International Journal of Wireless Communications and Mobile Computing
2024, Vol. 11, No. 1, pp. 11-18
https://doi.org/10.11648/j.wcmc.20241101.12

Research Article

Secure Routing Protocol Based on Junction Selection in VANETs (SERPROV)

Hamza Abassi*, Yenke Blaise Omer

Department of Mathematics and Computer Science, Faculty of Science, The University of Ngaoundere, Ngaoundere, Cameroun

Abstract

Road safety has become a major issue over the last twenty years. The existing transportation system has become inefficient as the number of vehicles has increased remarkably, causing more accidents and other problems. To meet these challenges, the field of Intelligent Transport Systems (ITS) has been proposed. ITS, also known as intelligent transport, is based on vehicle ad hoc networks (VANETs), a subset of mobile ad hoc networks (MANETs) that use moving cars as nodes to create mobile networks. ITS includes various applications such as cooperative traffic monitoring, blind crossings, collision avoidance and traffic flow control. However, dynamic topology and secure communication remain major challenges due to the high mobility of nodes and the random speed of vehicles. This paper proposes a secure protocol called SERPROV (Secure Routing Protocol based on Junction Selection in VANETs) that combines routing and security using a junction selection mechanism and applies an asymmetric cryptography protocol. Simulation results show that SERPROV improves response time and packet delivery ratio compared to existing protocols for a number of vehicles less than or equal to 300. We plan to implement blockchain technology in the future to replace the public key register, thus making the protocol fully decentralized and further exploring the confidentiality of messages exchanged in the VANET environment.

Keywords

ITS, VANET, Routing, Secure Communication, IoT, Adhoc Network

1. Introduction

The total number of vehicles in the world has experienced a remarkable growth, in India for example traffic is growing four times faster than the population [1]. More than 60% of accidents are due to the human errors and half of these accidents can be avoided if the drivers have been notified 0.5 second before [2, 3]. This makes the existing transportation system inefficient. To direct these challenges, a new research field called Intelligent Transportation System (ITS) has been proposed [5], ITS also called Smart Transportation is the new field which based on the vehicular network called Vehicular Ad-hoc network VANET is a subset of Mobile Ad hoc Networks (MANETs) that uses moving cars as nodes in a network to create mobile networks [4]. VANET provides communication among nearby vehicles and between vehicles and nearby fixed equipment i.e., roadside equipment [6]. ITS includes a variety of applications such as co-operative traffic monitoring, blind crossing, prevention of collisions, control of traffic flows nearby information services, advertising [4]. One of the

*Corresponding author: hamzaabassi14avril@gmail.com (Hamza Abassi)

Received: 11 June 2024; **Accepted:** 28 June 2024; **Published:** 15 July 2024

Copyright: © The Author(s), 2024. Published by Science Publishing Group. This is an **Open Access** article, distributed under the terms of the Creative Commons Attribution 4.0 License (http://creativecommons.org/licenses/by/4.0/), which permits unrestricted use, distribution and reproduction in any medium, provided the original work is properly cited.

mains problems in VANETs are dynamic topology and secure communication, Due to high node mobility and random speed of vehicles [7]. As a result of this, network topology in VANETs tends to change frequently, many communication protocols have been proposed in the literature. In VANET, the routing protocols are classified into five categories: Topology based, Position based, Cluster based, Geocast and Broadcast [6, 11, 12]. Position based routing is a suitable candidate for vehicular ad-hoc [8]. There are many position-based protocols, and those are based on "selection of junction", are the best in term of ratio and reliability of communication [9, 10]. According to the literature the Reliable Path Selection and Packet Forwarding Routing Protocol (RPSPF) and the Intelligent Junction Selection Based Routing Protocol (IJS) [35] are the only reliables protocols and no one is secured in "selection of junction" domain [9]. In this paper, we propose a secure protocol called SERPROV (Secure Routing Protocol based on Junction Selection in VANETs) that combine routing and security we are using junction selection mechanism and apply asymmetric cryptography protocol to it, that makes new secured protocol for junction selection-based protocol. The remainder of the paper is organized as follows. Section 2 presents the related works of selection junction-based routing in VANETs, section 3 presents the methodology approach and the protocol algorithm, section 4 presents the simulation environment and le result, then we end with conclusion in section 5.

2. Related Works

In this section, we begin by giving related works in the junction selection-based routing protocol field and end by the security in VANETs.

Intervehicular Position Aware Unicast Routing Schemes	Comparative Features											
	Secure Message Exchange	Traffic Density	Static Junction Selection	Dynamic One hop Junction Selection	Dynamic Multi hop Junction Selection	GPS Require	Digital Map Require	Local Optimum Recovery Technique	Reliability	Using RSUs	Hop Count	Realistic Mobility Flows
GPSR	✗	✗	-	✗	✗	✓	✓	Perimeter mode	✗	✗	Onehop	✓
GSR	✗	✗	✓	✗	✗	✓	✓	Switch back to greedy technique	✗	✗	Onehop	✓
A-STAR	✗	✗	✓	✗	✗	✓	✓	Anchor path reconstruction	✗	✗	Onehop	✓
GPCR	✗	✗	-	✗	✗	✓	✗	Right hand Rule	✗	✗	Onehop	✓
GyTAR	✗	✓	✗	✓	✗	✓	✓	Carry and forward	✗	✗	Onehop	✓
IJS	✗	✓	✗	✓	✗	✓	✓	Carry and forward	✓	✓	Onehop	✓
E-GTAR	✗	✓	✗	✓	✗	✓	✓	Carry and Forward	✗	✗	Onehop	✓
TFOR	✗	✓	✗	✓	✗	✓	✓	Carry and Forward	✗	✗	Twohop	✓
DGSR	✗	✗	✓	✗	✗	✓	✓	Carry and Forward	✗	✗	Onehop	✓
D-EGyTAR	✗	✓	✗	✓	✗	✓	✓	Carry and Forward	✗	✗	Onehop	✓
DMJSR	✗	✓	✗	✗	✓	✓	✓	Carry and Forward	✗	✗	One hop	✓
RPSPF	✗	✓	✗	✗	✓	✓	✓	Carry and Forward	✓	✗	One hop	✓

Figure 1. *Comparison of significant position-based routing protocols.*

2.1. Position Based Protocol and Junction Selection Protocol

Karp, B. et al. proposed Greedy Perimeter Stateless Routing (GPSR) which finds source vehicle locations with the help of GPS [14]. We have also Geographic Source Routing (GSR) developed for the urban scenarios to conquer the limitations of GPSR [9, 13, 16]. This chooses intersections statically without the consideration of traffic density [9]. Then we have also Greedy Perimeter Coordinator Routing (GPCR), it is developed for urban scenarios. The main idea of GPCR is to take advantage of the fact that streets and junctions [17]. Seet, B. C. et al. proposed Anchor-based Street and Traffic-Aware Routing (A-STAR) [18] the particular of A-STAR is the usage of information on city bus routes to identify an anchor path [9, 18]. Jerbi, M. et al. presented their protocol Greedy Traffic-Aware Routing (GyTAR) in [19]. Bhoi et al. proposed the IJS for Intelligent Junction Selection Based Routing Protocol which uses the concept of HV (helping vehicle) for better routing and junction selecting. It is geographical routing protocol for vehicular networks in urban environment. It is Based on a localization system like the GPS to relay data in the network considering the real time road traffic variation

and urban environment characteristics. It considers vehicles speeds, directions and double direction roads. After that, Bilal, S. M. et al. proposed the Enhanced Greedy Traffic-Aware Routing Protocol (E-GyTAR) [20]. This protocol is an enhancement of GyTAR. Enhanced GyTAR (E-GyTAR) is an intersection-based geographic routing protocol which uses GPS to find its own position [20]. Abbasi, I. A. et al. proposed an improves version of E-GyTAR in [21], the Traffic Flow Oriented Routing Protocol (TFOR) [21], this protocol improves the E-GyTAR protocol by taking into account the non-directional traffic density, but suffers from sudden link rupture problem [9]. We have also Directional Geographic Source Routing (DGSR) [10] this, use Geographic Source Routing (GSR) with directional forwarding strategy in city environment. It computes the shortest path to the destination using the Dijkstra algorithm, and uses carry and forward strategy in situation of local maximum problem [10]. We can mention Enhanced Greedy Traffic-Aware Routing Protocol Directional (EGyTAR-D) The extended protocol (E-GyTAR-D) uses directional greedy forwarding to relay packets between the junctions [10]. Abbasi, I. A. et al. developed a new protocol in [23]. Dynamic Multiple Junction Selection based Routing Protocol (DMJSR) [23], The difference between DMJSR and existing approaches is its new dynamic multiple intersection selection method. After Abbasi, I. A. et al. proposed the improves version of the last protocol called Reliable Path Selection and Packet Forwarding Routing Protocol (RPSPF) [22], it accomplishes route by considering multiple junctions and thereby route the packet towards destination [9, 22]. It based on link life-time and link stability to avoid packet-drops because of rapid link ruptures [22]. The weakness of this routing protocol is that it cannot exchange message securely [9].

2.2. VANETs Security

Many security models and security protocol have been proposed to solve the availability, authenticity, confidentiality, integrity and non-repudiation problems in VANETs. Xuejing Yue et al, proposed a blockchain-based decentralized conditional privacy-preserving authentication, which eliminate the risk of single point of failure [15]. Lin, X et al in [29] propose a Timed Efficient and Secure Vehicular Communication which aims at minimizing the packet overhead in terms of signature overhead and signature verification latency without compromising the security and privacy requirements. In Mejri et al. [31] presented the model of communication in VANETs proposed by De Fuentes in [32]. The model shown all component and how they interacting in the VANETs environment. The limit of this model is non-decentralization. Dorri, A et al, proposed a blockchain-based architecture to protect the privacy of users and to increase the security of the vehicular ecosystem [33]. In [28] Manish proposed a centralized model for VANETs security, with trusted authority, it uses traditional system which is not decentralized, they implemented hybrid encryption techniques by combining AES and RSA algorithm. Zhang et al. [24] proposed a data security sharing and storage system based on the consortium blockchain (DSSCB), the advantage this architecture is decentralization so it maintains the concept of self-organizing. Other advantages of DSSCB are: privacy protection, anonymity, and high efficiency [24]. Xiaodong Lin et al. [30] proposed a Timed Efficient and Secure Vehicular Communication (TSVC) scheme with privacy preserving, TSVC minimize the packet overhead by using short message authentication code tag attached in each packet for the packet authentication during the communication. Firdaus, M. et al. [27] proposed an architecture of blockchainbased, it is secure and decentralized. It is composed by three layers: the blockchain network layer, the blockchain edge layer and physical/user network layer. This architecture proposed in [27], user decentralized approach without an intermediary compared to the traditional VANETs framework that employs the centralized approach like [25]. Singh, M. et al. [26] proposed a cryptography based on blockchain technology, it used a concept of vehicular cloud and ensure a secure communication between vehicles. It is also decentralized, every message is considered as transaction, and after mining the block is added to the blockchain. Zhaojun et al. [30] proposed a Blockchain-based Anonymous Reputation System (BARS) to establish a privacy-preserving trust model for VANETs. Centralized schemes cannot handle the increasing complexity of intelligent transportation system structures. Most high privacy and high security are blockchain based solutions. Also, the blockchain gives superior adaptability in getting to the information and it gives better security and privacy in communication between nodes [32]. Singla, A et al [34] proposed three blockchain-based alternatives to the Central Authority-based Public Key Infrastructure for supporting IoT devices. In this approach, each node has a copy of the blockchain database in addition to the blockchain network. This key-sharing technique makes the ecosystem completely decentralized.

3. Methodology Approach

this section, we will discover the proposed protocol, the mechanisms.

3.1. The Junction Selection Algorithm

$$\alpha * NVs + \beta * SR + \gamma * DP + \lambda * NRSUs \text{ where}$$

NVs is the number of vehicles in the current road

SR is the Max speed of the current road

DP is the rapport between distance from current forwarder to destination and distance from neighbor to destination

NRSUs is the number of the Road Side Units on the current road

Figure 2. *Weight calculation formula.*

```
1   Input: α, β, γ, current_forwarder, neighbors
2   Ouput: The next intersection
3   begin
4       set road_list ← []
5       set ʎ ← 1 - α – β - γ
6       if current_forwarder is at the end of intersection then
7           set score ← []
8           set next_road_id ← Null
9           foreach neighbor in neighbors
10              if neighbors.road_id is current_forwarder.road_id then
11                  continue
12              endif
13              if neighbors.road_id not in road_list then
14                  road_list[neighbors.road_id] ← 0
15              endif
16              road_list[neighbors.road_id] ← road_list[neighbors.road_id] + 1
17              dp ← dn ← dc ← 0
18              if next_road_id Is Not Null then
19                  dn ← distance(next_road to destination)
20                  dc ← distance(neighbor current road to destination)
21              endif
22              if dc Is Not 0 then
23                  dp ← dn/dc
24              endif
25              current_road_score = calc_score(road_list[neighbors.road_id], neighbor.road.speed, dp,
26              neighbor.road.RSU.count())
27              next_road_score = calc_score(road_list[next_road_id],next_road.speed, dp,
28              next_road.RSU.count())
29              if next_road_id Not Null or next_road_score > current_road_score then
30                  next_road_id ← neighbor.road_id
31              endif
32          endforeach
33      else
34          normal forward
35      return next_road_id
36  end
37  function calc_score(nb_vehicle, speed, distance_rapport, nb_rsu)
38  begin
39      α ← β ←γ ← ʎ ←0,25
40      return α * nb_vehicle + β * speed + γ * distance_rapport + ʎ * nb_rsu
41  end
```

Figure 3. *junction selection algorithm.*

3.2. The Message Encryption and Forward Algorithm

The algorithm below shows the packet transmission mechanism. Each node generates a public/private key pair when it is initialized. Subsequently, each node's public key is stored in a global register indexed by unique vehicle identifiers. Before sending a message, each node encrypts it using the nexthop's public key. Figure 4 for the packet forward algorithm.

```
Input intersection, neighbors, current_forwarder output Next forwarking Begin
    f_next ← Null
    distance_dest ← Null
    foreach neighbor i of the currentVehicle do
        is_on_same_road ← is_same_road(neighbor)
        if distance_dest is Null) do
            distance_dest ← distance(neighbor to destination)
        endif
        if is_on_same_road and distance(neighbor to destination)< distance_dest do
            NextHop ← neighborVehicle
            distance_dest ← distance(neighbor to destination)
        endif
    endforeach
    if NextHop!=currentVehicle then
        NextHopPK ← getPublicKeyByID(ID)
        Encrypt packet using NextHopPK
        forward packet to NextHop
    else
        keep the packet with Cv (CurrentVehicle)
    endif
end
```

Figure 4. *packet forward algorithm.*

4. Simulation and Results

Through meticulous experimentation, this study reveals a set of compelling results that shed new light on junction selection routing. In this section, we present the results of our simulation, starting with a description of the simulation environment used. Our simulation environment is as follows (Table 1):

Table 1. *Simulation parameters.*

Simulation/Scenario	
Simulation time	100s
Map size	2000 X 2000 m2
Number of intersections	64
Weighting factors	$\alpha = \beta = \gamma = \lambda = 0.25$
Band Name	5.9 GHz
Band With	10 MHz
Radio Medium	IEEE80211
Number of vehicles	100-500
Cryptography algorithms	RSA

Our secure VANET routing protocol called SERPROV has been implemented in the above environment and has been compared in the same environment with one of the GyTar trunk selection routing protocols. The results are conclusive in terms of average reaction time, but also for the ratio, which is superior to the GyTar protocol for a number of vehicles less than or equal to 300. The following figures (Figure 5 and Figure 6) show the two graphs of the results obtained after simulation.

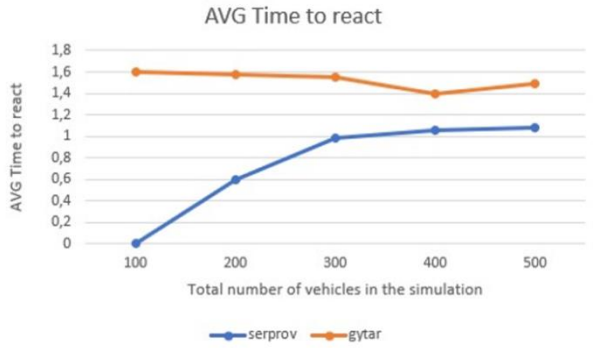

Figure 5. *Average time to react by number of vehicles.*

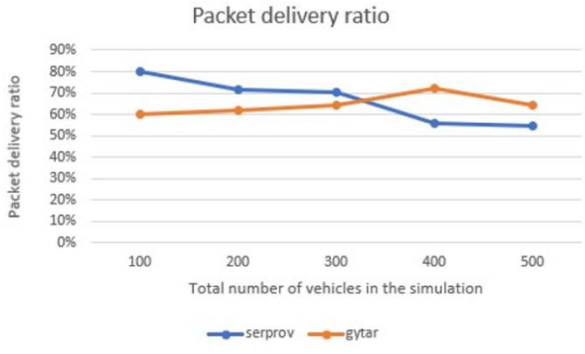

Figure 6. *Packets delivery ratio by number of vehicles.*

5. Conclusions

SERPROV is a secured routing protocol for VANET, in which the global registry is used for public-key exchanging. The protocol selects the better junction before sending pack-

age by considering the density inside two junctions. For every next junction, a score is calculated and the junction with the best score is selected. Then before sending the message. For the security the sender uses the receiver public-key which is accessible in the global registry and encrypts message before sending. The simulation results show that SERPROV performs well. We plan to implement the blockchain technology in near future for replacing the public-key registry for making the protocol completely decentralized and evaluate others criterias. We will also investigate more on privacy for other kind of messages which can be shared in VANET environment.

Abbreviations

ITS	Intelligent Transportation Systems
VANET	Vehicular Adhoc Network
SERPROV	Secure and Reliable Routing Protocol Based on Junction Selection in VANETs
IoT	Internet of Things
MANETs	Mobile Ad-hoc Networks
RPSPF	Reliable Path Selection and Packet Forwarding Routing Protocol
IJS	Intelligent Junction Selection Based Routing Protocol
GPSR	Greedy Perimeter Stateless Routing
GSR	Geographic Source Routing
GPCR	Greedy Perimeter Coordinator Routing
A-STAR	Traffic-Aware Routing
GyTAR	Greedy Traffic-Aware Routing
HV	Helping Vehicle
GPS	Global Positioning System
E-GyTAR	Enhanced Greedy Traffic-Aware Routing Protocol
TFOR	Traffic Flow Oriented Routing Protocol
DGSR	Directional Geographic Source Routing
GSR	Geographic Source Routing
EGyTAR-D	Enhanced Greedy Traffic-Aware Routing Protocol Directional
DMJSR	Dynamic Multiple Junction Selection based Routing Protocol
DSSCB	Data Security Sharing and Storage System based on the Consortium Blockchain
TSVC	Timed Efficient and Secure Vehicular Communication
BARS	Blockchain-Based Anonymous Reputation System
NVs	Number of Vehicles
SR	Speed of Current Road
DP	Distance from Current forwarder to Destination and Distance from Neighbor to Destination
NRSUs	Number of Roadside Units
RSA	Rivest-Shamir-Adleman

Author Contributions

Hamza Abassi: Conceptualization, Data curation, Formal Analysis, Funding acquisition, Investigation, Methodology, Project administration, Resources, Software, Validation, Visualization, Writing – original draft, Writing – review & editing

Yenke Blaise Omer: Supervision

Conflicts of Interest

The authors declare no conflicts of interest.

References

[1] Khekare, G. S., & Sakhare, A. V. (2013, March). A smart city framework for intelligent traffic system using VANET. In 2013 International Mutli-Conference on Automation, Computing, Communication, Control and Compressed Sensing (iMac4s) (pp. 302-305). IEEE. https://doi.org/10.1109/iMac4s.2013.6526427

[2] Rasheed, A., Gillani, S., Ajmal, S., & Qayyum, A. (2017). Vehicular ad hoc network (VANET): A survey, challenges, and applications. In Vehicular Ad-Hoc Networks for Smart Cities (pp. 39-51). Springer, Singapore. https://doi.org/10.1007/978-981-10-3503-6_4

[3] Toor, Y., Muhlethaler, P., Laouiti, A., & De La Fortelle, A. (2008). Vehicle ad hoc networks: Applications and related technical issues. IEEE communications surveys & tutorials, 10(3), 74-88. https://doi.org/10.1109/COMST.2008.4625806

[4] H. Ghafoor and K. Aziz, "Position-based and geocast routing protocols in VANETs", 7th International Conference on Emerging Technologies, IEEE, 2011. https://doi.org/10.1109/ICET.2011.6048483

[5] Abbasi, I. A., Khan, A. S. & Ali, S. A Reliable Path Selection and Packet Forwarding Routing Protocol for Vehicular Ad hoc Networks. J Wireless Com Network 2018, 236(2018). https://doi.org/10.1186/s13638-018-1233-z.

[6] N. V. Pardakhe and R. R. Keole, "Analysis of Various Topology Based Routing Protocols in VANET", International Journal of Advanced Research in Computer Science, Vol. 4, Issue 6, pp. 35-38, 2013. https://doi.org/10.26483/ijarcs.v4i6.1696

[7] Dinesh, D., & Deshmukh, M. (2014). Challenges in vehicle ad hoc network (VANET). International Journal of Engineering Technology, Management and Applied Sciences, 2(7), 76-88.

[8] S. M. Bilal, C. J, Bernardos, C. Guerrero, Position based routing in vehicular networks: A survey. Journal of Network and Computer Applications. 2013 Dec, 36(2013), pp. 685-697. https://doi.org/10.1016/j.jnca.2012.12.023

[9] Abbasi, I. A., & Mustafa, E. E. (2021). A Survey on Junction Selection based Routing Protocols for VANETs. International Journal of Advanced Computer Science and Applications, 174-180. https://doi.org/10.14569/IJACSA.2021.0120121

[10] Bilal, S. M., & Ali, S. (2017). Review and performance analysis of position based routing in VANETs. Wireless Personal Communications, 94(3), 559-578. https://doi.org/10.1007/s11277-016-3637-6

[11] R. Hajlaoui, H. Guyennet and T. Moulahi, "A Survey on Heuristic-Based Routing Methods in Vehicular Ad-Hoc Network: Technical Challenges and Future Trends," IEEE Sensors Journal, Vol 16 Issue 17, 2016. https://doi.org/10.1109/JSEN.2016.2583382

[12] Rejab Hajlaoui. Résolution à base d'heuristiques du problème de routage dans les réseaux ad hoc de vehicules. Réseaux et télécommunications [cs.NI]. Université Bourgogne Franche-Comté, 2018. Français.

[13] Blazevic L., Giordano S., and Boudec L., "Self Organized Routing in Wide Area Mobile Ad-Hoc Network," in Proceedings IEEE Symposium on Ad-Hoc Wireless Networks (Globecom), pp. 44-49, 2001. https://doi.org/10.1109/GLOCOM.2001.965943

[14] Karp, B., & Kung, H. T. (2000, August). GPSR: Greedy perimeter stateless routing for wireless networks. In Proceedings of the 6th annual international conference on Mobile computing and networking (pp. 243-254). https://doi.org/10.1145/345910.345953

[15] Yue, Xuejing and Hu, Huidan and Huang, Keke and Lin, Changlu, Bdcpa: Blockchain-Based Decentralized Conditional Privacy-Preserving Authentication Protocol for Vanets. http://dx.doi.org/10.2139/ssrn.4678944

[16] Lochert, C., Hartenstein, H., Tian, J., Fussler, H., Hermann, D., & Mauve, M. (2003, June). A routing strategy for vehicular ad hoc networks in city environments. In IEEE IV2003 Intelligent Vehicles Symposium. Proceedings (Cat. No. 03TH8683) (pp. 156-161). IEEE.

[17] Soni, Nupur & Tiwari, Shikha. (2013). Survey of Various Protocols in Geographical Based Routing in Vehicular Adhoc Networks. International Journal of Computer Applications Technology and Research. 2. 357-366.

[18] Seet, B. C., Liu, G., Lee, B. S., Foh, C. H., Wong, K. J., & Lee, K. K. (2004, May). A-STAR: A mobile ad hoc routing strategy for metropolis vehicular communications. In International conference on research in networking (pp. 989-999). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-24693-0_81

[19] Jerbi, M., Meraihi, R., Senouci, S. M., & Ghamri-Doudane, Y. (2006, September). GyTAR: improved greedy traffic aware routing protocol for vehicular ad hoc networks in city environments. In Proceedings of the 3rd international workshop on Vehicular ad hoc networks (pp. 88-89). https://doi.org/10.1145/1161064.1161080

[20] Bilal, S. M., Madani, S. A., & Khan, I. A. (2011). Enhanced junction selection mechanism for routing protocol in VANETs. Int. Arab J. Inf. Technol., 8(4), 422-429.

[21] Abbasi, I. A., Nazir, B., Abbasi, A., Bilal, S. M., & Madani, S. A. (2014). A traffic flow-oriented routing protocol for VANETs. EURASIP Journal on Wireless Communications and Networking, 2014(1), 1-14. https://doi.org/10.1186/1687-1499-2014-121

[22] Abbasi, I. A., Khan, A. S., & Ali, S. (2018). A Reliable Path Selection and Packet Forwarding Routing Protocol for Vehicular Ad hoc Networks. EURASIP Journal on Wireless Communications and Networking, 2018. https://doi.org/10.1186/s13638-018-1233-z

[23] Abbasi, I. A., Khan, A. S., & Ali, S. (2018). Dynamic multiple junction selection based routing protocol for VANETs in city environment. Applied Sciences, 8(5), 687. https://doi.org/10.3390/app8050687

[24] Zhang, X., & Chen, X. (2019). Data Security Sharing and Storage Based on a Consortium Blockchain in a Vehicular Adhoc Network. IEEE Access, 1-1. https://doi.org/10.1109/ACCESS.2018.2890736

[25] De Fuentes, J. M., Gonz√°lez-Tablas, A. I., & Ribagorda, A. (2011). Overview of security issues in vehicular ad-hoc networks. In Handbook of research on mobility and computing: Evolving technologies and ubiquitous impacts (pp. 894-911). IGI global.

[26] Singh, M., & Kim, S. (2018). Branch Based Blockchain Technology in Intelligent Vehicle. Computer Networks. https://doi.org/10.1016/j.comnet.2018.08.016

[27] Firdaus, M.; Rhee, K.-H. On Blockchain-Enhanced Secure Data Storage and Sharing in Vehicular Edge Computing Networks. Appl. Sci. 2021, 11, 414. https://doi.org/10.3390/app11010414

[28] Manish, M. T. S. K., Raghuwanshi, N., & Chourasia, B. (2021). A Method for Privacy-Preserving Authentication Based on Hybrid Cryptography for Vanet.

[29] Lin, X., Sun, X., Wang, X., Zhang, C., Ho, P. H., & Shen, X. (2008). TSVC: Timed efficient and secure vehicular communications with privacy preserving. IEEE transactions on wireless communications, 7(12), 4987-4998. https://doi.org/10.1109/T-WC.2008.070773

[30] Lu, Z., Liu, W., Wang, Q., Qu, G., & Liu, Z. (2018). A Privacy-preserving Trust Model based on Blockchain for VANETs. IEEE Access, 1-1. https://doi.org/10.1109/ACCESS.2018.2864189

[31] Mejri, M. N., Ben-Othman, J., & Hamdi, M. (2014). Survey on VANET security challenges and possible cryptographic solutions. Vehicular Communications, 1(2), 53-66. https://doi.org/10.1016/j.vehcom.2014.05.001

[32] Iqbal, S., Bawany, N. Z., & Zulfiqar, A. (2021, January). Blockchain Based Security and Privacy in VANETs. In International Conference on Digital Technologies and Applications (pp. 469-482). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-73882-2_43

[33] Dorri, A., Steger, M., Kanhere, S. S., & Jurdak, R. (2017). BlockChain: A Distributed Solution to Automotive Security and Privacy. IEEE Communications Magazine, 55(12), 119-125. https://doi.org/10.1109/MCOM.2017.1700879

[34] Singla, A., & Bertino, E. (2018, October). Blockchain-based PKI solutions for IoT. In 2018 IEEE 4th International Conference on Collaboration and Internet Computing (CIC) (pp. 9-15). IEEE.

[35] Bhoi, S. K., & Khilar, P. M. (2014). IJS: An intelligent junction selection based routing protocol for VANET to support ITS services. International Scholarly Research Notices, 2014. October 2022). https://doi.org/10.1155/2014/653131