Secure Cluster Selection in Autonomous Vehicular Networks

Mohammed Alkhathami[1†]

Information Systems Department, College of Computer and Information Sciences, Imam Mohammad Ibn Saud Islamic University (IMSIU), 11432, Riyadh, Saudi Arabia.

Summary
Vehicular networks are part of the next generation wireless and smart Intelligent Transportation Systems (ITS). In the future, autonomous vehicles will be an integral part of ITS and will provide safe and reliable traveling features to the users. The reliability and security of data transmission in vehicular networks has been a challenging task. To manage data transmission in vehicular networks, road networks are divided into clusters and a cluster head is selected to handle the data. The selection of cluster heads is a challenge as vehicles are mobile and their connectivity is dynamically changing. In this paper, a novel secure cluster head selection algorithm is proposed for secure and reliable data sharing. The idea is to use the secrecy rate of each vehicle in the cluster and adaptively select the most secure vehicle as the cluster head. Simulation results show that the proposed scheme improves the reliability and security of the transmission significantly.

Key words:
Vehicular network, Intelligent transportation systems, autonomous driving, security.

1. Introduction

Intelligent Transportation Systems (ITS) have gone through many revolutionary changes in the last two decades. With the advancement in sensors and wireless communication, vehicles are becoming more and more secure [1-5]. The sensors deployed in the car not only help make actions such as lane changing to the driver but also help in selecting the best routes to their destination. In fact, driving is moving from fully manual to totally autonomous in the coming days [6-9].

Autonomous driving requires robust wireless communication among all the vehicles and the utilization of sensor data for safe driving [10-13]. The wireless communication challenge is to send data with proper security and reliability. The loss of data can be critical in this vehicular application and can result in loss of lives. Hence, it is important to ensure data privacy and collision free data transmission to enable autonomous driving applications [14-19].

Security and reliability in vehicular networks have two dimensions [20-24]. The first is that the data should be received at the receiver with a very low latency and the packet loss rate should be negligible. This aspect requires efficient data transmission algorithms that can improve the above metrics and ensure data reliability. The second dimension is that the data should remain private and confidential. The integrity of the data needs to be protected. In this case, the data must be protected from eavesdropping of malicious users and other attacks launched by them. To ensure this, cryptographic and physical layer security techniques are needed. There is a critical tradeoff between security and Quality of Service (QoS) as adding a huge amount of security overhead can reduce the latency of the packets. Thus, security needs to be seen in line with the QoS especially for the vehicular networks.

Vehicular networks are composed of several nodes including the vehicles, the Road Side Units (RSUs) and other cloud servers. Data is generally transmitted between vehicles and between vehicles and RSUs. As huge amounts of data are regularly generated, efficient data transmission algorithms are needed. Moreover, to manage data in such a large network, centralized techniques may not perform that well. Thus, the network must be divided into clusters and cluster heads need to be selected. As a result, data can be managed efficiently in a distributed manner as cluster heads will be responsible for collecting and sharing data.

In this paper, a novel cluster head selection scheme is proposed for data collection and transmission in vehicular networks. The idea is to utilize secrecy rate for each link between the vehicles in the cluster and select the cluster head as the one with the maximum average secrecy rate per link. The cluster head vehicle selection is updated periodically. A vehicular network scenario is implemented in MATLAB and detailed simulation results are carried out. Simulation results show that the cluster head selection scheme outperforms the other schemes in the literature.

The paper is organized as follows. Literature review is presented in Section 2. The system model is presented in Section 3. The proposed scheme is presented in Section 4. Simulation results and description of simulation model is presented in Section 5. Conclusions and future work are presented in Section 6.

Manuscript received January 5, 2023
Manuscript revised January 20, 2023
https://doi.org/10.22937/IJCSNS.2023.23.1.2

2. Related Works

2.1 Vehicular Communications

Vehicular communication involves wireless transceiver placed on the vehicle itself which helps it to communicate with other vehicle transceivers. Road Side Units (RSUs) are installed at regular places on the road to provide infrastructure communication services as well as other functionalities such as data caching, task computing, and service provisions. Vehicular network uses Cellular Vehicle to Everything (V2X) communications or Wi-Fi based communications to share data among the nodes. In Wi-Fi based communications, IEEE 802.11p is used whereas in C-V2X communications, 5G networks are used. As shown in Table 1, Autonomous driving can be handled by C-V2X communications whereas short range Wi-Fi communications is used for periodic data sharing among vehicles.

Table 1: Vehicular communication technologies

Wireless Technology	***Range***	**Applications**
IEEE 802.11p	Short	Periodic data sharing
C-V2X	Long	Autonomous driving

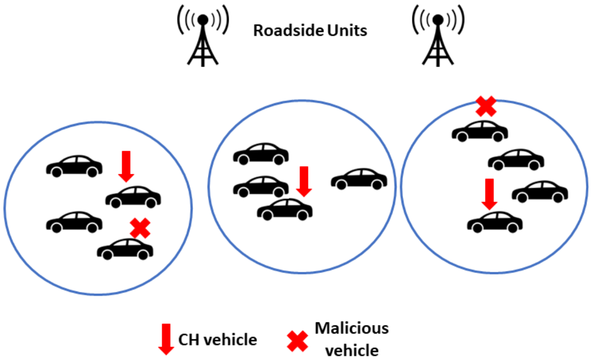


Fig. 1 Vehicular Network System Model.

2.2 Literature Review

In the literature, many techniques have been used clustering approach to handle the data sharing among vehicles. Some approaches that are used for cluster head selection involve time-based and channel quality based [26-27]. In a time-based approach, the cluster head is selected as the vehicle that remains longest within the cluster [26]. The advantage of this approach is that the cluster head selection is stable and lasts for long time. As a result, the overhead for reselection of cluster head is saved. Moreover, data that is transmitted to RSU and to be returned back to the vehicle is handled by the same cluster. This also saves the data transfer among the outgoing and incoming cluster heads.

In comparison, the channel-based approaches of cluster head selection uses wireless channel quality to find the cluster head [27]. The idea is to select the vehicle which has the best channel among all vehicles in the cluster to act as the cluster head. The rationale of this technique is that the vehicle with the best channel can receive and transmit data with higher rates and greater reliability. Since wireless channels are dynamic and changing rapidly, cluster heads are updated regularly. This can result in instability of the cluster head selection. However, this technique can achieve high data rates.

Another issue with this technique can be wireless channel fading. Due to muti-path fading, the signal power at the receiver can be varying. It can be very high at times and low at other times. As a result, channel quality is hard to predict and results in frequent cluster head selection. This also results in data handover problem among the cluster heads in case of changing cluster heads.

One missing issue in the above techniques is that they do not consider security of the links for cluster head selection. This is a critical factor as links with low secrecy rates can result in eavesdropping by malicious users. Data privacy can be compromised in these cases. The focus of this work is to address this missing challenge in the current work.

3. System Model

The system model considered in this paper is shown in Fig. 1. It consists of several vehicles on the road traveling on multiple lanes. The vehicles have wireless transceivers that are C-V2X enabled. Vehicles also have Global Positioning System (GPS) for positioning information. There are RSUs placed on several places on the road which provide long range connectivity to the vehicles. Vehicles regularly share messages with each other and also with RSUs.

The data transmission between vehicles and RSUs is managed with the help of clusters. The road has several clusters of fixed size. Each cluster can contain a different number of vehicles depending on vehicle density. Each cluster has one designated cluster head that manages data sharing between vehicles and RSUs. Also, there are several malicious vehicles on the road with an aim to eavesdrop data.

4. Proposed Scheme

The proposed scheme provides a secure cluster head selection method for vehicular networks. The idea of the scheme is to use vehicles as cluster heads that can maximize the secrecy rate.

The data rate of the link between two vehicles i and j can be given as follows:

$$D(i,j) = B \times \log_2(1 + \frac{p_i \times h_{i,j}}{No}) \qquad (1)$$

Here B is the bandwidth of the vehicular network, p_i is the transmission power of the transmitter, $h_{i,j}$ is the channel gain between the transmitter and receiver link, and No is the noise.

The data rate of the link between vehicle i and malicious vehicle m can be given as follows:

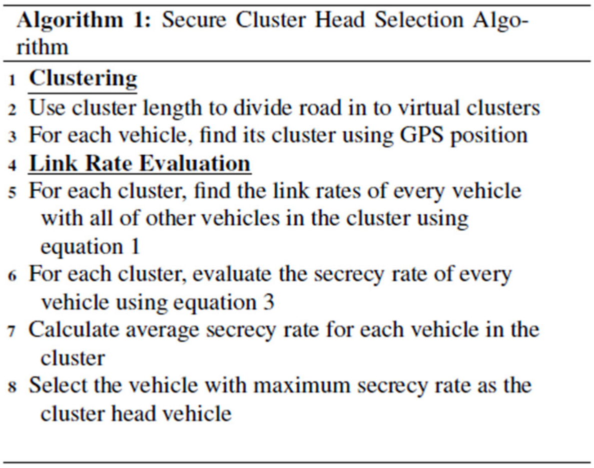
$$D(i,m) = B \times \log_2(1 + \frac{p_i \times h_{i,m}}{No}) \qquad (2)$$

Here$h_{i,m}$ is the channel gain between the transmitter and malicious vehicle link.

The secrecy rate of the link between vehicle i and vehicle j can be given as follows:

$$S(i,j) = D(i,j) - D(i,m) \qquad (3)$$

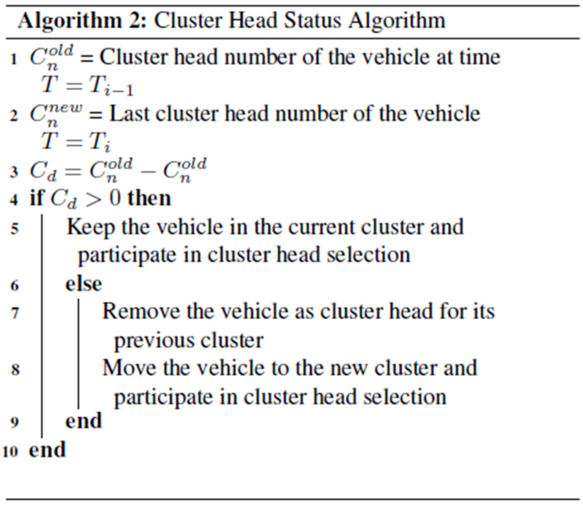
In the proposed scheme, the RSU finds the cluster head for each cluster. For each vehicle that is candidate for the cluster head selection, RSU evaluates its secrecy rate with all other vehicles. An average secrecy rate is computed afterwards for each vehicle. The vehicle that has the maximum secrecy rate is selected as the cluster head vehicle. The algorithm for evaluating the cluster head selection is shown in Fig. 2.



```
Algorithm 1: Secure Cluster Head Selection Algorithm
Clustering
Use cluster length to divide road in to virtual clusters
For each vehicle, find its cluster using GPS position
Link Rate Evaluation
For each cluster, find the link rates of every vehicle
  with all of other vehicles in the cluster using
  equation 1
For each cluster, evaluate the secrecy rate of every
  vehicle using equation 3
Calculate average secrecy rate for each vehicle in the
  cluster
Select the vehicle with maximum secrecy rate as the
  cluster head vehicle
```

Fig. 2 Secure Cluster Head Selection Algorithm

It should be noted that the cluster head can be changed once the data rates are updated. Hence, the secrecy rates are also updated, and new cluster head vehicles are selected. Moreover, if a cluster head vehicle moves to a new cluster head, its status of cluster head is revoked. It enters the new cluster as a normal vehicle and participates in cluster head selection procedure. Also, the previous cluster selects a new cluster head. The algorithm for cluster head status is shown in Fig. 3.



```
Algorithm 2: Cluster Head Status Algorithm
$C_n^{old}$ = Cluster head number of the vehicle at time
  $T = T_{i-1}$
$C_n^{new}$ = Last cluster head number of the vehicle
  $T = T_i$
$C_d = C_n^{old} - C_n^{old}$
if $C_d > 0$ then
    Keep the vehicle in the current cluster and
      participate in cluster head selection
    else
        Remove the vehicle as cluster head for its
          previous cluster
        Move the vehicle to the new cluster and
          participate in cluster head selection
    end
end
```

Fig. 3 Cluster Head Status Algorithm

5. Simulation Results

In this section, simulation results are provided. The simulations are carried out in MATLAB and a vehicular scenario based on Fig. 1 is implemented. A highway scenario is implemented with 2 lanes in each direction. The vehicle density varies from 100 vehicles/km to 300 vehicles/km. The cluster area is taken as 300m. The communication range of wireless transceiver is taken as 500m. The multi-path fading model is Nakagami-m. The speed of vehicles is uniformly distributed between 15 m/s and 30m/s. The vehicle message sharing is 10 messages from vehicles to RSU. Simulation parameters are given in Table 2.

Table 2: Simulation Parameters

Simulation Parameter	***Value in the simulation***
Road Length	3km
Number of lanes	4
Lanes per direction	2
Cluster Area	300m
Vehicle Density	100-300 vehicles/km

Communication Range	500m
Fading Model	Nakagami-m
Speed of vehicle	15 – 30 m/s
Vehicle message sharing	10 messages per second

The results of the proposed Cluster Head Selection (CHS) technique labelled as Proposed CHS are compared against two other protocols. The first is the Channel based CHS technique in which the vehicle with best channel in the cluster is selected as the cluster head. The second is that time-based technique in which vehicle which has highest left over time in the cluster is selected as the cluster head.

Results in Fig. 4 show packet delay against the vehicle density. The results indicate that the packet delay of proposed CHS technique is the best among all techniques. The proposed technique sends packets within 6ms even at high density. Channel based CHS is the second performing technique with delay of less than 10ms. The time-based technique manages to send packets within 12ms.

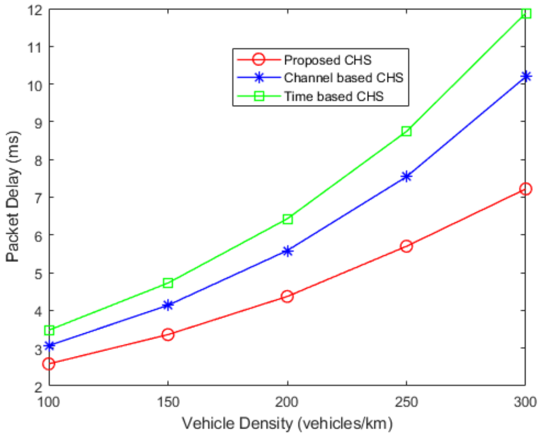


Fig. 4 Vehicular Network System Model.

Results in Fig. 5 show packet loss ratio plotted against vehicle densities. It is clear from the figure that the proposed CHS has the lowest packet loss ratio which means less collisions and data loss. Also, the impact of malicious users' attack is less in the proposed technique. It maintains a loss ratio of 3% or less. Other techniques can go up to a loss of 7-9% which is not suited for autonomous vehicle applications and can cause loss of urgent data.

Results in Fig. 6 show secrecy rate performance of all the techniques. Results give a clear advantage to the proposed technique as it gives the highest secrecy rate. This is important for prevention against eavesdropping attacks by the malicious users. The proposed CHS has almost double the secrecy rate as compared to the other technique. As a result, the proposed technique is much more secure as compared to other techniques. The reason of this increased security lies in the secrecy rate metric utilization in the cluster head selection which was ignored in the literature.

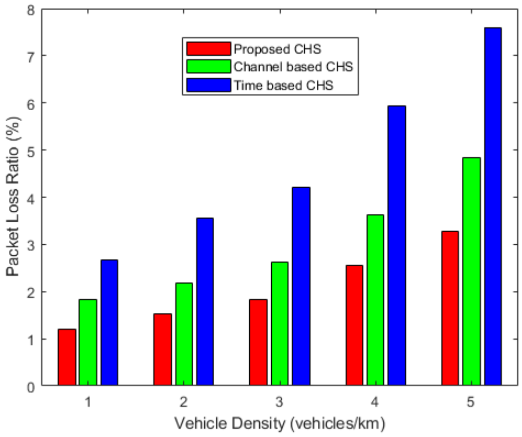


Fig. 5 Vehicular Network System Model.

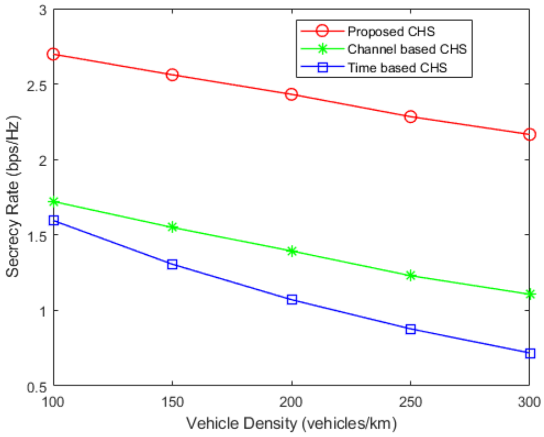


Fig. 6 Vehicular Network System Model.

Results in Fig. 6 shows the percentage of security outage in the proposed technique as compared to the other techniques. The proposed technique is more secure and reliable as it results in very few security outages and eavesdropping incidents. The other techniques have higher security outages. For time-based CHS, this security outage goes up to 6% at a vehicle density of 150 vehicles/km and up to 10% at a vehicle density of 300 vehicles/km. The channel-based shows better security outage performance as it gives 4% security outage at 150 vehicles/km of vehicle density. When the vehicle density is increased to 300 vehicles/km, the security outage is increased to 8%. This is 2% less than the security outage given by time-based CHS. At 300 vehicles/km, the security outage of the proposed CHS technique is less than 0.5%. This shows significant performance gain as compared to the other techniques in terms of security.

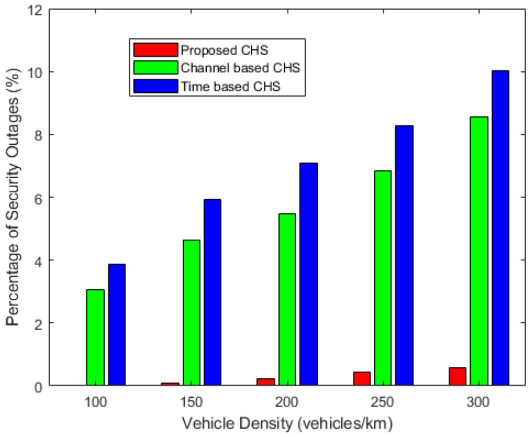


Fig. 7 Vehicular Network System Model.

6. Conclusion

The paper is focused on providing secure and safe data transmission from vehicles to RSUs using cluster heads. The challenge of cluster head selection is addressed by the paper and a secure cluster head selection approach is proposed. The novel idea is to use secrecy rate for cluster head selection so that the cluster head that manages the data relaying is the most secure node in the cluster. Also, the cluster head is regularly updated based on the secrecy rate metric. Simulations have been developed in the MATLAB simulator and many performance metric results are provided at different vehicle densities. The performance of the proposed technique is found to be better in terms of packet delay, packet loss ratio, secrecy rate and percentage of security outages.

References

[1] W. Hu et al., "Formulating Vehicle Aggressiveness towards Social Cognitive Autonomous Driving," in IEEE Transactions on Intelligent Vehicles, doi: 10.1109/TIV.2023.3234253.

[2] S. Zeadally, M. A. Javed and E. B. Hamida, "Vehicular Communications for ITS: Standardization and Challenges," in IEEE Communications Standards Magazine, vol. 4, no. 1, pp. 11-17, March 2020, doi: 10.1109/MCOMSTD.001.1900044.

[3] U. M. Malik, M. A. Javed, S. Zeadally and S. u. Islam, "Energy-Efficient Fog Computing for 6G-Enabled Massive IoT: Recent Trends and Future Opportunities," in IEEE Internet of Things Journal, vol. 9, no. 16, pp. 14572-14594, 15 Aug.15, 2022, doi: 10.1109/JIOT.2021.3068056.

[4] Q. Xu, Y. Liu, J. Pan, J. Wang, J. Wang and K. Li, "Reachability Analysis Plus Satisfiability Modulo Theories: An Adversary-Proof Control Method for Connected and Autonomous Vehicles," in IEEE Transactions on Industrial Electronics, vol. 70, no. 3, pp. 2982-2992, March 2023, doi: 10.1109/TIE.2022.3165293.

[5] F. Jameel, M. A. Javed and D. T. Ngo, "Performance Analysis of Cooperative V2V and V2I Communications Under Correlated Fading," in IEEE Transactions on Intelligent Transportation Systems, vol. 21, no. 8, pp. 3476-3484, Aug. 2020, doi: 10.1109/TITS.2019.2929825.

[6] M. A. Javed, N. S. Nafi, S. Basheer, M. Aysha Bivi and A. K. Bashir, "Fog-Assisted Cooperative Protocol for Traffic Message Transmission in Vehicular Networks," in IEEE Access, vol. 7, pp. 166148-166156, 2019, doi: 10.1109/ACCESS.2019.2953529.

[7] N. Gu, D. Wang, Z. Peng, J. Wang and Q. -L. Han, "Advances in Line-of-Sight Guidance for Path Following of Autonomous Marine Vehicles: An Overview," in IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 53, no. 1, pp. 12-28, Jan. 2023, doi: 10.1109/TSMC.2022.3162862.

[8] W. U. Khan, A. Ihsan, T. N. Nguyen, Z. Ali and M. A. Javed, "NOMA-Enabled Backscatter Communications for Green Transportation in Automotive-Industry 5.0," in IEEE Transactions on Industrial Informatics, vol. 18, no. 11, pp. 7862-7874, Nov. 2022, doi: 10.1109/TII.2022.3161029.

[9] C. Kim, Y. Yoon, S. Kim, M. J. Yoo and K. Yi, "Trajectory Planning and Control of Autonomous Vehicles for Static Vehicle Avoidance in Dynamic Traffic Environments," in IEEE Access, vol. 11, pp. 5772-5788, 2023, doi: 10.1109/ACCESS.2023.3236816.

[10] W. U. Khan et al., "Learning-Based Resource Allocation for Backscatter-Aided Vehicular Networks," in IEEE Transactions on Intelligent Transportation Systems, vol. 23, no. 10, pp. 19676-19690, Oct. 2022, doi: 10.1109/TITS.2021.3126766.

[11] A. N. Alvi et al., "OGMAD: Optimal GTS-Allocation Mechanism for Adaptive Data Requirements in IEEE 802.15.4 Based Internet of Things," in IEEE Access, vol. 7, pp. 170629-170639, 2019, doi: 10.1109/ACCESS.2019.2955544.

[12] F. Jameel, M. A. Javed, S. Zeadally and R. Jäntti, "Efficient Mining Cluster Selection for Blockchain-Based Cellular V2X Communications," in IEEE Transactions on Intelligent Transportation Systems, vol. 22, no. 7, pp. 4064-4072, July 2021, doi: 10.1109/TITS.2020.3006176.

[13] J. Lin, P. Yang, N. Zhang, F. Lyu, X. Chen and L. Yu, "Low-Latency Edge Video Analytics for On-Road Perception of Autonomous Ground Vehicles," in IEEE Transactions on Industrial Informatics, vol. 19, no. 2, pp. 1512-1523, Feb. 2023, doi: 10.1109/TII.2022.3181986.

[14] M. W. Shabir, T. N. Nguyen, J. Mirza, B. Ali and M. A. Javed, "Transmit and Reflect Beamforming for Max-Min SINR in IRS-Aided MIMO Vehicular Networks," in IEEE Transactions on Intelligent Transportation Systems, doi: 10.1109/TITS.2022.3151135.

[15] M. Farahani, S. H. Zegordi and A. H. Kashan, "Developing a solution algorithm for the autonomous electric vehicle routing problem considering the mixed fleet," in IEEE Access, doi: 10.1109/ACCESS.2023.3237481.

[16] J. Mirza, B. Ali and M. A. Javed, "Stable Matching for Selection of Intelligent Reflecting Surfaces in Multiuser MISO Systems," in IEEE Communications Letters, vol. 25, no. 8, pp. 2748-2752, Aug. 2021, doi: 10.1109/LCOMM.2021.3083485.

[17] M. A. Javed et al., "ODPV: An Efficient Protocol to Mitigate Data Integrity Attacks in Intelligent Transport Systems," in IEEE Access, vol. 8, pp. 114733-114740, 2020, doi: 10.1109/ACCESS.2020.3004444.

[18] H. Ren, K. Liu, G. Yan, Y. Li, C. Zhan and S. Guo, "A Memetic Algorithm for Cooperative Complex Task Offloading in Heterogeneous Vehicular Networks," in IEEE Transactions on Network Science and Engineering, vol. 10, no. 1, pp. 189-204, 1 Jan.-Feb. 2023, doi: 10.1109/TNSE.2022.3206228.

[19] M. A. Javed, T. N. Nguyen, J. Mirza, J. Ahmed and B. Ali, "Reliable Communications for Cybertwin-Driven 6G IoVs Using Intelligent Reflecting Surfaces," in IEEE Transactions on Industrial Informatics, vol. 18, no. 11, pp. 7454-7462, Nov. 2022, doi: 10.1109/TII.2022.3151773.

[20] G. Li, P. Wang, T. Yang and H. Che, "Secrecy Sum-Rate Enhancement for NOMA-VLC System With Pseudo User," in IEEE Communications Letters, vol. 27, no. 1, pp. 243-247, Jan. 2023, doi: 10.1109/LCOMM.2022.3220231.

[21] F. Jameel, M. A. Javed, S. Zeadally and R. Jäntti, "Secure Transmission in Cellular V2X Communications Using Deep Q-Learning," in IEEE Transactions on Intelligent Transportation Systems, vol. 23, no. 10, pp. 17167-17176, Oct. 2022, doi: 10.1109/TITS.2022.3165791.

[22] G. Li, P. Wang, T. Yang and H. Che, "Secrecy Sum-Rate Enhancement for NOMA-VLC System With Pseudo User," in IEEE Communications Letters, vol. 27, no. 1, pp. 243-247, Jan. 2023, doi: 10.1109/LCOMM.2022.3220231.

[23] R. Sun, B. Yang, Y. Shen, X. Jiang and T. Taleb, "Covertness and Secrecy Study in Untrusted Relay-Assisted D2D Networks," in IEEE Internet of Things Journal, vol. 10, no. 1, pp. 17-30, 1 Jan.1, 2023, doi: 10.1109/JIOT.2022.3201021.

[24] H. Sharma, N. Kumar and R. K. Tekchandani, "SecBoost: Secrecy-Aware Deep Reinforcement Learning Based Energy-Efficient Scheme for 5G HetNets," in IEEE Transactions on Mobile Computing, doi: 10.1109/TMC.2023.3235429.

[25] Y. Jiang and Y. Zou, "Secrecy Energy Efficiency Maximization for Multi-User Multi-Eavesdropper Cell-Free Massive MIMO Networks," in IEEE Transactions on Vehicular Technology, doi: 10.1109/TVT.2022.3229742.

[26] Javed, M.A., Ngo, D.T. & Khan, J.Y. A multi-hop broadcast protocol design for emergency warning notification in highway VANETs. J Wireless Com Network 2014, 179 (2014). https://doi.org/10.1186/1687-1499-2014-179.

[27] Lei Liu, Chen Chen, Tie Qiu, Mengyuan Zhang, Siyu Li, Bin Zhou, A data dissemination scheme based on clustering and probabilistic broadcasting in VANETs, Vehicular Communications, Volume 13, 2018, Pages 78-88, ISSN 2214-2096, https://doi.org/10.1016/j.vehcom.2018.05.002.