Proceedings of the 25th International Conference on Automation & Computing, Lancaster University, Lancaster UK, 5-7 September 2019

A Survey on secure routing strategies in VANETs

Attiya khan
Department of Computer Science
Bahria University
Islamabad, Pakistan
attiya.lashari@gmail.com

Munazza Ishtiaq
Department of Computer Science
Bahria University
Islamabad, Pakistan
munazzaishtiaq10@gmail.com

Sajjad Anwar
Department of Computer Science
Bahria University
Islamabad, Pakistan
sajjad.bahrian@gmail.com

Munam Ali Shah
Department of Computer Science
COMSATS University
Islamabad, Pakistan
mshah@comsats.edu.pk

Abstract— **VANETS (vehicular ad hoc networks) have evolved from MANETS (mobile ad hoc networks) but facing more challenges because of the self-configuration, deployment and routing features. They follow an infrastructure based (V2I) communication and sometimes direct communication (V2V) between vehicles. In this paper, we focus on the security of VANETs routing protocols and provide an overview of the latest advancements on VANETs routing. We aim to provide an easy and concise view of all the possible vulnerabilities and attacks which can affect the performance of VANETs. This survey defines the security concerns in the connectivity and access techniques within the VANETs.**

Keywords- VANETs, MANETs, ITS (intelligent transportation system), DSRC, IOV, V2I (vehicle to internet), V2V (vehicle to vehicle), FoG computing

I. Introduction

VANETs has improved the experience of driving and vehicles safety. This all prevailed by the Internet of things who has made human life much easier. The things related to internet must work in reliable and secure manner. VANETS (Vehicular ad hoc networks) works mainly according to the working strategy of Manets (Mobile ad hoc networks). But the main difference is that Manets and VANETs protocols work differently because of speed differences of nodes. Many terminologies define this technology of VANETS such as car to car ad hoc mobile communication, network of ad mobile vehicles and ITS (intelligent transportation mobile ad hoc network). Vehicular ad hoc mobile networks are the future, some of its proposed features have been implemented so far. But still perks of VANETS are on way. There are some security threats which can affect the working performance.

Before discussing the security threats, we would like to highlight how VANETS works. Communication between different nodes work with the help of wireless protocol DSRC (dedicated short-range communication). Combination of GPS technology and DSRC has made this concept of low-cost communication between vehicles possible. This technology works only if other vehicles also containing the similar technology. Many countries are working currently to implement VANETS to make this technology implemented all over the world as its basis is network of vehicles. Common transmitted messages work in all vehicles working on principle of VANETS. These messages prevail to nearby vehicles and change accordingly when position of vehicle changes or another vehicle come closer. These messages are path prediction, heading state, vehicle speed, path history, current GPS position and acceleration manner. As all these messages are crucial for communication, so integrity must be ensured.

The exchange of information between vehicles has made road life free from accidents. With the help of predictive nature of VANETs, emergency situations can be dealt very easily. Traffic free road has led to time management efficiently. As VANETs work as interconnected network so malls or other products can share their advertisement easily. But sometimes attackers fabricate the information using unauthorized access. In this case there is need of non-repudiation mechanism for achieving security. VANETSs promises safety of vehicles and ease of drivers and roadside pedestrians as well. Safety measures includes intrusion movement assist, blind spot warning safety, road weather, forward collision warning, emergency electronic brakes lights and left turn assist. Dynamic message signs help drivers to get notified regarding speed. VANETS make smart traffic signals to predict which way and in how much time driver will have to wait. Dynamic transit operation and dynamic ride sharing are other incentives of VANETS. VANETS make your vehicles to communicate not only to other vehicles but to driver as well. Alarm in emergency including vibration of seat and red signs on indictors prevent from any kind of accident. Since there are very large number of nodes in the network. It is difficult to verify and authenticate every node in less time. So, in immediate situations if all nodes do not communicate with each other in mean time accidents can happen [1]. Large number of vehicles increases signals network and demands much larger bandwidth which can cause signals interferences and other signals issues. Due to decentralized system it is difficult to communicate with every vehicle in the network. Though it is a network system, so it is vulnerable to attackers. They can mis interrupt the messages or can inject some malicious information. Safety must be the major concern in implementation of VANETs. With the improvement in technology, different types of attacks improved, a hurdle in security services of the system. The main challenge which VANETS are facing regarding security are Denial of service attack, flooding, spamming and malwares. VANETs are time critical. It is necessary that information must get exchanged on time. But the jamming, which hinders the radio waves during transmission of data is one of the attacks which weakens the performance of VANETs.

The injection of malwares can affect the working of network systems to serious extent. Internet of things are in air nowadays, internet of vehicles (IOV) is coming for sure. Idea is prevailing all over the world and some counties have implemented this idea to some extent till now. Nowadays term "Inter vehicle communication" is being used for VANETS. Many terminologies are being used for this vehicular ad hoc network, but focus is one and that is implementation of spontaneous network of vehicles. This can happen only when solution to every security attack works. Unfortunately, still there are many attacks against VANETs which lack in attaining all security services. There are different attacks that can be a vulnerability for the security of VANETs. Attackers can access the whole network and can use it for their own purpose. In VANETs it is mandatory that the network is always online, all the information exchanged between genuine sender and receiver are authenticated, all the vehicles in network are authenticated and exchange of information is done confidentially between users [2]. Attackers can shut down the whole network, change the information, read the information and can intrude in the network without authentication and become a danger for whole network.

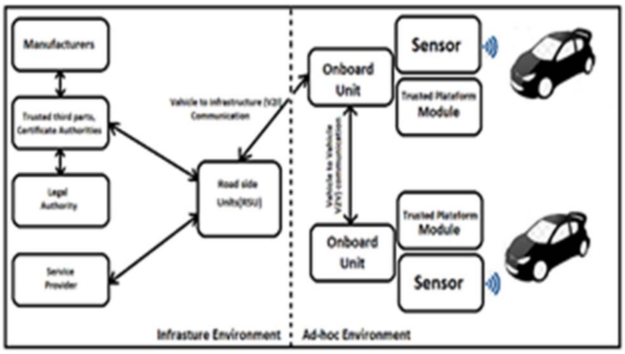

Figure 1: Secure environment in VANETs

II. LITERATURE REVIEW

It is mandatory that each vehicle equipped with radio interface units so that every vehicle can act as sender or receiver and permits detailed information such as GPS or DGPS. The number of unit's distribution is dependent on different communication protocols. Recently researchers put a great effort on its design and architecture but there are still areas that are needed to be improved like widespread adoption of scalable, reliable, robust and secure VANET architectures, protocols, technologies and services [2]. To deal with challenges and risks [3], authors focused on security attacks of Vehicular ad hoc networks and proposed some solutions. This research not only focused on security attacks but on security issues as well. Main security issues in implementation of Vehicular ad hoc networks are key management, location, privacy, reputation and anonymity. This paper provided awareness about malicious attacks which can compromise the performance of VANETs and can leave catastrophic results. These attacks are such as malicious nodes and solution which authors proposed is VARS (a distributed complete approach which focused on reputation and enabled the decision of messages). The solution for traffic analysis attack is VIPER, a proposed protocol which provided anonymity and mixing of nodes [3]. Status, challenges and results of vehicular ad hoc networks [2] have focused on latest research areas related to improved performance of Vehicular ad hoc networks. QoS, security, broadcasting and routing techniques are the main research areas which authors concentrated and concluded salient results. Besides the authors made us realized about new research areas, they explained the latest simulation techniques for the simulation of VANETs.

VANETs technologies [4] work differently in different scenarios. This is due to ITS (Intelligent transportation system) which is the main pillar in the deployment of VANETs technology. As all the nodes which work in VANETs are anonymous to each other and has some unique ids and scenarios. This is the reason we cannot judge one specific result to the challenges which VANETs are facing in their deployment. VANETs architecture comprises of VANETs characteristics, applications, wireless access technologies, communication domain, architecture components, challenges and requirements. To decide about all these components which are necessary for the VANETs architecture is the difficult and still unsolved task. ASPE [5], this is a policy enforcement in VANETs using "Attribute based secure policy". As we have mentioned above that main challenge of VANETs is the difference of scenario and anonymity of nodes. This paper has focused on the high-speed vehicles, which is the challenging task as their communication status with other nodes or vehicles become unpredictive. That's why author suggested attribute based secure policy, focused on developing of trust among nodes in dynamic conditions. These authors have proposed the ASPE framework by using attribute-based encryption. This framework has considered the different situations of roads as an attribute. This proposed framework has provided solution for the main problems which a highly dynamic environment faces and that are security policy enforcement, data access control, key management and secure group information [5]. The researchers [6] reviewed the security challenges precisely, secure infrastructure and potential applications of VANETs. This proposed novel scheme has used the session keys and provided not only the privacy but also the liability maintenance in secure environments. The main feature which made future ITS more attractive is IVC (Inter vehicular communication), enabled by its security services. This reviewed work criticized the previous work that they are not enough solutions for the security of VANETs. The novel secure scheme proposed by authors has provided non-repudiation and confidentiality by using the session keys. This research supports robustness of this proposed scheme [6] As VANETs do not depend on fixed network infrastructure, so security of ad hoc networks remains on question mark. Securing ad hoc networks [7] elaborated security of VANETs by proposing a framework. Besides all these vehicular ad hoc networks depend on each other to keep network connected. Another challenge in designing these networks is their vulnerability to security attacks. For these kind of challenges replication and new cryptography techniques are used like threshold

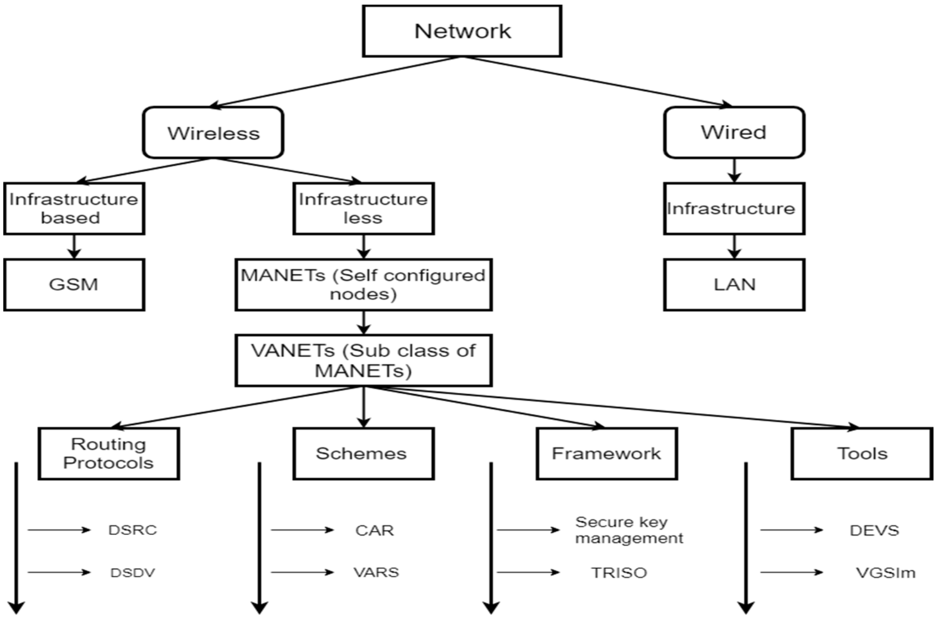

Figure 2: Taxonomy Diagram

cryptography for right management system which terms the core of security frame work [7].

As we know that VANETs have evolved from MANETs [8] authors have provided "energy based efficient authenticated routing protocol" (EBEARP) to increase efficiency of network. In this protocol efficient node selection is used which minimizes power consumption and provides efficient security against route discovery attacks. EBEARP provides better security with less energy consumed [8]. Power consumption is the main challenge of ad hoc networks so [9] provides us with Tirso framework for efficient network. Another challenge arise with the introduction of ad hoc networks is identity protection. Anonymous communication networks were the previous method used for identity protection. Traffic analysis, disclosure and spam attacks are also great challenges in these ad hoc networks. Different protocols have been proposed to make working of VANETs efficient. Designing of these protocols differ according to situation and environment. This paper [10] elaborates the transportation system and designing of protocols for VANETs. This research used the "Virtual laboratory environment" and presented versatile models for the different features of VANETs. This research not only explained but also tested models through simulators and concluded results in real world scenarios of road traffic [10]. Nodes with limited CPU processing capability and Denial-of-Service attacks is another challenge in VANETs. In some cases, some nodes can use excess network bandwidth or processing time which is not good for other nodes. These kinds of challenges also arise in implementation of VANETs. To overcome these kinds of issues, Secure Efficient Ad Hoc Distance vector routing protocol (SEAD) [11] is proposed. It will provide robustness against attackers which hit attacking nodes in VANETs. This research not only focused on attacks but also showed incorrect routing states. To implement the VANETs architecture and services in real world, one more challenge arises and that is the law enforcement [12]. This law enforcement will control network regarding misbehavior of operations. "Privacy preserving defense technique" has been proposed in this research. This research has handled misbehavior of operations in network. Such as VANETs access by deploying an "identity-based cryptosystem" [12]. SECSPP [13] a proposed scheme not only brought improvement regarding communication of nodes in VANETs environment, but also provided anonymous behavior regarding communication. Anonymity of nodes with security is the main challenge in implementation of VANETs. This proposed scheme cohesive blind signature technique and by making comparison with other proposed protocols elaborated its benefits in defined way [13]. There are many security protocols for securing vehicular ad hoc networks [14]. These protocols include RTDP, DRP and RCCRL. Authors of this paper has focused that all the security mechanisms and protocols proposed before these three protocols are not enough [14]. Three things which must be designed carefully for the implementation of VANETs in real life are standards, application and architecture. This tutorial survey [15] has cleared the vision of VANETs by depicting its link with wireless environment. Vehicular ad hoc networks have brought innovation regarding traffic management, safety issues of roads and vehicles communication. As this technology has given us benefits but it also has made road infrastructure vulnerable to security attacks. Human dependence on vehicles has increased after the advent of this technology. In this research focus has been made on "WAVE" applications [16]. Practical implementation of standards is very important and to make this clear author considered two main issues. These issues conditional privacy preservation and certificate revocation consideration has proposed a "novel scheme" [16]. CIA [17] triads are very important pillar in implementation of VANETs. We have come across the thing that accuracy of location is crucial for the nodes participating in VANETs. For achieving this accuracy, achievement of integrity, confidentiality and availability is necessary. Authors have provided security of location by proposing mechanisms. These mechanisms are also an ultimate source to provide privacy in implementation of VANETs [17].

Table 1: Services Achieved in Literature Review

Reference	Privacy	Confidentiality	Integrity	Authentication	Non-Repudiation	QoS
Sherali&Ray[2]	No	No	No	Yes	No	Yes
JT Isaac&S Zeadally [3]	Yes	No	No	No	No	No
NW Wang& WMChen[6]	Yes	Yes	No	Yes	Yes	No
LZhou&ZJ Haas[7]	Yes	Yes	No	No	No	No
Savithri&MR Babu[8]	Yes	No	No	Yes	Yes	Yes
E Ramat&Sondi[11]	Yes	Yes	No	Yes	No	Yes
YC Hu&Johnson[12]	Yes	Yes	Yes	Yes	Yes	Yes
J Sun&Y Fang[13]	Yes	No	Yes	Yes	Yes	Yes
CT Li&YP Chu[14]	Yes	No	No	Yes	Yes	No
M Raya&Hubaux[15]	Yes	Yes	Yes	Yes	Yes	No
Hartenstein&Laberteaux[16]	Yes	No	No	No	No	No
G Sun&L Song[29]	Yes	No	Yes	Yes	Yes	Yes
A Ullah&Shaheen[30]	No	No	Yes	Yes	No	Yes

Our research up till now have made us aware of the fact that position and location of nodes must be addressed first in implementation of VANETs. Security of VANETs can be achieved through active position of nodes in the network [18]. This position detection is a way to detect security attacks.

A Solution has been proposed in this research and simulations have confirmed the correctness and efficiency of this proposed mechanism [18]. To implement VANETs, many issues and requirements must be kept in mind. One of the major requirements is deployment in less cost. We have noticed this issue in [19], where authors have addressed pseudonyms authentication in vehicular ad hoc networks. This approach has been suggested as a vital approach for the deployment of VANETs in real world to control overhead of computational cost [19]. Cheating position of nodes in VANETs can lead to serious security attacks [20]. A solution has been proposed to address this issue and many simulations has been done against this solution. Simulations has confirmed that this solution has prevented falsification of nodes. Before this solution all solutions were dependent on hardware and special infrastructures. Proposed solution is independent regarding hardware issues and is efficient as well to detect false location of nodes [20]. GSIS [21] have brought a worth mentioning protocol which has solved two issues. One issue regarding traceability and second one regarding privacy of nodes. This protocol not only provides privacy but also reveal identity of nodes in case of any dispute. Nodes are anonymous but in case of need their identity can be find out by this specific GSIS protocol [21]. Validation of an emergency event is also a crucial requirement of VANETs. AEMA [22] has been introduced for this validation. In case of emergency events, this approach will help in verification of messages. This scheme is an assured and can differentiate between false emergency messages and correct one [22]. Because of extended research, a scheme has been proposed which has not only provided full requirements of VANETs but also a prevention against security attacks in VANETs. TEAM [23], is based on "hash-based authentication" fulfilling requirements of VANETs with extended security features. The validation of aggregated data has been done to discourage security attacks.

This research [24] has focused on timestamping and signing issues. We have gone through an extensive research and come to the point that besides protocols, mechanisms and scheme an infrastructure [25] is also required for the deployment of VANETs in real world. A secure MAC [26] protocol has been proposed which ensures the safety as well as reliability of VANETs applications [26]. In VANETS intervehicle communication is used by multi-hop broadcasting. In VANETS roadside communication is done through single hop broadcast [27]. If we want to go through detail study of infrastructure based and infrastructure less VANETs deployment, then [28] has provided comprehensive research. This research has provided us with the fact that intelligent transportation system helps a lot regarding best deployment of VANETs. Using ITS enabled technology with FOG computing [29] position-based routing has brought routing advances in VANETs. Parked vehicle assistant relay routing has solved the communication problems and progressed the V2V routing. One thing is important for solving communication problems and that is to enable exact location.

III. DISSCUSSION

This survey paper has covered all the aspects to provide betterment for VANETs. Different mechanisms and protocols have been discussed in related work section. Some protocols which has provided solutions for security attacks VIPER, OLSR, EBEARP, SEAD and RTDP. Survey has been to cover CIA triads and other parameters such as privacy, non-repudiation and quality of service. Classification has been done to elaborate which of these parameters are fulfilled by adapting the schemes and protocols mentioned above. Research has cleared the view that routing protocols must be chosen according to QOS requirements. Although, VANETs work according to the principles of MANETs but their routing protocols and deployment mechanism differs a lot. This survey research considers numerous questions related to Application constraints, security architecture, trust models and challenges related to security.

Table 2. Comparative Analysis

Reference#	Framework	Scheme	Protocol	Technologies	Tools
Sherali & Ray [2]	WAVE	(CAR) routing scheme	OLSR, AODV	IEEE 802.15.3	VGSim
JT Isaac & S Zeadally [3]	Identification and local containment framework	VARS, PVN	VIPER	ITS	---
D Huang & M Verma[5]	Secure key management	ASPE	---	---	---
NW Wang & WMChen [6]	Software based framework	Novel secure communication	DSRC enhanced with safety	IEEE 802.11-p	---
LZhou & ZJ Haas [7]	Key management service	Threshold cryptography	DSDV	---	---
Savithri & MR Babu[[8]	---	---	EBEARP	---	---
M Chinnadurai[9]	Tirso				
Chebbi & Rivoirard[10]	---	CBL	OLSR	Virtual laboratory Environment	DEVS
E Ramat & Sondi [11]	---	HORS signature scheme	SEAD	---	---
YC Hu& Johnson [12]	Identity based cryptosystem	Pseudonym based scheme	---	Privacy preserving defense	---
J Sun& Y Fang [13]	---	SECSPP	EAP-TLS authentication	---	---
CT Li& YP Chu [14]	Security architecture	CARAVAN	RTDP, DRP and RCCRL	Bluetooth, cellular and short range	---
Hartenstein& Laberteaux[16]	conditional privacy preservation and certificate revocation	Novel scheme		Wave applications	
G Sun& L Song [29]	FOG oriented	Position based	DTN	ITS enabled	---
A Ullah& Shaheen [30]	Auto regressive integrated moving average model	PVARR (parked vehicle assistant relay routing)	Position based routing protocols	IEEE 802.11-p	Java tools
G Sun& H Yu[31]	SDVNs (software-based video networking)	SDVN architecture	Traditional all protocols	5G	---
WB Jaballah & C Lal[32]	Secure AOMDV architecture	SE- AOMDV	SAODV, TS-AOMDV	ITS	NS2
Makhlouf & Guizani[33]	Improved TDMA model	Channel sensing scheme	TDMA	IEEE 802.11-p	NS2
R Singh & KS Man[34]	QFRG framework	RWE scheme	---	QOF routing	---

IV. Future work and Conclusion

VANETs are an emerging technology and will get integrated in coming years. This survey research concluded that still there is need of more research for better VANETs environment. There is need of evaluation for the performance of protocols needed for routing of VANETs. There are some techniques, mechanisms and schemes mentioned in related work which are lacking the simulation results. Some parameters such as QOS, credibility, trust model's evaluation and scalability must be calculated or evaluated in efficient manner. One of the biggest challenges of VANETs is to work for response time. Still the research has been done so far is good but as the technology is getting more challenging day by day so VANETs deployment should cover every aspect regarding security, efficiency, less energy consumption, more reliable and robust.

References

[1] Balu, M., G. Kumar, and S.-J. Lim, *A REVIEW ON SECURITY TECHNIQUES IN VANETS.* International Journal of Control and Automation, 2019. **12**(4): p. 1-14.

[2] Zeadally, S., et al., *Vehicular ad hoc networks (VANETS): status, results, and challenges.* Telecommunication Systems, 2012. **50**(4): p. 217-241.

[3] Isaac, J.T., S. Zeadally, and J.S. Camara, *Security attacks and solutions for vehicular ad hoc networks.* IET communications, 2010. **4**(7): p. 894-903.

[4] Al-Sultan, S., et al., *A comprehensive survey on vehicular ad hoc network.* Journal of network and computer applications, 2014. **37**: p. 380-392.

[5] Huang, D. and M. Verma, *ASPE: Attribute-based secure policy enforcement in vehicular ad hoc networks.* Ad Hoc Networks, 2009. **7**(8): p. 1526-1535.

[6] Wang, N.-W., Y.-M. Huang, and W.-M. Chen, *A novel secure communication scheme in vehicular ad hoc networks.* Computer communications, 2008. **31**(12): p. 2827-2837.

[7] Zhou, L. and Z.J. Haas, *Securing ad hoc networks.* IEEE network, 1999. **13**(6): p. 24-30.

[8] Savithri, M. and M.R. Babu, *Energy-based efficient authenticated routing protocol for MANETs for DDOS attacks with minimised power consumption.* International Journal of Networking and Virtual Organisations, 2018. **19**(2-4): p. 289-304.

[9] Manivannan, R. and M. Chinnadurai, *An efficient protocol for power consumption in wireless enterprise ad hoc virtual community network with Triso framework.* International Journal of Enterprise Network Management, 2018. **9**(3-4): p. 317-332.

[10] Chebbi, E., et al., *Simulation of a Clustering Scheme for Vehicular Ad Hoc Networks Using a DEVS-based Virtual Laboratory Environment.* Procedia computer science, 2018. **130**: p. 344-351.

[11] Chebbi, E., P. Sondi, and E. Ramat, *A Formal Model for the Chain-Branch-Leaf Clustering Scheme in OLSR based Vehicular Ad hoc Networks using Event-B.* Procedia Computer Science, 2019. **151**: p. 935-940.

[12] Hu, Y.-C., D.B. Johnson, and A. Perrig, *SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks.* Ad hoc networks, 2003. **1**(1): p. 175-192.

[13] Sun, J., et al., *An identity-based security system for user privacy in vehicular ad hoc networks.* IEEE Transactions on Parallel and Distributed Systems, 2010. **21**(9): p. 1227-1239.

[14] Li, C.-T., M.-S. Hwang, and Y.-P. Chu, *A secure and efficient communication scheme with authenticated key establishment and privacy preserving for vehicular ad hoc networks.* Computer Communications, 2008. **31**(12): p. 2803-2814.

[15] Raya, M. and J.-P. Hubaux, *Securing vehicular ad hoc networks.* Journal of computer security, 2007. **15**(1): p. 39-68.

[16] Hartenstein, H. and L. Laberteaux, *A tutorial survey on vehicular ad hoc networks.* IEEE Communications magazine, 2008. **46**(6): p. 164-171.

[17] Lin, X., et al., *Security in vehicular ad hoc networks.* IEEE communications magazine, 2008. **46**(4): p. 88-95.

[18] Yan, G., S. Olariu, and M.C. Weigle, *Providing location security in vehicular ad hoc networks.* IEEE Wireless Communications, 2009. **16**(6): p. 48-55.

[19] Yan, G., S. Olariu, and M.C. Weigle, *Providing VANET security through active position detection.* Computer communications, 2008. **31**(12): p. 2883-2897.

[20] Calandriello, G., et al. *Efficient and robust pseudonymous authentication in VANET.* in *Proceedings of the fourth ACM international workshop on Vehicular ad hoc networks*. 2007. ACM.

[21] Leinmuller, T., E. Schoch, and F. Kargl, *Position verification approaches for vehicular ad hoc networks.* IEEE Wireless Communications, 2006. **13**(5): p. 16-21.

[22] Lin, X., et al., *GSIS: A secure and privacy-preserving protocol for vehicular communications.* IEEE Transactions on vehicular technology, 2007. **56**(6): p. 3442-3456.

[23] Chuang, M.-C. and J.-F. Lee, *TEAM: Trust-extended authentication mechanism for vehicular ad hoc networks.* IEEE systems journal, 2013. **8**(3): p. 749-758.

[24] Picconi, F., et al. *Probabilistic validation of aggregated data in vehicular ad-hoc networks*. in *Proceedings of the 3rd international workshop on Vehicular ad hoc networks*. 2006. ACM.

[25] Qian, Y., K. Lu, and N. Moayeri. *A secure VANET MAC protocol for DSRC applications*. in *IEEE GLOBECOM 2008-2008 IEEE Global Telecommunications Conference*. 2008. IEEE.

[26] Vaibhav, A., et al., *Security challenges, authentication, application and trust models for vehicular ad hoc network-a survey.* IJ Wirel. Microw. Technol, 2017. **3**: p. 36-48.

[27] Ahmed, S., et al., *VANSec: Attack-resistant VANET security algorithm in terms of trust computation error and normalized routing overhead.* Journal of Sensors, 2018. **2**018

[28] Ullah, A., et al., *Advances in Position Based Routing Towards ITS Enabled FoG-Oriented VANET-A Survey.* IEEE Transactions on Intelligent Transportation Systems, 2019.

[29] Sun, G., et al., *V2V routing in a VANET based on the autoregressive integrated moving average model.* IEEE Transactions on Vehicular Technology, 2018. **68**(1): p. 908-922.

[30] Ullah, A., Yao, X., Shaheen, S., & Ning, H. (2019). Advances in Position Based Routing Towards ITS Enabled FoG-Oriented VANET-A Survey. IEEE Transactions on Intelligent Transportation Systems.

[31] Sun, G., Song, L., Yu, H., Chang, V., Du, X., & Guizani, M. (2019). V2V Routing in a VANET Based on the Autoregressive Integrated Moving Average Model. IEEE Transactions on Vehicular Technology, 68(1), 908-922.

[32] Jaballah, W. B., Conti, M., & Lal, C. (2019). A Survey on Software- Defined VANETs: Benefits, Challenges, and Future Directions. arXiv preprint arXiv:1904.04577.

[33] Makhlouf, A. M., & Guizani, M. (2019). SE-AOMDV: s secure and efficient AOMDV routing protocol for vehicular communications. International Journal of Information Security, 1-12.

[34] Singh, R., & Mann, K. S. (2019). Improved TDMA Protocol for Channel Sensing in Vehicular Ad Hoc Network Using Time Lay. In Proceedings of 2nd International Conference on Communication, Computing and Networking (pp. 303-311). Springer, Singapore.

[35] Liu, L., Chen, C., Wang, B., Zhou, Y., & Pei, Q. (2019). An Efficient and Reliable QoF Routing for Urban VANETs with Backbone Nodes. IEEE Access.

[36] Saxena, R., Jain, M., Sharma, D. P., & Jaidka, S. (2019). A review on VANET routing protocols and proposing a parallelized genetic algorithm based heuristic modification to mobicast routing for real time message passing. Journal of Intelligent & Fuzzy Systems, 36(3), 2387-2398