A Comprehensive Review on SDN and VANETS Technology, Architecture and Security Implications

Zakia Feroze[1], Shan Khan[2]

[1] School of Computer Science, National College of Business Administration & Economics Lahore, Pakistan

[2]University of South Asia, Lahore

*Corresponding Author: Zakia Feroze. Email: Zakiamalikawan@gmail.com

Abstract: Software-Defined Networking (SDN) stands as a pivotal method facilitating reliable interaction and operation of software in wireless environments. It is a centralized network system designed to intelligently control network management, enabling efficient bandwidth allocation, robust restoration mechanisms, and heightened security protocols. Within the realm of Mobile Communication, Vehicle Adhoc Network (VANET) services, including 4G/LTE, focus on enhancing road safety, traffic management, and optimizing traffic flow efficacy. This review amalgamates insights into the architecture, historical evolution, requisites, and the amalgamation of SDN and VANET technologies. It examines the tools within SDN technology, addresses challenges encountered within the SDN/VANET landscape, and underscores their collaborative efforts in ensuring the robustness, integrity, and authentication of broadband communication channels.

Keywords: *Wireless Choice, SDN, Centralized Network System, Vehicle Ad hoc Network (VANET), Mobile Communication 4G/LTE, Traffic Services, Security, Architecture, Paradigm, Authentication of Broadband Communication*

1 Introduction

In current Era, Computer Systems provides facility to manage multiple network devices via routers, switches and other type of devices that are used to transfer the communication signals safely that cannot be discard to its actual format. The Network handling concerned is liable to configure different policies to manage extensive series of networks with regard to their use of applications. For that purpose they had to work hard to build lot of policies that handle the software application and network data transformation demand. If they change the any network they shuffle to change the policies which were really difficult choice to manage while distinguishing the networks.

Many Software Personals creates different policies to handle security and communications ways to interlink different networks. In past different protocols have been used for data communication that cause hard labor to accomplish different common controlling tasks. [2] In that environment there have already been great needs to attach different devices to communicate in different ways.

For Data Communication there is need to use such schemas and possibilities that control the different task together without connecting more devices to accomplish all management and security tasks. SDN is technology which, control the different tasks together to avoid enormous labour of programming. [1] And enable the network to control network resources in very easy way with respect to invest high cost investment for network devices. To reset or combine all limitation there come an idea there should be one thing which set aside all limitation and make a benefits for all above given solution. [3]

Software Defined Networking (SDN) is a novel interacting Technology for the communication between different networks which able to hardware to work independently leading towards accurate decisions. In otherworld’s it assures proper network management and authorizes networks towards unique and updated Development. The core notion is of SDN Technology is to enable the Software Engineers to manage network storage and interlinked peripherals.

The idea of implementing of software defined networking is new even it is mounting speedily and many researchers are working on its challenges day by day. Software Defined Networking SDN is immense technology, which moves networks officials, as Open Flow specially has been new innovation in networking. Which go through centralized control by using simple protocols and modulate the hardware, the same reduce the use of middle boxes. [4].

In the Section-II, We will discuss about Vehicular Ad Hoc Networks (VANET) Technology, History, Traffic Congestion, Component of VANET, Deployment Areas, VANNET Simulation Component, Confidentiality & Authentication of VANET, Routing Approaches/Categories of VANET, Classification of Wireless Network, Rules to be deploy on VANET/Broadcasting, VANET Basic Architecture, Protocols and their implementation consideration, Mode of Attacks in VANET, VANET Cloud perspective Application, Raw Data Fetch Method.

SDN Technology Working vs. Pre-SDN Data Control Mechanism:-

In past Data streaming is controlled via different communication devices i.e., routers and switches. The author incorporated in [5], [6] recent network paradigm is immobile if parallel to discover SDN. Operators do not have any mechanism to work over data packets. Normally this task is done through different switches and routers whereas in SDN, Operators can manage his own data traffic due to de-centralize system of SDN (Software Defined Networking). Through this paper [5], [6], the author furnished the assessment of outmoded networks and SDN (Software Defined Networking). Additionally they also incorporated that the SDN (Software Defined Networking) is core approach where the operators can manage the data packets flow with their own choice as the Software Defined Networking deliver a very easy interface for the security purpose protocols and quires solution in very easy manners.

SDN unable to users, not invest on cost effective devices i.e., switches/router. [7], [8].

Moreover in past the network is being working with data plane which is responsible to hold data from the data packets via one node to parallel other node by working with huge labour of defining different protocols, control plane where the data packet logically forward to management plane. [9]

SDN is a latest networking novel idea which covers centralized, programmable control planes and data plane [10] perception, as in SDN Architecture data planes and control planes are decoupled so that network operators can manage the resources with their own choice, as show in Fig 1. Software Defined Networking emphasis on features i.e., separation of the control plane from the data plane, centralized controller and open interfaces to communicate via control plane and data plane

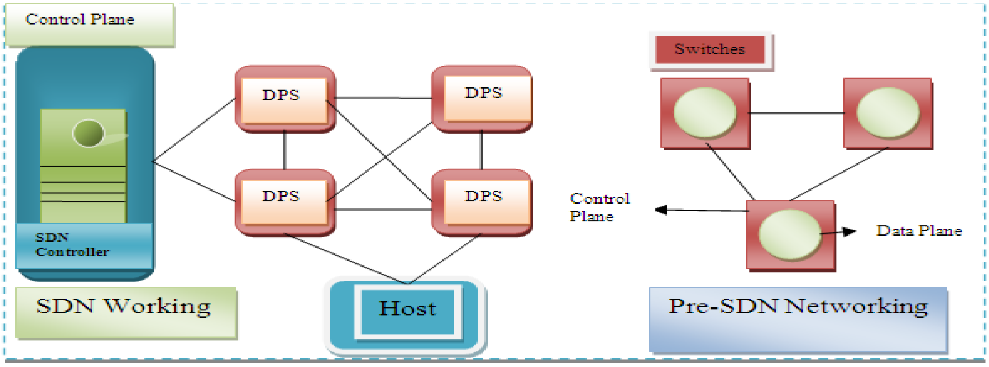

Figure: 1 Basic Architecture of Pre SDN Networking and SDN Model Management

Simultaneously the external applications are [11] utilized through SDN Technology. Globally it is surveyed that the usage of SDN Technology is increasingly worldwide since 2013. It is evaluate that the use of Software Defined Networking will fulfil the task of management of networks with less labour of programming till 2021. [11].

SDN Model Emphasis on basic concepts:-

SDN vanished the idea of control plane and data plane together. SDN is a model of latest thinking which is able to reduce the complexity of network management and programmability to transform data in very secure and efficient way. [12,13]. Currently SDN set up a large number of wireless environments, application with respect to virtualization, load balancing and handle heterogeneous network through refined routing strategies. [14, 15]. Different concepts which SDN took for the development of core model making. There are different concepts i.e., network virtualization (NV), Evolutionary Approach (EA), Open Flow and Network Function Virtualization [16], [17].

Network Virtualization (NV):-

The main purpose of Network Virtualization is to refrain the restrictions on Local Area Network Protocols/standards to ensure the capability to [16] manage networks. The big advantage of Network Virtualization is multitenant clouds certainly.

Evolutionary Approach (EA):

SDN adopt the Evolutionary Approach for the concept, to opt this mechanism in SDN Architecture to control and enhance the working of software functions in network types i.e., it be in LAN/WAN/MAN. So the Evolutionary Approach capable [16] SDN to work on any network with the combination of wide range of network.

OpenFlow (OF):-

Basically, SDN and OpenFlow terms are the same work, but SDN is the enhanced version of the Model. There is delusion that the [18] OpenFlow and SDN are the same terms, and OpenFlow comes first to SDN. An OpenFlow term is usually followed by SDN because it handles the working of NAT Firewall and manages the different procedure and working that rely on packet handling algorithm. Due to having the concept of these switching/router/firewall NAT-like benefits, SDN emphasises the OpenFlow Model. [19]

Network Function Virtualization (NFV):-

Network Function Virtualization [20] denotes the virtualization of network task explicitly for example Firewall, Wide Area Network Consumers work, data Traffic Load Management and providing a reasonable path for data traffic, Network Function Virtualization technique handles a number of services/task which are running parallel in combination of different network. Virtualization could be work on various software of connection together different network at the same time. Due to having this ability of virtualization, SDN manage the data plane. Moreover SDN is relied on virtualization to enhance the data plane capacity through virtual accessories.

Extensions used for Software Defined Networking with aspect to Network Management and Network Security:-

SDN conceptually centralized controller-is used different Extension Models for which SDN Model build network base information collection Schema and self-making networking policy amending in very short way. So that SDN methods can be utilized to obtain different benefits in network management and Security Areas by utilizing the Extension working with SDN Architecture. Table 1: Showing the enrollment of different concepts that leads to SDN toward accurate Network Management and Security credibly.

Extensions used in SDN Architecture for Network Management & Extensions used in SDN Architecture for Network Management & Security.		
Network Management	Extensions	Usage of Different Extension in SDN Architecture
	Aster*x	In SDN Architecture the OpenFlow with the work of Aster*x determine the network status by and then network and forward the path exactly.[21].The author of the paper [22] consume used this term to minimize the risk of packet loss.
	FleXam	OpenFlow controller [23] while working with FleXam is able to patch the data packet collection. The author state in [24, 25] that while developing any application it is necessary to know about the architecture of SDN to aim developing network SDN based technologies. Due to having benefit of getting precise traffic [33] measurement FleXam is good approach for SDN Architecture.
	Open Sketch	SDN Architecture used this OpenSketch [26] extension to measure the data traffic and then adopt a way to manage data packet that is accurate by way of data plane and control Plane.
	NOX OpenFlow	Usually OpenFlow Controller is the second form of [27] NOX. NOX and OpenFlow are working together by utilizing the services of management for routing in any developing [28] networks
	Plun-n-Serve	Plug-n-Serve is a key for web base Application traffic [29] controller. The aim of Plug-n-Serve in SDN Open Flow Controller is to change the switch devices' formation and arrangement [30], [31] to keep the data traffic steady and safe consecutively.
	SIMPLE	SIMPLE [32] is an SDN-based policy implementation tier for proficient middlebox-unique traffic management. SIMPLE uses SDN technologies to certify that the traffic is engage in uniform way by utilizing different application
	FlowTags	FlowTags [34] allows all network concerned devices to link sending data packets that have been used in switches and policy making devices. SDN enables to insert numerous network services, such as business achievements [35], where a software control in the middle of the network injects related advertisements based on the session content. The general framework for developing in-network services or middlebox functionalities is discussed in [36, 37].
Network Security	OFRHM (OpenFlow Random Host Mutation)	Being SDN is a Central Control of network, is also the helpful to secure the implementation of Application. OpenFlow Random Host Mutation (OFRHM) [38] is a method which conceals the network concerned all resources from the internal or external intruders. For that approach SDN is beneficial approach for network security. In this method, basically OpenFlow controller dynamically assigns random virtual IP that every intruder could not fetch the real IP.
	Resonance	Resonance [39] makes secure the network initially which connected to the policies making switches as the Resonance is common to provide the security of network. SDN is able to manage security by the use of

		Resonance on network and applications that are used in the network [40], [41]
	Virtual Machine (VM)	Earlier the Virtual Machine (VM) is very tough to handle its work as its need updates with the passage of time. So SDN with the coordination of Virtual Machine and SLA work has been wondered to organize the variation of network on its security context. [42].
	LIME	In author [43] emulates the LIME ability to data plane in to a novel idea of development of switches (concerned to security purposes) by the connecting of SDN and VMs technologies.
	ElasticTree	SDN working in background the Model ElasticTree which is responsible to look the data plane traffic of the network and according to enhance the efficiency of network power sources [44]
	Scissor	The Work of Scissor [45] in SDN Technologies to discard the unnecessary data traffic and permit to switches sends data on just flow known host.
	NCP	Basically NCP (Network Control Protocol) [46] is the provision to SDN a reliable duplication Flow in data centers. In other words NCP scalable service replication in data centers through SDN. NCP recognize current network path and destination path for which the rules is to be opted through server.
	B4	B4 [47] manipulates OpenFlow to link Google's data centers to fulfil vast bandwidth necessities and liable to manage bandwidth limitation on the data plane network.
	SWN (Software Driven WAN)	The purpose of SWAN [48], improving the consumption of inter-data center networks. SWAN empowered data traffic services and re-generating toward data plane as per data traffic demand.

VANET Primer:-

VANET is well suited discipline for Researcher, as its standard and development is great latent for the performance of working of vehicle traffic as concerned to drivers and passengers. Vehicular Ad Hoc Networks (VANETs) have raised the necessities towards a huge number of wireless items that could be formed in transportation [49, 50].

VANETs is wide ranging term that is exploited in safety and non-safety applications, which permit value added services for example Transportation items well-being driving, mechanized toll payment, traffic management, enriched routings [51], informatics and entertainment applications via offering internet facility.

In the vehicular System, the vehicle takes place core roll as sender, receiver. The router is responsible to [52] transmit the data of regarding vehicular toward vehicular network system Organization, which is considered and pretty like to be non-violent, congestion free traffic. As concerned to vehicular communication, the communication between vehicles is laying in three aspect; i) Inter-vehicle Communication ii) Vehicle to roadside communication iii) Routing-based communication. The Inter-vehicle Communication is liable to use multi-hop multicast/broadcast to transfer vehicular information on the behalf of multiple hops. In this type of communication the messages are classified in two terms further; i) native broadcasting ii) intelligent broadcasting [53].

It is observed by the author [54] that it is the native broadcasting method is inadequate regarding to handle large number of transmission of messages. And it is failure to observe secure message traffic due to having the attempt of crashes in message forwarding. It is reviewed [53], the intelligent broadcasting with absolute/confirmed message is doubtful to spreading the message in emergency situation.

The communication in Vehicle-to-roadside is totally based on single hope broadcasting, in which the vehicular while sending a message depends on their situated tools/products located in that particular area [54].

In the communication of Routing based the concept is introduce a multi-hop unicast technique. In this communication the vehicle fetch the message information regarding their destination area. The vehicular when receiving the message the vehicular send a unicast message that it can be received the confirmation message toward the point of that vehicular from the message is sent [53].

Contextual History of VANET Technology:-

In 1990s vehicle-to-vehicle and vehicle to roadside units were communicated through the radio and infrared waves, which was the basic concept to go toward development for such system which able to communicate intelligently. The author [55] introduced the initial vision of roadway items automation and such communication method which makes the vehicular traffic safe [56] proper organized. According to the Institute of Electrical and Electronics Engineers (IEEE), it is come to knowledge that wireless networks has two areas, where the wireless communication are established: one is called Infrastructure based network (IBN) and other is Infrastructure less network (ILN). The Infrastructure less network (ILN) further divided into three category i.e., wireless sensor network (WSN), wireless mesh network (WMN), Mobile Adhoc network (MANET). The Mobile Ad-hoc network (MANET) further categorized communication in two ways, one is VANET and other is UAVAN.

The wireless choice becoming a popular in every field of life communication which delivers wire free environment to their clients that they are able to move everywhere spontaneously [57]. In VANET the wireless is focusing on nodes (vehicles) which are vigorously planning for Network topologies.

For wireless system, A Terms MANET (Mobile ad-hoc network) is focusing in communication. In MANET every node works freely and can go in any way. MANNET is considered a network which is supporting to mobility infrastructure. As this technology is dynamically working, the devices that are connecting with its aspect can be diverse its link from one to other device and its outcomes found energetic and self-directed. Every appliance and tools support as router. It is pertinent to deliver the information that in wire environment, routers plays its own task, whereas in wireless network, an explicit node can be work as its access point [58].

In the field of MANET, the researchers and scientists determining the new ideas for moving the communication with less beavering items connection. VANET is newly innovation and subset of MANET for the communication. In other words the VANET (Vehicular Ad Hoc Network) is supporting a logic “computer on wheel” [59] and its purpose to communicate the driver of the vehicles, where the nodes transferring the information to the others linked nodes. In this topology the devices are sending all information to the other nodes and managing its information flow certainly.

The devices which linked to the VANET (Vehicular Ad Hoc Network) topology are proficient hardware, that transforms the data consecutively without delaying the information to reach its destination node, and these nodes might be linked through internet.

VANET is the provision of decision making. The communication is empowered between vehicles through wireless devices. Through VANET security of drivers and near road nodes are ensure. MANET (Mobile ad-hoc network) and VANET (Vehicular Ad Hoc Network) are the same in its features as they both are self-configuration of nodes. Comparatively the working of both is diverse with each other with respect to node movement, driver conduct, unnecessary hurdles on mobility and capricious network situation [60].

Features of VANET:-

VANET has rapid growing technology with regard to vehicular safety application [61]. The author elaborated the basic features of VANET i.e., effectiveness in destruction, scalability and density of network, effect of vehicular controlling by driver conduct, minimum mistake occurrence, less traffic congestion, extension of network [62]. The author of [60] also explained the feature of VANET regarding its high mobility, high speed and less time for communication establishment, node allocation and vehicle organized system with utilization of power supplies. The author also characterized the VANET for its Global Positioning System, Mobile Modeling Architecture & Prediction. On the other hand, the benefits of VANET are node distribution pattern, GPS for the nodes, network scalability volume (capability). According to [63] the nodes allocation scheme is not a defaulted for the partition of road units as concerned to speed of vehicle.

VANET Components/Taxonomy:-

Components are the basic element of the VANET, the source [64] expounded about the three prime components of VANET i.e.; onboard unit (OBU), roadside unit (RSU) and backhaul network. Further it is illustrated that regarding vehicular communication VANET Taxonomy is divided in two ways one is Road Vehicle Communication (RVC) and second is inter-vehicle communication (IVC). There are different layers to work on vehicular communication network i.e., Physical Layer (PHY), Media Access Control ((MAC) Layer. In the study [65], it is observed that wherever the VANET is applied, there must be some of simulation of Model deployment. The author explained the component of simulation of any VANET Model:-

i. A Traffic Simulator
ii. A Network Simulator.

The Traffic Simulators will produce the place and movement data of any vehicle in VANET network/environment. Whereas the, Network Simulator provides the exact and active path for the routing of vehicle. The author further argued that such environment where the simulation of VANET is deployed, are school area and hospital areas.

Rules for the broadcasting in VANET:-

Everything in the word is relaying on some rules or techniques by which, any system can run. In the communication of wireless network VANET, there are some rules and regimes which are followed for broadcasting in VANET [66]. VANET is focusing in three concentrations:-

A. Dense Traffic (In that rule, while traffic is much more loaded instead following the certain cost of vehicular, there exist a great problem so broadcasting is measured accordingly).

B. Sparse Traffic (In that scenario at particular time which is defined by the network the traffic may cause for collusion with aspect to slow traffic and nodes cannot transmit information accordingly).

C. Regular Traffic (It is look like locally connectivity of vehicle communication and every vehicle give reflect as global connectivity).

Attacks on VANET:-

Owing to fetching large number of unknown network members and availability of human or such misconduct of nodes vehicular Network faces different types of Attacks. An Attacker can attack by involving their wrong intention and put wrong messages to the network [67]. An Attacker can attack on basic component of VANET i.e., OBU, RSU or on network layer. The author enlightened the Attack classification such as Spreading Unknown/un-relevant information, duplicitous with sensing nodes, ID hiding, Denial of Services, replying and sending unnecessary messages, hide the vehicle positioning, Record a vehicle location, send it to wrong place and such Sybil Attach, Jamming Attack [69], Platooning Attach [70] and Betrayal Attach. The security is the main subject in any field of deployment. As concerned to VANET the security become a topic for debate. There are some elements by which fulfill the security is confirmed. As concerned to the confidentiality and Authentication of VANET there are some contents. Confidentiality is likely to be said the privacy. In other words the requisite data is to be received by the elected host and it is ensure that the data is not fetching by unknown users. To considering the confidentiality the author [68] described some sort of attacks that are cause harmful for the confidentiality of VANET i.e., Unknown vehicle entry Attach, Social Abuse Attack, Wrong Traffic direction Attach, Fetching confidentiality data Attach, Wrong Sensor information Attach. Regarding the Attach on Vehicular Network some effort has been done [71].

Raw/False Data Fetch Method:-

Different Applications are uses for the Vehicular Network. Some wrong/false information, misbehave to the trusty host. In the study of [72] there are two kind of misbehave one is intentionally misbehave and other is unintentionally misbehave. The author further explained, the intentionally misbehave is link to the qualities like selfishness and malicious intention whereas unintentional misbehave is cause to signal loss or some like of technical fault in sensors of nodes. In [73], The False data detection Method is purposed by two way:-

1. Node Centric Detection Method
2. Data Centric Detection Method

Node Centric Detection Method:-

It is a security relevant Model, which monitor the node, signature through the support of PKI [74]. It is the mechanism in which the behavior of node is verify via packet and message pattern. In node Centric Detection method the behavior of the node is recognized that the node sent a message by normal strength of the message. Trust base detection of message make ensured by analyzing the past and present reputation of the node behavior. Reputation is the base of [75] analyzing the message by maintaining the record of last and current message packets.

Data Centric Detection Method:-

Application Data is bound to use neighbor data. It is collected from different neighbor nodes. The data, which is gathered from other neighbor host, to be verified to avoiding the collusion [76].

VANET Application Category/Routing:-

Owing to have high mobility nodes and authenticity of vehicular Network, Application are divided into two Groups. One is Intelligent Transportation Application and other is Comfort Application. The major application of the VANET is Intelligent Transportation Application, which is the main component of Intelligent Transportation System (ITS). On the other hand, the comfort application is linked to the passenger nodes. Its purpose to permit the passengers to communicate with other node of the network (vehicle/host/passengers) [77].

According to the author through the comfort application passengers are able to download any type of entertainment programs such as music, movie, send e-mail or play any internet game. Therefore, it is to say that application are the dynamically facilitating the nodes/passengers.

As the VANET is dynamically mobile/Vehicular nodes network, choosing a trustworthy/authenticated path is very inspiring research area for the researchers. Routing in VANET is done by different type of Protocols which able to nodes find and track the secure and authentic path for the passengers/ Vehicles/ Nodes.

Different Protocols have been purpose in different studies. To keep the quality of service [78] the author has purposed four protocols for quality of routing services, namely Point-based broadcast routing protocol, cluster-based routing protocol, [79] position-based routing protocol and all-pervasive routing protocol in VANET. Other one protocol namely Dynamic Soiree routing (DSR) [80] is which is also used in VANET for routing purpose.

Traffic Congestion and SDN/VANAT immersion:-

Such traffic congestion is going in verse condition due to enhancing the use of vehicles. And traffic congestion is standing toward problems like unfeasible path, facing accidents, even though the Intelligent Transportation System is delivering the maximum facilities with the use of different application. To avoid the maximum traffic congestion, the author [81] has purpose a Model of VANET with the consolidation of work Software Defined Network (SDN). In that Model to overcome the problems that were facing in VANET environment for example prolong end to end delay, Longer message path delivery and emergency condition reply not receiving), SDN Architecture is gather with VANET. The core object of the SDN-VANET Architecture for Traffic Congestion is to logically centralize the control plane from the data plane [82], [83], [84]. According to the author SDN Controller work with the Open Flow protocol for doing the job of messaging [81] forwarding. The Open Flow then linked the network in data plane and application layer. SDN permitted to wireless nodes of mobile network and RSU which having stationary nodes, will obtain the messages from the control plan. Each logically SDN wireless host will have a logical host, come to know as SDN-Agent. Via agent the controller work simultaneously.

REFERENCES

1. Othmran S. Al-Heety Zahriladha Zakaria, Mahamod Ismail, Mohammed Mudhafar Shakir, Sameer Alani, Hussein Alsariera. -A Comprehensive Survey: Benefits, Services, Recent Works, Challenges, Security, and Use Cases for SDN-Vanet [Journal] / auth.Malaysia : IEEE Access, 2020. April 16,.

2. Bruno Astuto A. Nunes Marc Mendonca, Xuan-Nam Nguyen, Katia Obraczka, and Thierry Turletti.A Survey of Software Defined Netoworking: Past Present, and Future of Programmable Netoworks [Journal] /France : IEEE, 2014. - October 28, 2013.

3. Hamid Farhady HyunYong Lee, Akihiro Nakao Software-Defined Networking: A Survey [Article] /Computer Networks. - Tokyo, Japan : ScienceDirect, 2015. - 26 February.

4. Thomas A. Limon celli. Open flow: a radical new idea in networking. Common. ACM, 55(8):42–47, August 2012

5. Open Flow switch specification Version 1.3. Open Networking Foundation. Avaible at:Http://www.opennetworking.org/. 2012.

6. Open Networking Foundation. “OpenFlow /Software Defined-networking (SDN)”. http://www. www.opennetworking.org/.

7. http://www.zdnet.com/10-key-questions-about-software-Definedd networking-sdn-7000015822/[5]http://globalconfig.net/software-Definedd-networking-vs-traditional/

8. http://readwrite.com/2013/04/23/software-Definedd-networking-dn#awesm=~omPg0fn3rysfHX

9. IBM. "IBM Systems and Technology Thought Leadership White Paper". 2012

10. Spindox Digital Soul, “Software Defined Networks: The road to DevOps goes through virtualization, Sept 2017 available at https://www.spindox.it/en/blog/software-defined-networks. [Accessed: 18 May 2018].

11. Statista, Global SDN market size, the Statistic portal, https://www.statista.com/statistics/468636/global-sdn-marketsize/ [Accessed: 20 June 2018].

12. A. Drescher, “A survey of software-defined wireless networks,” Dept. Comput. Sci. Eng., Washington Univ. St. Louis, St. Louis, MO, USA, Tech. Rep, pp. 1–15, 2014.

13. Orrego, Juan Fernando Gonzalez, and Juan Pablo Urrea Duque. "Throughput and delay evaluation framework integrating SDN and IEEE 802.11s WMN." Communications (LATINCOM), 2017 IEEE 9th Latin-American Conference on. IEEE, 2017.

14. C. Chaudet and Y. Haddad, “Wireless Software Defined Networks: Challenges and opportunities,” in 2013 IEEE International Conference on Microwaves, Communications, Antennas, and Electronic Systems (COMCAS 2013). IEEE, 10 2013, pp. 1–5.

15. Maleki, Atefeh, et al. "An SDN Perspective to Mitigate the Energy Consumption of Core Networks–GÉANT2." International SEEDS conference in 2017.

16. https://searchnetworking.techtarget.com/ tip/Three-models-of-SDN-explained

17. European Telecommunications Standards Institute, Network Functions Virtualization, 2012.

18. K. Greene, TR10: Software-Defined Networking – MIT Technology Review, 2009

19. B. Ahlgren, C. Dannewitz, C. Imbrenda, D. Kutscher, B. Ohlman, A survey of information-centric networking, IEEE Commun. Mag. 50 (7) (2012) 26–36.

20. European Telecommunications Standards Institute, Network Functions Virtualization, 2012. <http://portal.etsi.org/NFV/NFVWhite_Paper.pdf.

21. N. Handigol, S. Seetharaman, M. Flajslik, R. Johari, N. McKeown, and Aster⁄x: Load-balancing as a network primitive, in: Proceedings of ACLD, 2010

22. S. Agarwal, M. Kodialam, T. Lakshman, Traffic engineering in software defined networks, in: IEEE INFOCOM, 2013, pp. 2211–2219.

23. S. Shirali-Shahreza, Y. Ganjali, FleXam: flexible sampling extension for monitoring and security applications in OpenFlow, in: ACM SIGCOMM HotSDN, 2013, pp. 167–168

24. Takagiwa, S. Ishida, H. Nishi, SoR-Based Programmable Network for Future Software-Defined Network, in: IEEE COMPSAC, 2013, pp.165–166.

25. Z.A. Qazi, J. Lee, T. Jin, G. Bellala, M. Arndt, G. Noubir, Application awareness in SDN, in: Proceedings of the ACM SIGCOMM, 2013, pp.487–488.

26. M. Yu, L. Jose, R. Miao, Software defined traffic measurement with opensketch, in: USENIX NSDI, vol. 13, 2013\

27. https:// www. google. com/ search? ei=qbr-X9mFE5KpgAbbhpr4Bw&q=NOX+ OpenFlow+in+SDN+what+is&oq=NOX+OpenFlow+in+SDN

28. R. Bennesby, P. Fonseca, E. Mota, A. Passito, An inter-as routing component for software-defined networks, in: IEEE NOMS, 2012, pp. 138–145.

29. N. Handigol, S. Seetharaman, M. Flajslik, N. McKeown, R. Johari, Plug-n-serve: Load-balancing web traffic using OpenFlow, in: ACM SIGCOMM Demo, 2009.

30. A. Khurshid, W. Zhou, M. Caesar, P. Godfrey, Veriflow: verifying network-wide invariants in real time, ACM SIGCOMM CCR 42 (4) (2012) 467–472.

31. P. Kazemian, G. Varghese, and N. McKeown, Header space analysis: static checking for networks, in: USENIX NSDI, 2012, pp. 9–9

32. Z.A. Qazi, C.-C. Tu, L. Chiang, R. Miao, V. Sekar, M. Yu, SIMPLE-fying Middlebox Policy Enforcement Using SDN, in: ACM SIGCOMM, 2013.

33. Hohn, N., and Veitch, D. 2006. Inverting sampled traffic. IEEE/ACM Trans. Netw. 14(1). 68-80.

34. S. Fayazbakhsh, V. Sekar, M. Yu, J. Mogul, Flowtags: Enforcing network-wide policies in the presence of dynamic middlebox actions, ACM SIGCOMM HotSDN

35. Y. Nishida, A. Nakao, In-network ad-targeting through wifi apvirtualization, in: 2012 International Symposium on Communications and Information Technologies (ISCIT), IEEE, 2012, pp. 1092–1097.

36. J. Lee, J. Tourrilhes, P. Sharma, S. Banerjee, No more middlebox: integrate processing into network, ACM SIGCOMM CCR 41 (4) (2011) 459–460.

37. M. SHIMAMURA, T. IKENAGA, M. TSURU, A design and prototyping of in-network processing platform to enable adaptive network

Services, IEICE Trans. Inf. Syst. E96-D (2) (2013) 238–248.

38. J.H. Jafarian, E. Al-Shaer, Q. Duan, OpenFlow random host mutation:transparent moving target defense using software defined networking, in: ACM SIGCOMM HotSDN, 2012, pp. 127–132.

39. Resonance. <\\http: resonance. Noise. gatech.edu>.

40. M. Suenaga, M. Otani, H. Tanaka, K. Watanabe, Opengate on OpenFlow: system outline, in: 2012 Fourth International Conference on Intelligent Networking and Collaborative Systems, IEEE, 2012, pp. 491–492.

41. S. Shin, P. Porras, V. Yegneswaran, M. Fong, G. Gu, M. Tyson, FRESCO: modular composable security services for software- defined networks, in: Proceedings of Network and Distributed Security Symposium, 2013

42. S. Ghorbani, M. Caesar, Walk the line: consistent network updates with bandwidth guarantees, in: ACM SIGCOMM HotSDN, 2012, pp. 67–72

43. E. Keller, S. Ghorbani, M. Caesar, J. Rexford, Live migration of an entire network (and its hosts), in: ACM SIGCOMM HotNets, 2012, pp. 109–114

44. B. Heller, S. Seetharaman, P. Mahadevan, Y. Yiakoumis, P. Sharma, S. Banerjee, N. McKeown, ElasticTree: Saving Energy in Data Center Networks, in: USENIX NSDI, vol. 3, 2010, pp. 19–21

45. K. Kannan, S. Banerjee, and Scissors: Dealing with header redundancies in data centers through SDN, in: IEEE CNSM, 2012, pp. 295–301.

46. V. Mann, K. Kannan, A. Vishnoi, A.S. Iyer, Ncp: Service replication in data centers through software defined networking, in: IFIP/IEEE IM, 2013, pp. 561–567

47. S. Jain, A. Kumar, S. Mandal, J. Ong, L. Poutievski, A. Singh, S. Venkata, J. Wanderer, J. Zhou, M. Zhu, and B4: Experience with a globally-deployed software defined WAN, in: ACM SIGCOMM, 2013, pp. 3–14.

48. C.-Y. Hong, S. Kandula, R. Mahajan, M. Zhang, V. Gill, M. Nanduri, R. Wattenhofer, Achieving high utilization with software-driven WAN, in: ACM SIGCOMM, 2013, pp. 15–26

49. Raya, M., & Hubaux, J. (2005). The security of vehicular ad hoc networks. In Proceedings of the 3rd ACM workshop on security of ad hoc and sensor networks (SASN 2005) (pp. 1–11), Alexandria, VA.

50. Harsch, C., Festag, A., & Papadimitratos, P. (2007). Secure position-based routing for VANETs. In Proceedings of IEEE 66th vehicular technology conference (VTC-2007), fall 2007 (pp. 26–30), September 2007.

51. Gerlach, M. (2006). Full paper: assessing and improving privacy in VANETs. www.network-on-wheels.de/downloads/ escar2006gerlach.pdf (accessed: May 29, 2010).

52. Jinyuan, S., Chi, Z., & Yuguang, F. (2007). An ID-based framework achieving privacy and non-repudiation. In Proceedings of IEEE vehicular ad hoc networks, military communications conference (MILCOM 2007) (pp. 1–7), October 2007

53. Sherali, R.Hunt. Y.Shyan, Angela, Ahsan. (2012). Vehicular ad hoc networks (VANETS): status, results, and challenges. Springer (pp.218), LLC, 2010

54. Bickel, G. (2008). Inter/intra-vehicle wireless communication. http://userfs.cec.wustl.edu/~gsb1/index.html#toc (accessed: May 29, 2010).

55. Shladover S 1989 Research needs in roadway automation. Vehicle/Highway Automation: Technology and Policy Issues pp. 89–104.

56. Lasky TA and Ravani B 1993 A review of research related to automated highway systems (AHS). Advanced Highway Maintenance and Construction Technology Research Center, UCD-ARR-93-10-25-01, Dept. of Mechanical and Aeronautical Engineering, University of California, Davis, October, 1993.

57. Hammad, R.A. Rehman, B.Seo (2018) Hindawi, Services and Security Threats in SDN Based Vanets: A Survey. Wiley.

58. B. T. Sharef, R. A. Alsaqour, and M. Ismail, “Vehicular communication

ad hoc routing protocols: a survey,” Journal of Network and Computer Applications, vol. 40, no. 1, pp. 363–396, 2014.

59. Raya, M., & Hubaux, J. P. (2007). Securing vehicular ad hoc networks. Journal of Computer Security, 15(1), 39-68.

60. Liu, Y., Bi, J., & Yang, J. (2009). Research on vehicular ad hoc networks. In IEEE Control and Decision Conference, 2009. CCDC'09. Chinese (pp. 4430-4435).

61. Yousefi, S., Altmaiv, E., El-Azouzi, R., & Fathy, M. (2007). Connectivity in vehicular adhoc networks in presence wireless mobile base-stations. In Telecommunications IEEE, 2007. ITST'07. 7th International Conference on ITS (pp. 1-6).

62. Raya, M., & Hubaux, J. P. (2007). Securing vehicular ad hoc networks. Journal of Computer Security, 15(1), 39-68.

63. Ho, I. W. H., Leung, K. K., & Polak, J. W. (2012). A Methodology for studying VANET performance with practical vehicle distribution in urban environment. ArXiv Preprint, 1211.6251.

64. Peng, Y., & Chang, J. M. (2010). A novel mobility management scheme for integration of vehicular ad hoc networks and fixed IP networks. Mobile Networks and

Applications, 15(1), 112-125.

65. Anjana,Y.S, (2018). VANNET based Virtual Dash Board. IJERT, ISSN.22780181 in NCESC Conference Proceedings.

66. Ozan.T, N.Wisitpongphan, F.Bai, P.Mudalige, Varsha.Sadekar (2007) Broadcasting in VANET, IEEE. USA.

67. Raya, M., Hubaux, J.-P.: Securing vehicular ad hoc networks. J. Comput. Secur. 15(1),39–68 (2007)

68. Azees, M., Vijayakumar, P. and Deborah, J. (2016), Comprehensive survey on security services in vehicular ad-hoc networks, in Proc. Of International Journal of lET Intelligent Transport Systems, vol. 10, pp.379-388.

69. R. Minhas and M. Tilal, Effects of Jamming on IEEE 802.11p Systems, Chalmers University of Technology, Gothenburg, Sweden, 2010.

70. C. A. Kerrache, C. T. Calafate, J. Cano, N. Lagraa, and P. Manzoni, “Trust management for vehicular networks: an adversary-oriented overview,” IEEE Access, vol. 4, pp. 9293–9307, 2017.

71. Lu, R., Lin, X., Liang, X. and Sheen, X. (2012), A Dynamic Privacy Preserving Key Management Scheme for Location-Based Services in VANETs, in Proc. of IEEE Transactions on Intelligent Transportation Systems, vol. 13, pp. 127-139.

72. F Ghaleb, A Zainal, M Rassam, Data verification and misbehavior detection in vehicular ad-hoc networks. J. Teknologi. 73(2), 37–44 (2015).

73. M.Arshad, Z.Ullah, N.Ahmad, M.Khalid, H.Criuckshank, Y.Cao, A survey of local/cooperative-based malicious information detection techniques in VANETs. EURASIP.4-5(2018).

74. R van der Heijden, S Dietzel, F Kargl, Misbehavior detection in vehicular ad-hoc networks. (Proceedings of the 1st GI/ITG KuVS Fachgesprach Inter-Vehicle Communication (FG-IVC 2013), (2013).

75. RW van der Heijden, S Dietzel, T Leinmuller, F Kargl, Survey on misbehavior detection in cooperative intelligent transportation systems (2016). arXiv preprint rXiv:1610.06810

76. U Khan, S Agrawal, S Silakari, in Information Systems Design and Intelligent Applications. A detailed survey on misbehavior node detection techniques in vehicular ad hoc networks. (Springer, 2015), pp. 11–19.

77. Y.Wang, F.Li, S.Misra. Vehicular Ad-Hoc Network, Chap.20 (505), Beijing Institute of Technology, Beijing, China (2009).

78. T. B. Reddy, I. Karthigeyan, B. Manoj, and C. S. R. Murthy. (2006). Quality of service provisioning in ad-hoc wireless networks: a survey of issues and solutions. Ad-hoc Networks. vol. 4. pp. 83-124.

79. E. C. Eze, S.-J. Zhang, E.-J. Liu, and J. C. Eze. (2016). Advances in vehicular ad-hoc networks (VANETs): Challenges and road-map for future development. International Journal of Automation and Computing. vol. 13. pp. 1-18.

80. J. M. Jaffe. (1984). Algorithms for finding paths with multiple constraints. Networks. vol. 14. pp. 95-116.

81. T.Adbeb, W.Di, M.Ibrar. Software-Defined Network (SDN) based VANET Architecture: Mitigation of Traffic Congestion. IJACSA. Vol.II (2020), Dalian, China

82. I. Ku, Y. Lu, M. Gerla, R. L. Gomes, F. Ongaro, and E. Cerqueira, “Towards software-defined vanet: Architecture and services,” in 2014 13th annual Mediterranean ad hoc networking workshop (MED-HOCNET). IEEE, 2014, pp.103–110.

83.K. L. K. Sudheera, M. Ma, and P. H. J. Chong, “Link stability based optimized routing framework for software defined vehicular networks,” IEEE Transactions on Vehicular Technology, vol. 68, no. 3, pp. 2934–2945, 2019.

84.L. Zhao, W. Zhao, A. Al-Dubai, and G. Min, “A novel adaptive routing and switching scheme for software-defined vehicular networks,” in ICC 2019-2019 IEEE International Conference on Communications (ICC). IEEE, 2019, pp. 1–6.