Available online www.jsaer.com

***Journal of Scientific and Engineering Research*, 2019, 6(11):58-65**

Review Article

ISSN: 2394-2630
CODEN(USA): JSERBR

Vehicular Ad-hoc Network (VANET): A Primer

M. N. O. Sadiku[1], S. R. Nelatury[2], S.M. Musa[1]

[1]College of Engineering, Prairie View A&M University, Prairie View, TX 77446
Email: mnsadiku, smmusa @pvamu.edu
[2]School of Engineering and Engineering Technology, Pennsylvania State University, Erie, PA 16563-1701
Email: srn3@psu.edu

Abstract Nowadays, a growing number of vehicles are equipped with the communication devices to facilitate vehicle-to-vehicle and vehicle-to-infrastructure communication and increase the safety of the passengers. New type of networks called Vehicular Ad Hoc Networks (VANETs) provide us with the infrastructure for developing new systems to enhance drivers' and passengers' safety and comfort. Vehicular networks are special types of mobile ad hoc networks (MANETs) that are used to help drivers access necessary information. They improve the driving safety of vehicles through communications between on-board units (OBUs) and roadside units (RSUs). This paper provides a primer on VANET, its applications, benefits, and challenges.

Keywords vehicular networking, VANET, MANET, smart cities

Introduction

Cars are used in our daily life. If data communication network exists between vehicles, mobile phones, and home based telephones, it will increase the safety of the passengers.

Today, car manufacturers are willing to increase road safety by equipping and making them become "computers on wheels." Modern vehicles are equipped with many on-board sensors and computers, navigation systems, and multiple user interfaces. Through smart-city initiatives, roadside sensors now deployed in highways and in urban areas. The electronic gadgets will dramatically increase the cars' awareness of their environment, thereby increasing safety and optimizing traffic. A car is regarded smart if it is equipped with an on-board unit (OBU) with computational and processing functionality, a navigation system such as GPS device, graphical user interface (GUI), and IEEE 802.11p-based wireless interface card [1].

Recent advances in wireless communication networks have led to the introduction of a new type of networks called Vehicular Networks, which provide us with the infrastructure for developing new systems to enhance drivers' and passengers' safety and comfort. Vehicular networks are self-organized communication networks built up from roaming vehicles. Such ad hoc networks are characterized by the high mobility of the nodes (vehicles), uneven distribution of vehicles, the limited communication between nodes, and being able to establish any where because they do not depend on a fixed infrastructure.

Overview of Vanet

Vehicular Networks (also known as VANETs) are indispensable components of a smart city environment due to their ability to enhance the experience of safe driving, improve the efficiency of the roadway systems, and improve the quality of life and security. They are special type of Mobile ad hoc Networks (MANET). VANET can be deployed by network operators, service providers or through integration between operators, providers, and a governmental authority.

VANETs are essentially the result of applying the principles of MANETs to the domain of vehicles. They enable communications from mobile vehicles to other vehicles and also to fixed roadside infrastructure. The primary goal of vehicular networks is to provide safer driving conditions. To accomplish this, vehicles are required to periodically broadcast safety messages providing precise position information to nearby vehicles. Broadcasting is more prevalent than other transmission methods due to the need to facilitate rapid, brief communications with nearby vehicles. VANET is a combination of sensor networks and ad hoc networks. It uses wireless channel for both transmission and communication.

As illustrated in Figure 1 [2], VANET consists of the following components [3]:

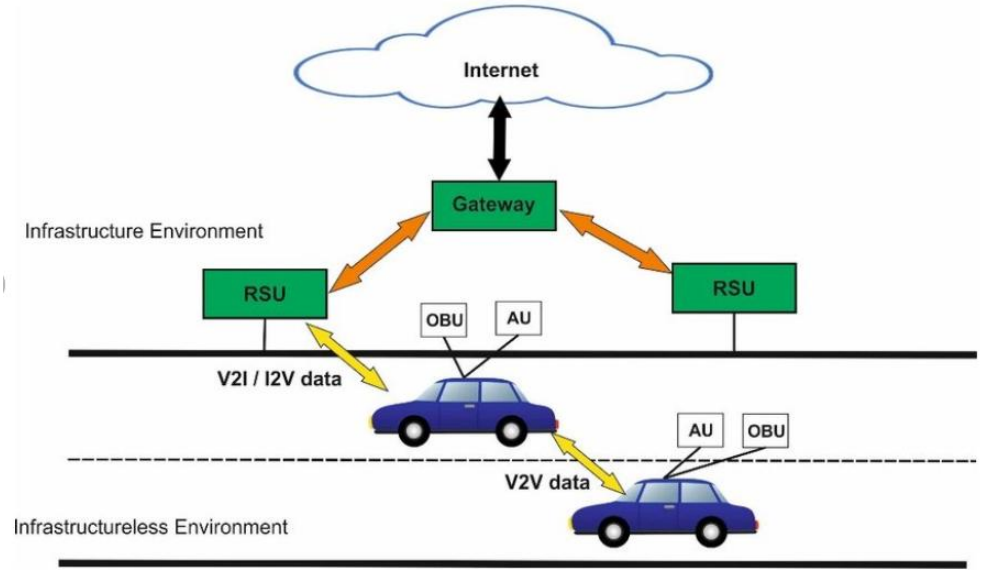

Figure 1: The components of VANET [2]

1. Application Unit (AU): This is the gadget equipped within the vehicle that uses the applications provided by the provider. The AU communicates with the network exclusively via the OBU which takes the task of all mobility and networking actions.

2. On Board Unit (OBU): The major function of the OBU is wireless radio access, ad hoc and geographical routing, network blocking control, consistent message convey, data safety, and IP mobility. OBUs may communicate with Internet via RSUs.

3. *Roadside Unit* (RSU): This is a static node. An RSU can be connected to the Internet via the gateway. RSUs can communicate with each other directly or via multi-hop as well. The RSU is a device commonly set along the road side or in dedicated locations, such as at junctions or near parking places. The RSU is equipped with one network gadget for a dedicated short range communication based on IEEE 802.11p radio technology.

VANET is composed of two types of nodes: mobile and fixed. The mobile nodes represent vehicles, while fixed nodes represent road side units (RSU) and base stations (BS). The fixed equipment can belong to the government, private network operators or service providers. Each node can be static, moderately mobile or highly mobile. The network uses three types of connections: vehicle-to-vehicle (V2V), vehicle- to-infrastructure (V2I), and infrastructure-to-infrastructure (I2I) [4]. V2V refers to the direct or multihop communications among vehicles. V2I refers to the communication between vehicles and RSU, base station, and access point (AP) connected with Internet. A typical VANET is depicted in Figure 2 [5].

The FCC has allocated a bandwidth of 75MHz for vehicular communications, usually referred to as DSRC (Dedicated Short Range Communications). Vehicular communications (referring to information exchange among vehicles, pedestrians, and infrastructures) are now the dominant mode of transferring information between mobile vehicles. VANET can use any wireless networking technology such as Wi-Fi or ZigBee. It can also be cellular technologies such as LTE. The network enables useful functions such as cooperative driving, probe vehicle data, notification of traffic conditions, road accident warnings, web access, location-based service, driving safety, intelligent transport services, mobile Internet access, and file sharing.

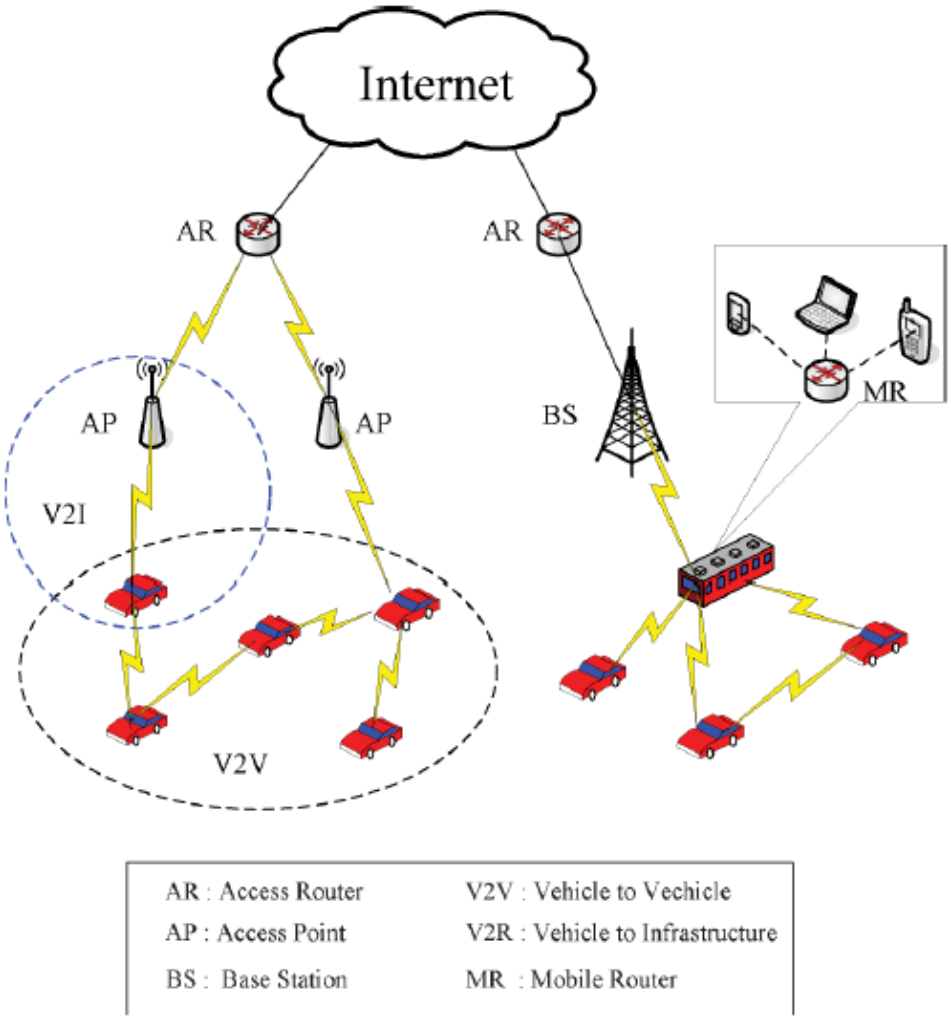

Figure 2: A typical vehicular network [5].

VANETs are a critical component of the intelligent transportation systems (ITS). ITS include a set of different technologies that aim at improving the efficiency and security of the current transportation system by combining vehicular networks and advanced logistics. ITS and related technologies have been deployed recently for toll collection, fleet logistics and management, anti-theft protection, pay-as-you-go insurance, traffic information, and active road-side signs.

With the continuous development of vehicular technology and the emergence of new applications, it becomes urgent to connect VANET to the Internet. The Internet is connecting everything on the globe, including vehicles. For vehicles to effectively communicate on the Internet and for global reachability, assigning IP addresses to every vehicle is required. With large address space, IPv6 can support a unique address for each sensor or mobile device in the vehicles.

VANET Characteristics

VANETs have some unique characteristics that distinguish them from MANET. These include: High Mobility, Rapid Changing, Network Topology, Unbounded Network Size, Frequent Exchange of Information, Wireless Communication, Time Critical, Sufficient Energy and better Physical Protection. Some of these characteristics are explained as follows [6,7].

1. *High mobility:* VANET nodes are characterized by high relative speed (up to 500 km/h) which makes VANET environment dynamic. Its mobility is constrained by the underlying road network topology. The high speed makes it difficult to predict a node position.

2. *Rapidly changing topology:* Due to the random speed of a node (vehicle), its position changes frequently. This causes the network topology to change frequently in VANET.
3. *Wireless Communication:* VANET runs on is a wireless technology, therefore nodes are connected and information exchange are done wirelessly.
4. *Predictable and restricted mobility patterns*: Unlike the random mobility of MANET, VANET node movements are governed by restricted rules.
5. *No power constraints*: Each vehicle is equipped with a battery that is used as an infinite power supply for all communications and computation tasks.
6. *Localization:* Vehicles can use the Global Positioning System (GPS) to identify their locations with high accuracy.
7. *Abundant network nodes:* VANET networks can be very large due to high density of the vehicles. VANET is geographically limitless.
8. *Hard delay constraints*: Safety messages are the main goal of VANETs. Therefore, safety messages should be given high priority and must be delivered on time.
9. *Lower latency:* Five times reduced end-to-end latency.

Like other communication networks, the communication among the nodes in VANET follows the Open Systems Interconnection (OSI) standardization, which is divided into seven layers (physical, data link, network, transport, session, presentation, and application) and provides general guidelines for network operation [8]. In VANET, the session and the presentation layers are omitted.

Security and Privacy Needs

Authorities, car manufacturing industries, and researchers in academia agree that security and privacy enhancing mechanisms are a prerequisite for the acceptance and deployment of VANET. Security is a major concern all around the world. Security, safety, and privacy are indispensable in vehicular communications for successful acceptance of such the technology. The security and privacy issues of VANETs must be addressed before they are implemented [9]. Safety is one of the main goals of VANET because safety reduces accidents and save lives. Vehicles should be able to authenticate themselves so that their activities are not tracked by illegal parties that are eavesdropping on them.

In traditional networks the major security concerns confidentiality, integrity, and availability [10].

1. *Confidentiality:* This denotes the concealment of information. This is not a relevant goal for VANETs.
2. *Integrity:* This refers to the trustworthiness of data, i.e., the prevention of unauthorized changes. in VANETs. Integrity can be addressed by asymmetric cryptographic schemes.
3. *Availability:* This denotes the ability to use a system at all times. In VANET, availability is under-investigated.

None of these involves life safety. In order to be able to thwart any attack, the security system for vehicular must meet the following requirements: Authentication, Verification of data consistency, Availability, Non-repudiation, Privacy, and Real-time constraints. These are illustrated in Figure 3 with typical attacks [11] and explained as follows [12].

1. Authentication: Vehicle reactions to events should be based on legitimate messages. Therefore we need to authenticate the senders of the messages.
2. Verification of data consistency: The legitimacy of messages also encompasses their consistency with similar ones, because the sender can be legitimate while the message contains false data.
3. Availability: Some attacks (e.g., denial of service) can bring down the network. Therefore, availability should be also provided by alternative means.
4. Non-repudiation: A sender should not be able to deny the transmission of a message.
5. Privacy: The privacy of drivers against unauthorized observers should be guaranteed.
6. Real-time constraints: At the very high speeds typical in VANETs, strict time constraints should be respected.

These general requirements can be mapped to specific VANET-enabled applications

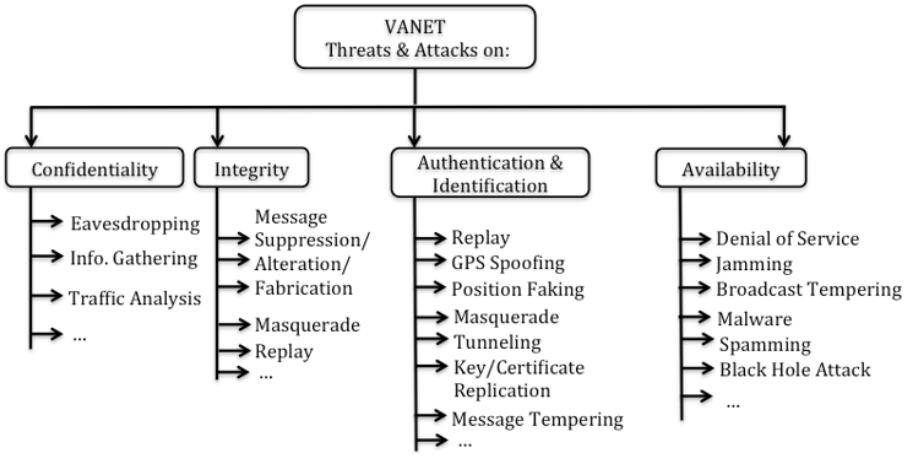

Figure 3: VANET attacks classification [11]

Applications

Vehicular networks have been expanding to perform several applications and strategies related to vehicles, ambulances, traffic jam, drivers, and even passengers. Applications range from road safety applications oriented to the vehicle or to the driver, to entertainment, and commercial applications for passengers. Specific applications of VANETs include [13]:

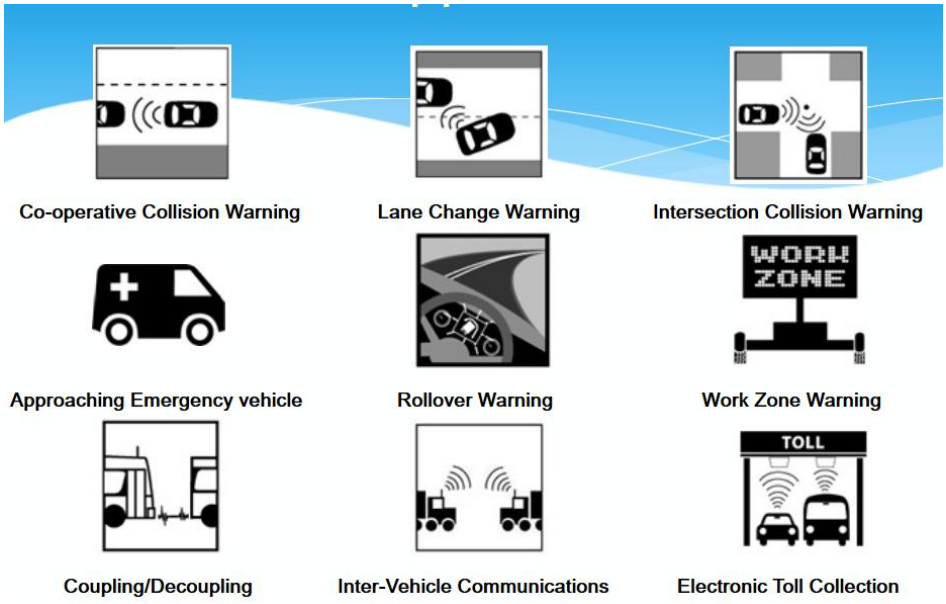

Figure 4: Some applications of VANET [14]

- Electronic brake lights, which allow a driver to react to vehicles breaking.
- Platooning, which allows vehicles to closely (down to a few inches) follow a leading vehicle by wirelessly.
- Traffic information systems, which use VANET communication to provide up-to-the minute obstacle reports to a vehicle's satellite navigation system.
- Road emergency services, where VANET networks, road safety warning, and status information dissemination are used to reduce delays and speed up emergency rescue operations to save the lives of those injured.
- On-the-road services in which VANETs can help advertise services (shops, gas stations, restaurants, etc.) to the driver.
- Accident warning, in which approaching vehicles are warned quickly so that drivers can react carefully and keep the situation under control.
- Traffic congestion detection, which is designed to alert drivers to potential traffic jams, providing increased efficiency.

- Deceleration warning system, in which each vehicle reduces its speed significantly and broadcast a warning on order to avoid traffic accidents.
- Cooperative collision avoidance: This application is to prevent collisions. The safety applications will be triggered automatically when there is a possibility of collisions between vehicles.

Some of the applications are illustrated in Figure 4 [14]. All these applications rely on a trustworthy, secure, and reliable network infrastructure for providing correct traffic and road system data. The applications were designed and developed by the joint effort of different governments and major car manufacturers such General Motors. A significant number of the promising applications for VANETs are becoming a reality.

Future VANETS

Traditional VANETs face several challenges in deployment and management due to less flexibility, scalability, poor connectivity, and inadequate intelligence. Cloud computing, fog computing, co-operative networking, software defined networking, social network, and cognitive radio network are emerging technologies to produce future or next generation VANET.

- *Vehicular Social Networks* (VSN): This is an emerging concept that uses two kinds of networks: Vehicular Network and Mobile Social Network (MSN). It may also be considered as the integration of social networks and the Internet of Vehicles (IoVs) to improve the quality of life for citizens. It is a particular class of VANET, characterized by social aspects and features. It consists of a set of vehicles equipped with OBU and RSU deployed on roads infrastructure. The social networking features include friend finders, job recommendations, content sharing, gaming, etc [15].
- *Software-defined VANETs:* This is a prospective technology. Software-defined networking (SDN) has been proposed in order to support flexibility, agility, and ubiquitous accessibility among vehicles. Software-defined VANET is the integration of SDN on VANET. It improves programmability and flexibility of VANET through software-defined network (SDN) features. SDN technology decouples the control and data planes. The control plane is responsible for making logical decisions of protocols, while the data plane is in charge of accepting the commands. The reason for this separation of control and data planes is to simplify the functions and increase programming, virtualization, and availability. SDN puts the intelligence of the vehicular networks in a central controlling software called SDN controller. In SDN, communication between the control layer and network layer takes place through the SDN control protocol. SDN is an important technology for the next generation network since it provides V2X services in future intelligent transportation systems. With the emergence of SDNs, the flexibility and the programmability of the network have impacted the design of new vehicular network [16]. SDN is applied in vehicular networks to improve management, increase flexibility, apply V2V and V2I connections, select path and channel, and use network resources optimally. A typical software-define VANET is shown in Figure 5 [17].

In addition to these, cloud computing and blockchain technologies will have impact on future VANET. Cloud computing services have the potential to improve services and performance of vehicular services through its flexible and valuable services. Blockchain (BC) is a concept used in order to introduce security services using distributed approach. It can also be used as a mechanism of synchronization between the nodes changing the system state. BC is a distributed ledger to record transactions, where untrusted individuals can interact with each other in a verifiable manner.

Benefits and Challenges

Vehicular networks improve the safety, security, and the efficiency of the transportation system. They have the characteristics like low delay and high reliability. They aim at reducing the accidents and increasing the flow of information among vehicle and the road users. They are expected to be cost-effective and adaptable, making them ideal to provide network connection service to drivers and passengers on the roads. They are suitable networks that can be used in smart cities, smart transportation system, and intelligent transportation systems.

Besides the benefits it offers, VANETs are highly vulnerable to attacks. Due to this reason much attention is given to the security and privacy issues in VANETs. Security issues in VANETs are also important because of its diverse implications in safety related applications. Vehicular networks need security architecture that will protect them from different types of security attacks. Most of the concerns of interest to MANETs are of interest in VANETs, but with differing details. A major challenge with high mobility rates in vehicular environments is the short duration of connectivity available. Due to the high speed of vehicles and the short connecting time among them, it is challenging to establish trust among vehicles. These technical challenges must be addressed before vehicular networks become a reality.

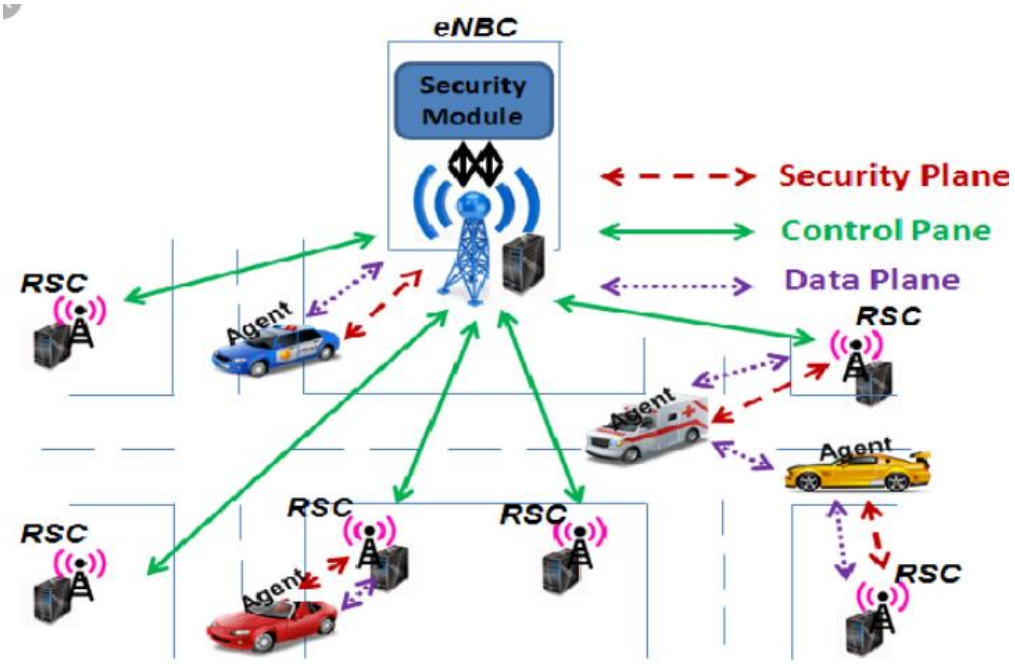

Figure 5: A typical software-define VANET [17]

Conclusion

Vehicular ad hoc networks (VANETs) have gained momentum worldwide as a promising technology for revolutionizing the transportation systems and providing broadband communication services to vehicles. These emerging networks promise to make our driving experience more efficient, safer, comfortable, and enjoyable. They also provide intelligent transportation systems as well as drivers and passengers' assistant services. VANETs are migrating from theory to practice. There is an on going effort to define the standards for vehicular communication including frequency allocation, standards for physical and link layers, routing algorithms, as well as security issues. More information about VANET can be found in the books in [18-23] and related journals: *Vehicular Communications*, *Vehicular Communications and Networks*, and *Ad Hoc Networks.*

References

[1]. K. Ullah et al., "A beaconing-based roadside services discovery protocol for vehicular ad hoc networks," Turkish Journal of Electrical Engineering & Computer Sciences, vol. 27, 2019, pp. 2036 – 2051.

[2]. G. Kumar et al., "Multidimensional security provision for secure communication in vehicular ad hoc networks using hierarchical structure and end-to-end authentication," IEEE Access, vol. 6, August 2018, pp. 46558 – 46567.

[3]. N. Panjrath and M. Poriye, "A comprehensive survey of VANET architectures and design," International Journal of Advanced Research in Computer Science, vol. 8, no. 5, May-June 2017, pp. 2099-2103.

[4]. A. J. Kadhim and S. A. H. Sen, "Energy-efficient multicast routing protocol based on SDN and fog computing for vehicular networks," Ad Hoc Networks, vol. 84, March 2019, pp. 68-81.
[5]. K. Zhu et al, "Mobility and handoff management in vehicular networks: A survey," Wireless Communications and Mobile Computing, vol. 11, 2011, pp. 459–476.
[6]. Z. Y. Rawashdeh and S. M. Mahmud, "Communications in vehicular networks," http://cdn.intechweb.org/pdfs/12877.pdf
[7]. A. Sari, O. Onursal, and M. Akkaya, "Review of the security issues in vehicular ad hoc networks (VANET)," International Journal of Communications, Network and System Sciences, vol. 8, 2015, pp. 552-566.
[8]. J. A. Alves and E. C. G. Will, "Routing in vehicular ad hoc networks: Main characteristics and tendencies," Journal of Computer Networks and Communications, 2018.
[9]. J. M. de Fuentes et al., "Security models in vehicular ad-hoc networks: A survey," IETE Technical Review, vol. 31, no.1, 2014, pp, 47-64.
[10]. E. Schoch et al., "Dependable and secure Geocast in vehicular networks," Proceedings of the seventh ACM international workshop on Vehicular InterNETworking, Chicago, September 2010, pp. 61-68.
[11]. M. Li, " Security in VANETs," https://www.cse.wustl.edu/~jain/cse571-14/ftp/vanet_security/index.html
[12]. M. Raya and J. P. Hubaux, "The security of VANETs," Proceedings of the 2nd ACM international workshop on Vehicular ad hoc networks, Cologne, Germany, September 2005, pp. 93-94.
[13]. "Vehicular ad-hoc network," Wikipedia, the free encyclopedia https://en.wikipedia.org/wiki/Vehicular_ad-hoc_network
[14]. S. Nahum, "Network model of VANET modeling," https://slideplayer.com/slide/10389788/
[15]. A. M. Vegni and V. Loscrí, "A survey on vehicular social networks," IEEE Communication Surveys & Tutorials, vol. 17, no. 4, Fourth Quarter 2015, pp. 2397-2419.
[16]. L. Nkenyereye, "Software-defined network-based vehicular networks: A position paper on their modeling and implementation," Sensors, 2019.
[17]. A. Hussein et al., "SDN VANETs in 5G: An architecture for resilient security services," Proceedings of the Fourth International Conference on Software Defined Systems, May 2017.
[18]. P. Santi, Mobility Models for Next Generation Wireless Networks; Ad Hoc, Vehicular and Mesh Networks. John Wiley & Sons, 2012.
[19]. R. Daher and A. Vinel (eds.), Networks for Vehicular Communications; Architectures, Applications, and Test Fields. Information Science Reference, 2013.
[20]. R. A. Santos et al. (eds.), Wireless Technologies in Vehicular Ad Hoc Networks: Present and Future Challenges. Information Science Reference, 2012.
[21]. W. Chen (ed.), Vehicular Communications and Networks: Architectures, Protocols, Operation and Deployment. Woodhead Publishing, 2015.
[22]. K. Zheng et al., Heterogeneous Vehicular Networks. Springer, 2016.
[23]. S. Olarius and M. C. Weigle (eds.), Vehicular Networks from Theory to Practice. Boca Raton, FL: CRC Press, 2009.

Authors

Matthew N.O. Sadiku is a professor in the Department of Electrical and Computer Engineering at Prairie View A&M University, Prairie View, Texas. He is the author of several books and papers. His areas of research interest include computational electromagnetics and computer networks. He is a fellow of IEEE.

Sudarshan R. Nelatury is an associate professor at Penn State University, The Behrend College, Erie, Pennsylvania. His teaching and research interests lie in electromagnetics and signal processing.

Sarhan M. Musa is a professor in the Department of Electrical and Computer Engineering at Prairie View A&M University, Texas. He has been the director of Prairie View Networking Academy, Texas, since 2004. He is an LTD Sprint and Boeing Welliver Fellow. His research interests include computer networks and computational electromagnetics.