large scale services and protocols. Therefore, research scholars propose SDN as an emerging network paradigm for addressing the issue of scalability in VANETs. Ku et al. (2014) demonstrated how the concept of SDN can be implemented to improve the features and services of VANETs. A Software-Defined VANET improves its resource utilization, selects the best routes, and facilitates network programmability by implementing the concepts and functionalities of SDN. The main components include: SDN controller (the central intelligence of the VANET system), SDN wireless node (data plane elements, vehicles), and the

SDN RSU (data plane elements, RSUs). The architecture deploys different wireless technologies to control and forward the planes in the future (flexibility). Long range wireless connections (LTE/ WiMAX) are used for the control plane and high bandwidth wireless connections (Wi-Fi) were used for the data plane. SDN also has an open-flow enabled switch that allows for different modes of operation to be carried out in VANET environment. Depending on the configuration of the services to be supported, the number of Wi-Fi interfaces used as data channels may vary. An SDN module consists of an interface that accepts data from a separated control plane, and packet processing units. The SDN wireless nodes have a local SDN agent which acts as a backup controller in the absence of SDN controller communication. These agents support traditional ad hoc routing protocols that provide fallback mechanisms for the SDN network to resume ad hoc operations in the absence of communication with SDN controller. As any information from any wireless node passes through its own SDN module, the SDN controller can evaluate user-traffic access into the network. The SDN wireless node internals are shown in Figure 4.

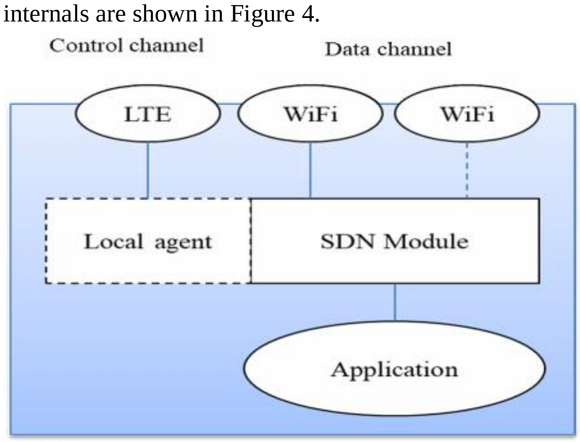

Fig.1.4 SDN Wireless node internals

SDN-based vehicular Adhoc with fog computing called FSDN VANET was proposed by Truong, Lee and Ghamri-Doudane (2015). Fog computing was proposed as it delivers delay sensitive and location-aware services. The components of the architecture include SDN controller: global intelligence and manages resources for the fog, SDN wireless nodes: data plane elements, SDN RSU: a fog device controlled by SDN controller, SDN RSU Controller: stores local road system information and provides emergency services, and Cellular Base Station: offers fog services. The work of SDN controller is shared with BSs and RSUCs in the hybrid control mode. The RSUCs, BSs and SDN controller offer virtualization to provide cloud services. The proposed architecture was found to optimize resource utilization, reduce latency and augment V2V, V2I, vehicle-base station communication, and SDN centralized control.

Salahuddin, Al-Fuqaha and Guizani (2015) proposed a novel SDN-based RSU cloud for IoV. In order to dynamically instantiate, replicate, and migrate the services, the architecture uses traditional and specialized RSUs that employ SDN. The deep programmability of SDN is supported by the decoupling of control and splitting of communication planes into the physical data plane and abstract control plane. The RSU microdatacenters have additional hardware and software components to provide SDN-enabled communication services and virtualization. The hardware includes a small form factor computing device and open-flow switch. The software components include the host OS and a hypervisor for providing virtualization. The datacentres also have OpenFlow controllers, cloud controllers, and RSU CRMs. While the RSU CRM communicates service hosting/ migration information to the OpenFlow and cloud controllers, in the data plane, the cloud controllers govern the service migration and hyervizers to instantiate new VMs to host services. The switch flow rules are updated by the OpenFlow controllers through the control plane.

D. Vehicular cloud architecture

A new shift in the technology that utilizes the advantages of cloud computing to serve the drivers of VANETs was observed. The resultant technology was known as Vehicular Cloud Computing (VCC). The evolution of VANETS with two emerging paradigms, namely, cloud computing and information centric networking was studied by Lee et al. (2014). The resultant system was known as the Vehicular Cloud Networking (VCN). The vehicle cloud is created by interconnecting the resources that are available in the vehicles and roadside units; thereby, maximizing the collaboration efficiency. Each vehicle in the cloud has three resources: data storage, computing and sensors. The data storage stores the vehicle information, the sensors detect and self-actuate the events in the physical environment, and the computing resource is a collection of mobile resources, thereby merging mobile cloud model with vehicular networks to handle network service provisioning. The resources are connected via P2P connections.

The potential of cloud computing technologies to improve road safety and the travel experience in ITS has been realized by various researchers. A multi-layered data cloud architecture that combines the technologies of cloud computing and IoT has been proposed by He, Yan and Da Xu (2014). The proposed vehicular data cloud platform integrates the following devices to support V2V and V2I communication mechanisms: controllers, actuators, sensors, mobile phones, internet access devices, road side infrastructure (street lights, smart metering), communication technology (satellite and wireless networks, internet), middleware, and cloud computing IoT. Such a multi-layered platform can provide secure and on-demand services using the associated clouds (conventional and temporary cloud). The IoT based vehicular cloud architecture is shown in Figure 5. While the conventional cloud which comprises of virtual computers provide cloud services for the client, the temporary cloud is formed on demand and comprises of storage and networking facilities and under-utilized computers. The bottom layer of the architecture provides the required functional support for the layers above. Heterogeneous web services, applications, middleware systems that provide information and communication services and connect in-vehicle and out-vehicle devices in the vehicular data cloud are integrated by applying Service-Oriented Architecture (SOA).

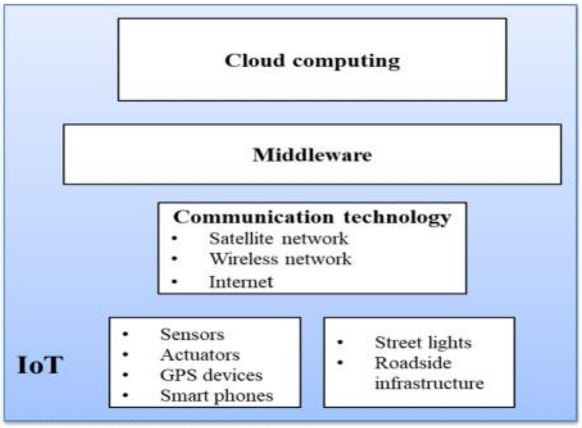

Fig.1.5 IoT based Vehicular Cloud architecture

A similar cloud computing model known as VANET Cloud was proposed by Bitam, Mellouk and Zeadally (2015). The permanent sub-model consists of virtual machines, storage and processing units, and bandwidth that are available to the VANET entities (vehicles and RSUs). The temporary sub-model consists of computing resources and passenger devices and is added to the permanent model. All the components are organized into layers: client layer, communication layer and the cloud layer. The client layer consists of the end users that use Service Access Points (SAPs) for sending service requests and receiving service responses. The communication layer establishes connections between the clients at the lower layer and the VANET cloud server. The communication technologies deployed at this layer include VANETs, wireless sensors, 3G/ 4G networks, RSUs, cellular base stations, private networks and so on. The cloud layer consists of the data centers that provide data services. The permanent and temporary sub-models are connected via a network that comprises of all the data centers from both the layers.

Ahmad et al. (2015) presented a Vehicular Cloud Networking (VCN) technology by integrating vehicles and the adjacent infrastructure with the traditional internet clouds. The architecture consists of three types of clouds (three-tier architecture), namely, Vehicular Cloud, infrastructure cloud (IC) and the traditional back-end (IT) cloud (BEC). The communication network and the scope of each cloud are shown in Table 1. VC consists of the physical resources of the vehicles that are shared among the vehicles; thereby, resulting in an overall higher efficiency of the network. IC consists of static RSUs and mobile entities, and the communication between different ICs is carried out with the help of local servers. BEC consists of extensive resources that can be used by the vehicles for data processing and storage and serves high bandwidth requirements.

Table 1.1 Communication networking of VCN (Ahmad et al., 2015)

Tier	Cloud	Communication network	Scope
1	Vehicular Cloud (VC)	Vehicle ↔ Vehicle Vehicle ↔ VC	Local
2	Infrastructure Cloud (IC)	Vehicle ↔ RSU Vehicle ↔ IC Base Station ↔ RSU Base Station ↔ IC Base Station ↔ Local Server	Local to small geographical areas
3	Back-End Cloud (BEC)	Local Server ↔ BEC	Large geographical areas

Clustering techniques have been proposed to solve the problem of resource limitation in vehicular cloud networks. Arkian et al. (2015) proposed a vehicular cloud architecture that consists of a flexible cluster. The cluster head is selected by means of a fuzzy logic and Q-learning techniques (to select a service provider) and queuing strategies were used to solve the resource allocation problem. As vehicles form dynamic clusters, the most suitable ones are assigned as the cluster heads (CH) which functions as the cloud controller and is held responsible for creating, maintaining and removing the vehicular cloud. The virtualized physical resources of the vehicles are registered with the CH, which in turn schedules the resources for the vehicles in the cloud. Vehicles are grouped into clusters based on their location, speed and direction of travel. This information is broadcasted to the neighboring vehicle within the communication range. The CH is elected for the cluster based on the Fit Factor of the nodes, which is calculated by a Fuzzy Logic Controller based on a set of fuzzy logic rules embedded in the fuzzy inference engine.

More recently, Hagenauer et al. (2017) presented a virtual network infrastructure that deployed clusters of parked cars to form a virtual network. The basic idea behind this infrastructure is that cars driving by connect to a parked car and accesses all the services or applications within the cluster through this parked car. In order to maintain an uninterrupted connection, the connection will be handed over to another parked vehicle after the lapse of a certain amount of time. The parked cars must be equipped with a short range networking technology such as IEEE 802.11p, a basic GPS server, an address-based routing protocol, and distributed storage functionality such as Distributed Hash Table (DHT). In order to minimize the load on the channel, a subset of the parked cars has been selected as the active gateways to the cluster.

E. Heterogeneous network architecture

Sadek et al. (2015) proposed a heterogeneous LTE/ Wi-Fi vehicular system to meet the different application requirements simultaneously. The proposed system supports both infotainment and ITS traffic control data. The heterogeneous vehicular system is a combination of long range (LTE) and short range services (Wi-Fi). While the LTE offers a high coverage area, Wi-Fi offers a relatively higher capacity that is cost-effective. The overall performance of the system is enhanced by coupling high capacity with long range communication. The architecture addresses the following VC networks: backhaul connection, Infrastructure-to-Vehicle (I2V) communication, and On-board Vehicle Communication (OVC). The I2V network connects vehicles with the LTE eNodeB (fixed along the roads) and provides access to the LTE network; whereas, the OVC network consists of OBUs fitted to the vehicles, Wi-Fi access points (APs), and passenger devices. Internet access and connectivity is provided using the LTE as a backhaul link, to the vehicles that use Wi-Fi to connect to the last mile link. The ITS data are sent to the vehicle's OBU through the Ethernet and the infotainment data is sent to the passenger's devices through Wi-Fi. Similarly, Ucar, Ergen and Ozkasap (2016) developed a hybrid architecture known as VMaSC-LTE by combining IEEE 802.11p based VANETs with the LTE cellular technology (4G cellular system) to achieve high data packet delivery ratio and low delay.

Heterogeneous vehicular networks (HetVNETs) have been believed to meet the various Quality of Sevices (QoS) requirements for ITS. However, on the face of ever changing network landscape, HetVNETs cannot effectively address the QoS requirements. Zheng et al. (2016) proposed the use of cloud RAN (Radio Access Network) architecture to support the dynamic nature of HetVNETs. The new architecture integrates various wireless access schemes. It consists of a Remote Radio Head (RRH) which converts the digital signals to amplified analog signals before air transmission. The base band processing cloud is responsible for implementing the functionalities of RAN. The RRH and the base band processing cloud are deployed separately and are connected by optical fiber cables; thereby, supporting soft-defined HetVNETs (SERVICE) and enabling dynamic shared resource allocation via open platform and real-time virtualization technology. The flexibility to customize the computing environments is also provided with the help of SERVICE. The SERVICE consists of a number of base stations with wireless access techniques, and its infrastructure has various processing and storage abilities. The multi-layered cloud architecture is deployed on the SERVICE, where each cloudlet consists of a cluster of communication resources and computation devices. The SERVICE cloudlet is integrated with the local RAN to provide physical proximity.

A heterogeneous wireless network for seamless VANET connectivity was proposed by Agrawal, Tyagi and Misra (2016). The hierarchical architecture comprises of WLAN (802.11p) that covers 150-300 m and has a high bandwidth, at the lowest level, followed by cellular technology that covers several kms at the middle level, and WiMAX technology that has a much wider coverage area (50 kms) and higher bandwidth is present at the top layer. Continuous availability of the network and reliable communication of messages has been made possible by the integration of these three wireless radio access technologies.

F. Cooperative network architecture

A cooperative vehicular networking architecture was proposed by Zhou et al. (2015). In the proposed architecture, multiple (UAVs) Unmanned Aerial Vehicles form an aerial subnetwork. The vehicular subnetwork on the ground is aided by the UAV through A2A (Air-to-Air) and A2G (Air-to-Ground) communications. As the UAVs are flexible in terms of mobility, they can be used as intermediate relays during network partitions in the round vehicular subnetwork. Further, disaster rescue and polluted area investigation can be carried out with the help of such cooperative networks. A multiple-UAV-aided vehicular network includes the following components: UAVs, Ground vehicles, and Control centers (Ground stations). The UAVs are equipped with sensors (imaging and position), communication modules and embedded processors. The collected image data are passed to the ground subnetwork. The ground vehicles carry communication and processing modules that facilitate cooperation between the UAVs and ground vehicles. The information from ground vehicles are transmitted through a multi-hop ground vehicle route. In order to maintain coordination within the two-layered network, it is inevitable to set up control centers that are mainly responsible for data processing, vehicle and UAVs scheduling, and connecting aerial and ground sub-networks. The present architecture houses three types of networks: aerial networks (A2A), ground networks (V2V), and air-ground networks (A2V). The A2A network uses heterogeneous radio interfaces (IEEE 802.15.4/ IEEE 802.11), V2V uses intermitted V2V links (IEEE 802.11p), the links in A2V network must facilitate component scheduling, subnetwork coordination, and communication relay.

During the following year, Kitazato et al. (2016) proposed a new system known as Proxy CAM (Cooperative Awareness Message) to assist V2V messaging. CAMs are the messages exchanged by vehicles in Cooperative Intelligent

Transportation System (CITS). The Proxy CAM generates V2V messages on behalf of sender vehicles in the roadside unit. The system design was based on the ITS Station architecture and compliant with CAM. The system consists of Roadside Sensors that detect vehicles and sends the vehicle information to the server in the infrastructure, Sensor Fusion Database stores the vehicle information in the database, Proxy CAM Generator generates the CAMs by inserting data into the CAM field in the database, and Proxy CAM Transmitter that broadcasts the generated proxy CAMs with the help of IEEE 802.11p at the network layer, GeoNetworking at the network layer and Basic Transport Protocol (BTP) at the transport layer.

In order to utilize the resources and infrastructure of intelligent transport system (ITS) effectively, Sharma, Moon and Park (2017) proposed a novel vehicular architecture known as Block-VN that is based on Blockchain in smart city which allows for the development of a distributed network of large scale vehicles effectively. The present architecture consists of the controller nodes, minor nodes, and other ordinary nodes. The controller and minor nodes are connected in a distributed manner to achieve scalability and availability of the network. Every time a new vehicle is registered, its manufacturers provide all the details about the vehicle to the revocation authority which decides on the minor nodes outside the nodes of the controller. The revocation node provides all the vehicle information to the ordinary and minor nodes in the distribute network. The controller node is equipped with a hash, timestamp, nonce, and a Merkle root that stores all the service information; whereas, the minor nodes have the devices for sensing, storing and computing. The controller node operates at the individual level to process the data and transmits the data securely in a distributed manner using public-private key encryption.

4. KEY FINDINGS OF THE STUDY

A summary of the review is presented in Table 2.

Table 1.2 Significant findings

Category	Author and year	Key findings
Hybrid	Miller (2008)	Offers the advantages of both V2V (fast queries and responses) and V2I architecture (distributed architecture).
	Santa, Gómez-Skarmeta and Sánchez-Artigas (2008)	Cellular networks can be adopted for dealing with V2I and V2V communications.
	Abd-Elrahman et al. (2015)	Integration of V2V with D2D architecture improves the dead-ends failure recovery delays.
WSN	Bohli et al. (2008)	Software solutionss that are independent of tamper resistant modules for sensor nodes to aid in accident prevention and investigation.
	Wang (2010)	ACP-based PtMS integrates engineering with social complexities for decision-making in complex networked traffic system.
	Qureshi, Abdullah and Anwar (2014)	Implementation of WSN in vehicular networks reduces the investment and enhances the traffic efficiency.
	Ratnani, Vaghela and Shah (2015)	Enables quicker distribution of data by utilizing the maximum available bandwidth.
SDN	Ku et al. (2014)	Software-defined VANETs enhances resource utilization, network routing, and scalability fo the network.
	Truong, Lee and Ghamri-Doudane (2015)	By integrating Fog framework with SDN-based VANET delay sensitive and location-aware services can be offered to meet the future needs of VANETs.
	Salahuddin, Al-Fuqaha and Guizani (2015)	The deep programmability of SDN can be used to reconfigure the services hosted by the network to meet the demands of the vehicles.
Vehicular cloud	Lee et al. (2014)	VCN combines the benefits of cloud computing and information networking, and enhances collaboration efficiency.
	He, Yan and Da Xu (2014)	Multi-layered cloud architecture combines cloud computing and IoT to provide on-demand services with the help of temporary and conventional clouds.
	Bitam, Mellouk and Zeadally (2015)	Cloud computing technologies provide flexible solutions for improving road safety and travel experience.
	Ahmad et al. (2015)	The VCN connects the vehicles with adjacent infrastructure to improve the overall efficiency of the network.
	Arkian et al. (2015)	Flexible clusters are formed to solve the issues of resource limitation.
	Hagenauer et al. (2017)	Clusters of parked cars can be used to form a virtual network to minimize the channel load.
Heterogeneous network architecture	Sadek et al. (2015)	Combines long range LTE with short range services (Wi-Fi) to meet various application requirements simultaneously.
	Ucar, Ergen and Ozkasap (2016)	Cellular technologies integration with VANETs increase the packet data delivery ratio.
	Agrawal, Tyagi and Misra (2016)	Continuous availability of network can be achieved by integrating radio access technologies at various levels.
	Zheng et al. (2016)	Cloud RAN architecture can be proposed for HetVNETs to meet

Category	Author and year	Key findings
		various QoS requirements.
Cooperative network architecture	Zhou et al. (2015)	Cooperative networks that combines aerial subnetwork and vehicular subnetwork, can be utilized effectively for disaster recovery and investigation of polluted areas.
	Kitazato et al. (2016)	The V2V messages are generated by proxy CAMs on behalf of sender vehicles to solve the issues of obstacle interference and mixed environment.

5. CONCLUSION AND KEY CHALLENGES

This paper presented a review of the existing network architectures with their relative advantages and disadvantages. Routing protocols are the kernels for any VC. While adopting position-based routing protocols for vehicular networks, enhancing the position accuracy and availability of vehicles in all environments, addressing the compatibility of routing protocols in a complex vehicular network environment, minimizing delay under various constraints, security support, and data protection are some of the key challenges to be addressed. High mobility and constant topological changes have always remained the key constraints for developing efficient routing techniques for communication network architecture.

In case of vehicular cloud networks, lifetime periods and forwarding zones for the data must be defined appropriately to avoid network congestion. Standardization of technologies to overcome the problem of technologies incompatibility and communication, and data aggregation techniques for optimizing resource utilization must be adopted to address the issues of technologies coexistence.

Architecture scalability challenges with respect to the organization, technology, and road topology must be addressed while defining a vehicular network. Further, information selection and dissemination policies must be selected carefully to optimize the resources and avoid network congestion by selecting suitable paths.

REFERENCES

[1] Abd-Elrahman, E., Said, A.M., Toukabri, T., Afifi, H. and Marot, M., 2015, February. A hybrid model to extend vehicular intercommunication V2V through D2D architecture. In Computing, Networking and Communications (ICNC), 2015 International Conference on (pp. 754-759). IEEE.

[2] Agrawal, S., Tyagi, N., & Misra, A. K. (2016, March). Seamless VANET connectivity through heterogeneous wireless network on rural highways. In Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies (p. 84). ACM.

[3] Ahmad, F., Kazim, M., Adnane, A. and Awad, A., 2015, December. Vehicular cloud networks: Architecture, applications and security issues. In Utility and Cloud Computing (UCC), 2015 IEEE/ACM 8th International Conference on (pp. 571-576). IEEE.

[4] Al-Sultan, S., Al-Doori, M.M., Al-Bayatti, A.H. and Zedan, H., 2014. A comprehensive survey on vehicular ad hoc network. Journal of network and computer applications, 37, pp.380-392.

[5] Arkian, H.R., Atani, R.E., Diyanat, A. and Pourkhalili, A., 2015. A cluster-based vehicular cloud architecture with learning-based resource management. The Journal of Supercomputing, 71(4), pp.1401-1426.

[6] Baldessari, R., Festag, A., Matos, A., Santos, J. and Aguiar, R., 2006, March. Flexible connectivity management in vehicular communication networks. In Proceedings of International Workshop on Intelligent Transportation. Alemania.

[7] Bitam, S., Mellouk, A. and Zeadally, S., 2015. VANET-cloud: a generic cloud computing model for vehicular Ad Hoc networks. IEEE Wireless Communications, 22(1), pp.96-102.

[8] Bohli, J.M., Hessler, A., Ugus, O. and Westhoff, D., 2008, March. A secure and resilient WSN roadside architecture for intelligent transport systems. In Proceedings of the first ACM conference on Wireless network security (pp. 161-171). ACM.

[9] Figueiredo, L., Jesus, I., Machado, J. T., Ferreira, J. R., & De Carvalho, J. M., 2001. Towards the development of intelligent transportation systems. In Intelligent Transportation Systems, 2001. Proceedings. 2001 IEEE (pp. 1206-1211). IEEE.

[10] Fujise, M., Kato, A., Sato, K., & Harada, H., 2002. Intelligent transport systems. In Wireless Communication Technologies: New Multimedia Systems (pp. 171-200). Springer, Boston, MA.

[11] Gerlach, M., Festag, A., Leinmüller, T., Goldacker, G., & Harsch, C., 2007, March. Security architecture for vehicular communication. In Workshop on Intelligent Transportation.

[12] Hagenauer, F., Sommer, C., Higuchi, T., Altintas, O., & Dressler, F., 2017, October. Parked Cars as Virtual Network Infrastructure: Enabling Stable V2I Access for Long-Lasting Data Flows. In 23rd ACM International Conference on Mobile Computing and Networking (MobiCom 2017), 2nd ACM International Workshop on Smart, Autonomous, and Connected Vehicular Systems and Services (CarSys 2017), Snowbird, UT.

[13] He, W., Yan, G., & Da Xu, L., 2014. Developing vehicular data cloud services in the IoT environment. IEEE Transactions on Industrial Informatics, 10(2), 1587-1595.

[14] Jalali, R., El-Khatib, K., & McGregor, C., 2015, February. Smart city architecture for community level services through the internet of things. In Intelligence in Next Generation Networks (ICIN), 2015 18th International Conference on (pp. 108-113). IEEE.

[15] Kargl, F., Papadimitratos, P., Buttyan, L., Müter, M., Schoch, E., Wiedersheim, B.,... & Hubaux, J. P., 2008. Secure vehicular communication systems: implementation, performance, and research challenges. IEEE Communications Magazine, 46(11).

[16] Kitazato, T., Tsukada, M., Ochiai, H., & Esaki, H., 2016, October. Proxy cooperative awareness message: an infrastructure-assisted v2v messaging. In Mobile Computing and Ubiquitous Networking (ICMU), 2016 Ninth International Conference on (pp. 1-6). IEEE.

[17] Ku, I., Lu, Y., Gerla, M., Ongaro, F., Gomes, R. L., & Cerqueira, E., 2014, June. Towards software-defined VANET: Architecture and services. In Ad Hoc Networking Workshop (MED-HOC-NET), 2014 13th Annual Mediterranean (pp. 103-110). IEEE.

[18] Lee, E., Lee, E. K., Gerla, M., & Oh, S. Y., 2014. Vehicular cloud networking: architecture and design principles. IEEE Communications Magazine, 52(2), 148-155.

[19] Miller, J., 2008, June. Vehicle-to-vehicle-to-infrastructure (V2V2I) intelligent transportation system architecture. In Intelligent Vehicles Symposium, 2008 IEEE (pp. 715-720). IEEE.

[20] Papadimitratos, P., Buttyan, L., Hubaux, J. P., Kargl, F., Kung, A., & Raya, M., 2007, June. Architecture for secure and private vehicular communications. In Telecommunications, 2007. ITST'07. 7th International Conference on ITS (pp. 1-6). IEEE.

[21] Papadimitratos, P., De La Fortelle, A., Evenssen, K., Brignolo, R., & Cosenza, S., 2009. Vehicular communication systems: Enabling technologies, applications, and future outlook on intelligent transportation. IEEE communications magazine, 47(11).

[22] Qureshi, K. N., Abdullah, A. H., & Anwar, R. W. (2014). Wireless sensor based hybrid architecture for vehicular ad hoc networks. TELKOMNIKA (Telecommunication Computing Electronics and Control), 12(4), 942-949.

[23] Ratnani, C., Vaghela, V. B., & Shah, D. J., 2015, February. A novel architecture for vehicular traffic control. In Computational Intelligence & Communication Technology (CICT), 2015 IEEE International Conference on (pp. 277-282). IEEE.

[24] Sadek, N. M., Halawa, H. H., Daoud, R. M., Amer, H. H., & Ali, N. A., 2015, March. Heterogeneous LTE/Wi-Fi architecture for ITS traffic control and infotainment. In Electrical Systems for Aircraft, Railway, Ship Propulsion and Road Vehicles, 2015 International Conference on (pp. 1-6). IEEE.

[25] Salahuddin, M. A., Al-Fuqaha, A., & Guizani, M. (2015). Software-defined networking for rsu clouds in support of the internet of vehicles. IEEE Internet of Things journal, 2(2), 133-144.

[26] Santa, J., Gómez-Skarmeta, A. F., & Sánchez-Artigas, M., 2008. Architecture and evaluation of a unified V2V and V2I communication system based on cellular networks. Computer Communications, 31(12), 2850-2861.

[27] Sharma, P. K., Moon, S. Y., & Park, J. H., 2017. Block-VN: A distributed blockchain based vehicular network architecture in smart City. Journal of Information Processing Systems, 13(1), 84.

[28] Truong, N. B., Lee, G. M., & Ghamri-Doudane, Y. (2015, May). Software defined networking-based vehicular adhoc network with fog computing. In Integrated Network Management (IM), 2015

[29] Ucar, S., Ergen, S. C., & Ozkasap, O. (2016). Multihop-cluster-based IEEE 802.11 p and LTE hybrid architecture for VANET safety message dissemination. IEEE Transactions on Vehicular Technology, 65(4), 2621-2636.

[30] Wang, F. Y., 2010. Parallel control and management for intelligent transportation systems: Concepts, architectures, and applications. IEEE Transactions on Intelligent Transportation Systems, 11(3), 630-638.

[31] Zheng, K., Hou, L., Meng, H., Zheng, Q., Lu, N., & Lei, L., 2016. Soft-defined heterogeneous vehicular network: Architecture and challenges. IEEE Network, 30(4), 72-80.

[32] Zhou, Y., Cheng, N., Lu, N., & Shen, X. S., 2015. Multi-UAV-aided networks: aerial-ground cooperative vehicular networking architecture. ieee vehicular technology magazine, 10(4), 36-44.