Jordanian Journal of Informatics and Computing
https://jjic.thestap.com/

Vehicular Ad-hoc Networks (VANETs): A Key Enabler for Smart Transportation Systems and Challenges

Haitham Albinhamad[1], Abdullah Alotibi[1], Ali Alagnam[1], Mohammed Almaiah[2], Said Salloum[3]

[1] *Department of Computer Networks and Communications, King Faisal University, Al-Ahsa 31982, Saudi Arabia*
[2] *Department of Computer Science, The University of Jordan, Amman, Jordan*
[3] *School of Science, Engineering and Environment, University of Salford, United Kingdom, UK*

ARTICLE INFO

Article History
Received 05-01-2025
Revised 20-04-2025
Accepted 05-05-2025
Published 07-05-2025

Academic Editor:
Dr. Shahed Almobydeen

Vol.2025, No.1

DOI:
https://doi.org/10.63180/jjic.thestap.2025.1.2

ABSTRACT

Vehicular Ad-hoc Networks (VANETs) are a specialized subset of Mobile Ad-hoc Networks (MANETs) designed to facilitate data exchange between vehicles and infrastructure. These networks operate in two primary modes: Vehicle-to-Vehicle (V2V) communication, which is decentralized and mobile, and Vehicle-to-Infrastructure (V2I) communication, which is centralized and relies on Road Side Units (RSUs). VANETs play a crucial role in Smart City applications, particularly in Intelligent Transportation Systems (ITS), which enhance road safety, reduce traffic congestion, and minimize environmental impact by leveraging real-time data collected from vehicle sensors. The unique characteristics of VANETs, such as high mobility and dynamic topology, enable critical functionalities like collision detection, traffic management, and emergency response coordination. Public service entities, including traffic police, ambulances, and firefighters, benefit significantly from VANETs by receiving real-time alerts and optimizing response times. However, several challenges hinder the widespread deployment of VANETs, including high vehicle speeds, data transmission delays, and cybersecurity concerns. Addressing these challenges is essential to fully realizing the potential of VANETs as a transformative technology in modern transportation systems.

Keywords: Vehicular Ad-hoc Networks (VANETs); Mobile Ad-hoc Networks (MANETs); Intelligent Transportation Systems (ITS).

How to cite the article
Albinhamad, H., Alotibi, A., Alagnam, A., Almaiah, M., Salloum, S., & . (2025). Vehicular Ad-hoc Networks (VANETs): A Key Enabler for Smart Transportation Systems and Challenges. Jordanian Journal of Informatics and Computing, 2025(1), 4–15. https://doi.org/10.63180/jjic.thestap.2025.1.2

*Corresponding author. Email: m.almaiah@ju.edu.jo

1. Introduction

Vehicular ad-hoc Networks (VANETs) are subdomain of Mobile Ad hoc Networks (MANETs) they are used with in vehicles for data communications exchange either between other vehicles which is called Vehicle to Vehicle (V2V) communication or Vehicle to Infrastructure (V2I) communication via radio transceivers located in roads called Road Side Units (RSU). Thus, VANETs considered as hybrid networks since they can be used in two different scenarios as mentioned above with V2V is a Mobile Ad hoc decentralized based communication whereas V2I is an Infrastructure centralized based communication. VANETs provide a short-range wireless connectivity for vehicles which plays a vital role in Smart cities applications. Smart cities promise to make human lives smarter, safer and much efficient through the exploiting Smart Applications that does not require human intervention. One of those Applications is The Intelligent Transportation System (ITS) it is a smart application that aims to improve the functioning Transportation Systems by reducing accidents, Car's traffic and pollution emissions all of this can be achieved with the help of VANETs where vehicles collect important data through embedded sensors and gadgets that provide a real time statistical data that helps in increasing the safety and improving the ground Transportation systems. Figure 1 shows the VANETs communication architecture.

The distinctive features of VANETS are high mobility and dynamic topologies forming due to the mobility nature of Cars. The main advantages of VANETs for driving are collision detection and warning, accidents waring, and Traffic avoidance and management. For governmental authorities especially for Traffic Police, Ambulances and Fire fighters VANETs will make the process of coordination and reaching locations much more efficient by receiving a precise real time information of accidents and emergency case's locations also, roads can be cleared with the help of smart lights to reach in a short time. Although VANETs have many advantages but there are some challenges that make them hard to be used and deployed as: high mobility with high speed of cars, high delay of critical data and security of private information all of these challenges make VANETs to be a not mature technology and needs more enhancements. Figure 2 depicts Accidents warning via VANETs to other vehicles within the area.

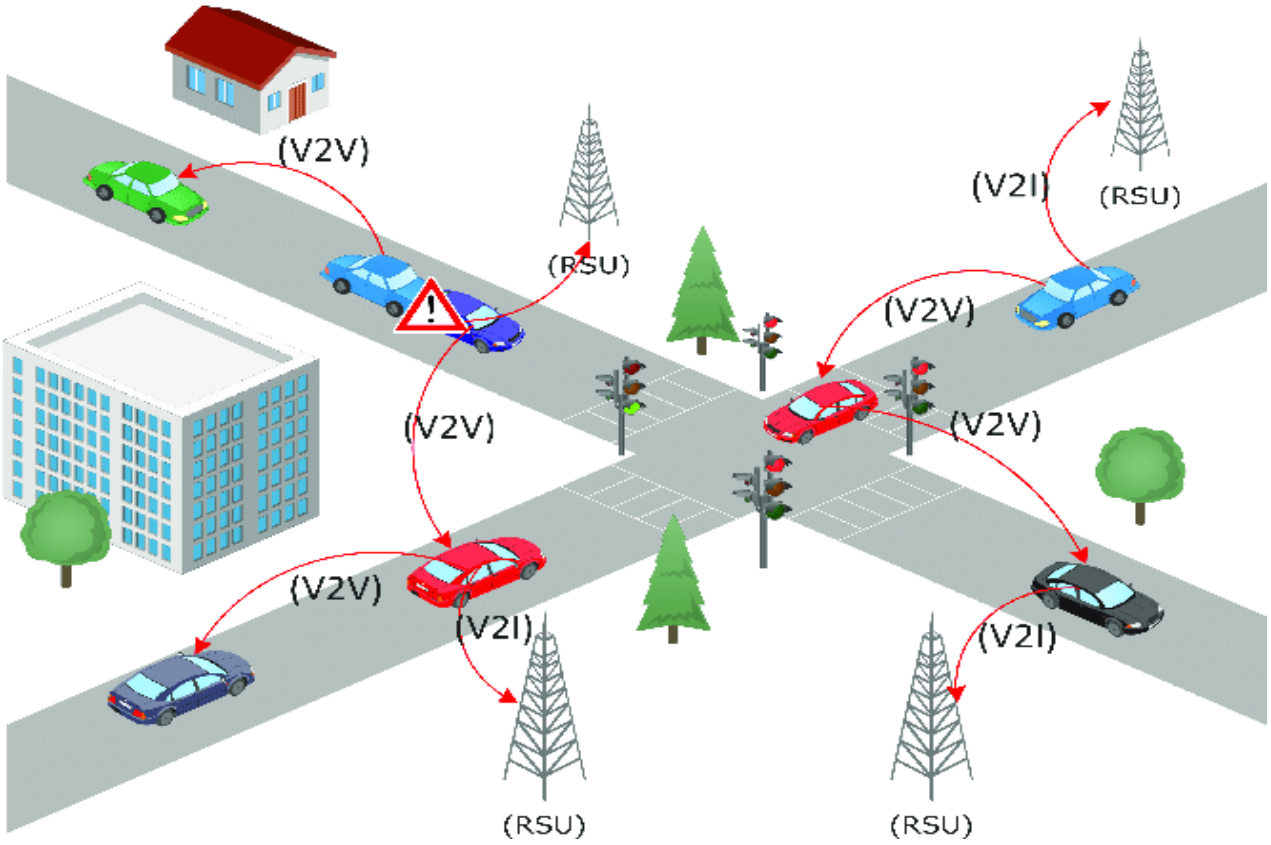


Figure 1. VANETs communication architecture.

*Corresponding author. Email: m.almaiah@ju.edu.jo

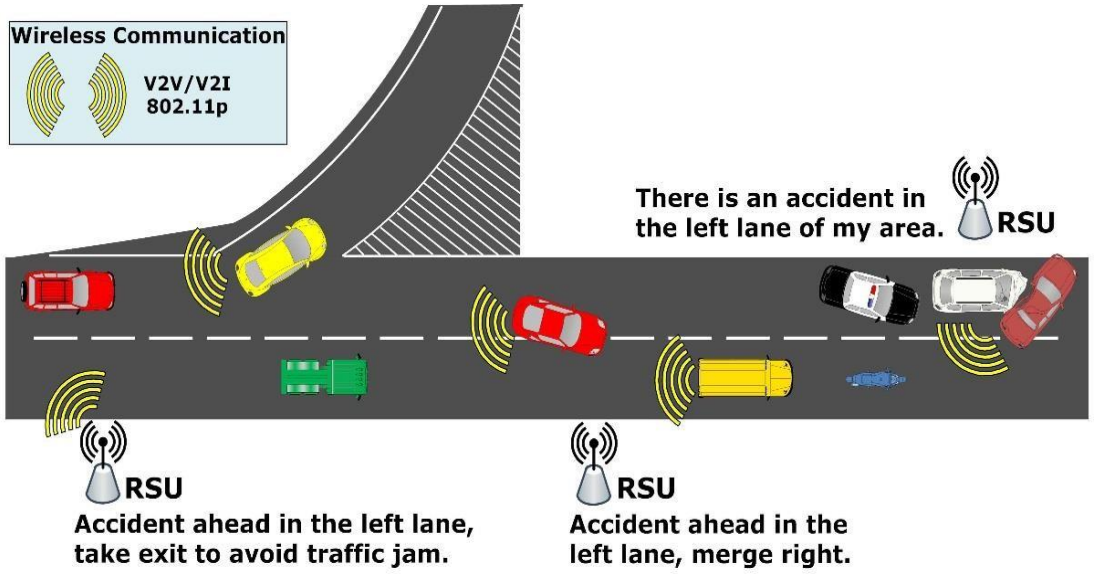


Figure 2. Accidents warning via VANETs to other vehicles within the area.

The objective of this study is to explore the role of Vehicular Ad-hoc Networks (VANETs) in enhancing smart transportation systems by enabling efficient Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communication. This research aims to:

1. Analyze the fundamental architecture, characteristics, and operational principles of VANETs.

2. Investigate the applications of VANETs in Intelligent Transportation Systems (ITS), including traffic management, accident prevention, and emergency response.

2. Related Works

Recent advancements in Vehicular Ad-hoc Networks (VANETs) have focused on improving security, communication efficiency, and real-world deployment challenges. Several studies between 2023 and 2025 have explored innovative solutions to enhance VANET capabilities, particularly in blockchain integration, machine learning-based security, and intelligent transportation systems. One of the notable studies, VANET-Sec: A Framework to Secure Vehicular Ad-Hoc Networks Using a Permissioned Blockchain (2023), introduced a blockchain-based security model that restricts unauthorized access while ensuring data integrity. This framework provided a trusted environment for vehicular communications, mitigating risks associated with fake nodes and unauthorized data transmissions. Similarly, A Secure and Efficient Blockchain-Enabled Federated Q-Learning for VANETs (2024) combined federated learning with blockchain technology to create a decentralized, privacy-preserving VANET system, improving network security and decision-making accuracy.

The integration of VANETs into smart city infrastructure has also been a key focus. A Comprehensive Review of Recent Developments in VANET for Smart Cities (2024) provided an extensive analysis of data acquisition devices, clustering techniques, and energy-efficient routing protocols that enable VANETs to function effectively in urban environments. The findings highlighted scalability and real-time data management as major challenges in the adoption of VANETs for traffic management and intelligent transportation systems (ITS). Another study, PLUG: A City-Friendly Navigation Model for Electric Vehicles with Power Load Balancing upon the Grid (2023), developed a navigation model for electric vehicles (EVs) that utilizes real-time VANET data to optimize power distribution in smart cities. These studies underscore the importance of VANETs in enabling sustainable and efficient urban mobility.

Security remains a major concern in VANETs, given their exposure to cyber threats and privacy issues. Detecting and Preventing False Nodes and Messages in Vehicular Ad-Hoc Networking (2023) introduced an AI-based security mechanism capable of identifying malicious nodes and fake messages that could disrupt communication. This study provided a machine learning-based anomaly detection system to filter out fraudulent data, thereby increasing network reliability. Similarly, Optimized Feature Selection for DDoS Attack Recognition and Mitigation in SD-VANETs (2024) addressed Distributed Denial of Service (DDoS) attacks in Software-Defined VANETs (SD-VANETs), proposing an AI-driven intrusion detection system (IDS) that significantly improved network security. These findings highlight the growing role of artificial intelligence in safeguarding vehicular networks.

*Corresponding author. Email: m.almaiah@ju.edu.jo

Another critical aspect of VANETs is their connectivity and efficiency in high-mobility scenarios. Connectivity Analysis of Directed Highway VANETs Using Graph Theory (2023) employed graph theory models to evaluate the stability of VANET communications on highways. The study found that vehicle density and speed variations play a crucial role in maintaining seamless connectivity. Additionally, Using LoRa Communication for Urban VANETs: Feasibility and Challenges (2023) explored the possibility of leveraging LoRa communication for long-range, low-power VANET applications. While LoRa was found to be cost-effective and energy-efficient, its performance was limited in high-speed vehicular environments, suggesting a need for hybrid communication models.

Trust management and authentication mechanisms are also gaining attention in VANET research. Existence of Trust-Field in Vehicular Ad Hoc Networks: Empirical Evidence (2024) introduced the novel concept of a "Trust Field", which measures the trustworthiness of nodes over time. This study proposed a new metric for assessing the reliability of vehicular communication participants, ensuring safer data exchanges. On a related note, Improvement of the Cybersecurity of the Satellite Internet of Vehicles through an Authentication Protocol Based on a Modular Error-Correction Code (2024) proposed a novel authentication system for satellite-based vehicular networks. This approach enhanced data security and reduced unauthorized access risks, particularly in remote and less-connected areas.
Furthermore, standardization and real-world deployment challenges remain crucial topics of discussion. Vehicular Ad Hoc Networks: Status, Results, and Challenges (2023) provided an extensive review of current VANET adoption trends, emphasizing standardization efforts, industry collaboration, and government regulations. This study identified high deployment costs and interoperability concerns as significant hurdles in real-world VANET implementation. Similarly, An Overview of VANET Vehicular Networks (2023) summarized the latest technological advancements in V2X (Vehicle-to-Everything) communication, highlighting 5G-V2X integration and the growing use of AI-based routing protocols. These findings indicate a shift toward next-generation vehicular networks that can handle high-speed mobility, multi-node connectivity, and dynamic topologies.

Lastly, Enhancing Intelligent Transport Systems through Decentralized Security Frameworks in Vehicle-to-Everything Networks (2025) proposed a blockchain and AI-driven security framework for Vehicle-to-Everything (V2X) networks. This research emphasized the importance of decentralized security mechanisms in modern transportation systems, reducing risks such as data breaches, spoofing attacks, and privacy violations. These advancements align with the overarching goal of making VANETs more secure, efficient, and resilient to cyber threats.

3. Background of the research

3.1 Architecture of VANET

Since VANET technology must perform all reorganizations a driver does when driving, like avoiding collisions with other vehicles by having a distance between them, taking the best path, turning either right or left when there is a curve, it uses Cooperative Intelligent Transport System (C-ITS). There are actually two communication types included in C-ITS, one is Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I). C-ITS provides data exchange between vehicles, and between vehicles and infrastructure, which ensures safety, efficiency and friendly environment. When we talk about V2V, we mean the communication and data exchange between the vehicles themselves while on the road which includes the location, the desire to turn either right or left, and the desire to slow down or to stop. And what we mean by V2I is the communication between vehicles and the centralized system on the road in which the system can tell a vehicle about the paths with less congestion, paths with accident. Since routing protocols are critical to any network for data to be transmitted efficiently and securely, both ways of communication require protocols to organize them. Figure 3 represents the main Architecture of VANET.

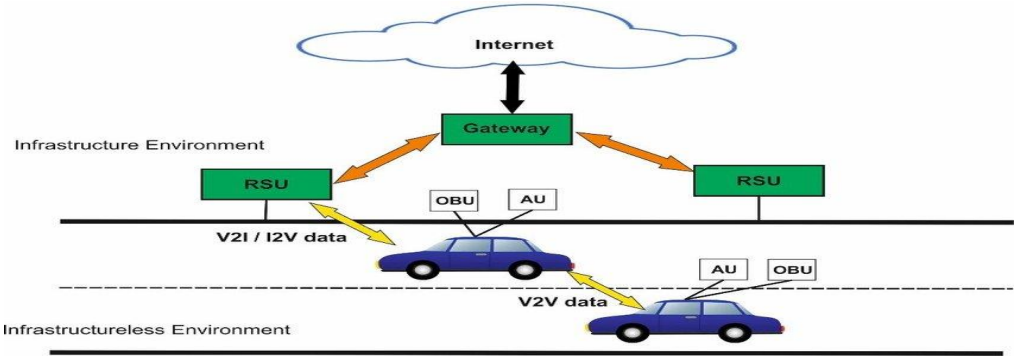


Figure 3. Architecture of VANET

3.2 Vehicle-to-Vehicle (V2V)

*Corresponding author. Email: m.almaiah@ju.edu.jo

The routing protocols are either proactive, reactive or hybrid. In proactive protocols, information on routing are maintained and updated between nodes of a network at all times such as Open Link State Routing protocol (OLSR). In reactive protocols, the information of routing are maintained and updated in demand and when needed such as Adhoc on Demand. Distance Vector protocol (AODV). In this paper, we are going to discuss the way these protocols can be used.
The routing types needed in VANET are broadcast in which a message is sent to all nodes or in other words to all vehicles on different roads, geocast in which a message is sent to all nodes within an area or within the sender's road. These two routing types are important in VANET because sometimes vehicles need to send and receive such messages to have a knowledge of the nearby vehicles status.

OLSR is a proactive protocol which means that the topology information are exchanged between nodes periodically whether there is a request or not. So, the topology information are already there when needed, not maintained when needed. In OLSR, there are nodes called multi point relays which can be used to transfer the control messages between nodes. In doing so, they calculate the routes between a given node and the destination. In the traffic scenario, these nodes can be vehicles that transfer information like congestion or accident to other nodes on the road.

VANET topology is a highly dynamic topology that changes in moments, which requires quick updates to the routing information for each node. In VANET, each vehicle has to inform other vehicles about its existence by sending a GeoNetworking beacon. A Location Table is built according to the Geo Networking beacons received by other vehicles and can be used at any time to know the locations of the neighboring nodes. The neighboring nodes are not just the direct neighbors with one-hop range, but also other nodes with two-hop range. As we said previously, that the vehicular topology is highly dynamic, a Location Table may not contain fresh information about the location of a node. In this case, a service called location service is used and it is simple. The sender sends a Location Request packet to the surrounding nodes in a way similar to the Topological Broadcast scheme. Whenever the packet reaches the destination or a node that has fresh information about the destination, a Location Reply packet is sent back to the sender. AODV protocol is also applicable in VANET. It's a reactive protocol in which when a node wants to send to another node, it searches through the network for the path for the destination on demand. This protocol can be helpful in traffic scenario in which broadcasting messages are sent when needed.

3.3 Vehicle-to-Infrastructure (V2I)

V2I communication plays a very critical role in VANET. It's a communication between the vehicles and the centralized system. The communication can be categorized as ad-hoc or infrastructure-based communication. The role of this communication is to give the best path to the vehicle when there are many paths, collecting data on road like the congestion and accidents to inform vehicles about other roads to avoid passing the

Congested roads, informing the vehicles about curves for the vehicles to turn right or left with an angel appropriate to the curve. It's actually the communication between the vehicle and the highway infrastructure. Both V2V and V2I use Dedicated Short Range Communication (DSRC) frequencies. The architecture of V2I should mainly contain (1) Vehicle On-Board Unit (OBU), (2) Roadside Unit (RSU) and (3) Safe Communication Channel. OBU is the vehicular side of the V2I system. Its architecture is the architecture of the vehicle that is needed to communicate with the infrastructure. It consists of a radio transceiver (using DSRC), a GPS system, an applications processor and interfaces. OBU may collect data from the vehicles and GPS data to transmit them to the RSU. RSUs may located at intersections, interchanges or even petrol stations. It consists of a radio transceiver (similar to OBU), an applications processor and interface to the V2I communication system. We could say that RSU is the infrastructure side of the V2I system. The DSRC roadside unit prevent collisions when there is a congestion. It can tell the location of the start of the congestion. It informs the vehicles to slow down and take different lanes or routing.

*Corresponding author. Email: m.almaiah@ju.edu.jo

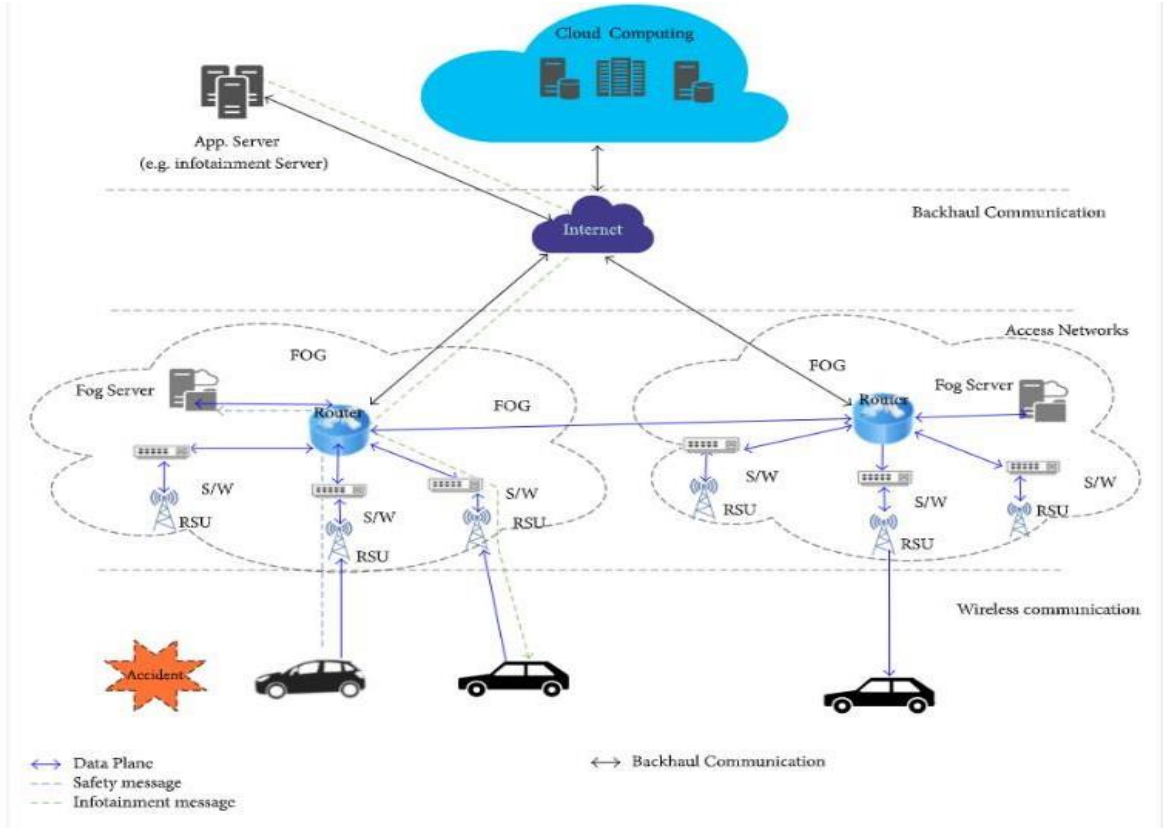


Figure 4. The mMobility nature of VANETs

4. Analysis and Findings

4.1 Findings of the main VANET challenges

The major Challenges requirements of future VANETs:

1- Support of network intelligence: one of the challenges of future VANETs is that it needs to support network intelligence. In future VANETs, there will be a large number of sensors installed in vehicles, and the edge cloud collects and preprocesses the collected data before sharing them with other parts of the network, more data needed more sensor applied for example, conventional cloud servers.

2- Low latency and real-time application: low latency is the fundamental requirement in future VANETs regarding real-time applications. Low latency can avoid accident in VANETs transportation system. Future VANETs should support real-time applications, like safety messages with very low latency.

3- High bandwidth: in future, infotainment and comfort applications such as high quality video streaming will be in high demand. In addition, traffic applications such as 3D maps and navigation systems require frequent automatic updates.

4- Connectivity: to meet the high communication requirements, future VANETs necessitate seamless connectivity between connected vehicles. Connected and driverless vehicles should maintain continuous and highly reliable communication between vehicles and fog devices. It should be able to avoid transmission failures in the communication system.

5- High mobility and location awareness: future VANETs require high mobility and location awareness of the vehicles participating in communication. Each vehicle should have the correct position of other vehicles in the network to deal with an emergency situation.

6- Connected vehicles are equipped with wireless sensors that aid in Vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I) communication. One of the challenges for connected vehicles is how to ensure that information sent across the network is secure.

*Corresponding author. Email: m.almaiah@ju.edu.jo

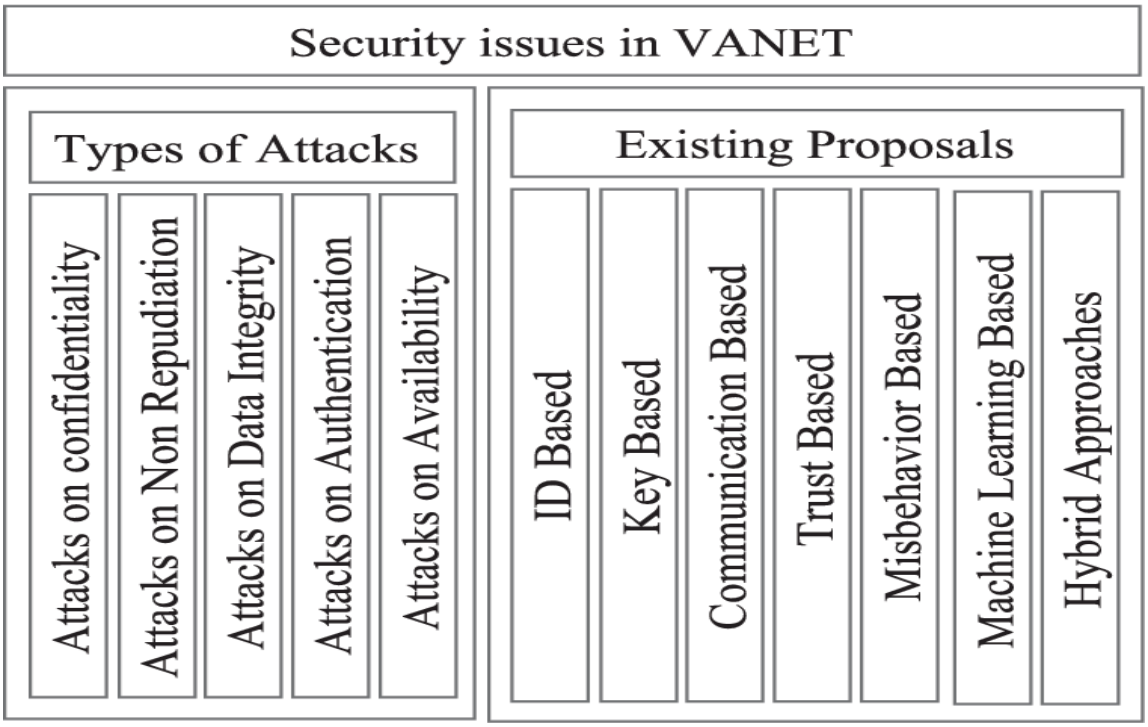


Figure 4: Security Issues and Existing Protocols

4.2 VANETs Applications

The Transportation Sector is facing many challenges and the keep on increasing due to the increase in the number of Cars and Buses that are being used in roads. Consequently, the number of accidents, traffic and pollution emissions has been which motivate the need for other smart solutions to control and reduce all of the overhead caused by the mobile transportations. Many applications are developed to deal with these challenges they ensure the safety, traffic control and reducing pollution emissions.

The main goal of the application is to minimize the traffic in roads by controlling traffic lights based on the real time traffic condition. A real time traffic data is being collected by loop detectors embedded in the Traffic Signals that can detect the presence of cars along with monitoring cameras deployed in roads. The loop detectors are connected to the traffic signal control which controls the signal opening and closing also the amount of the time interval of each. Moreover, Cars are using VANET for exchanging data into modes V2I and V2V, in V2I a real time data for critical safety data is being send to a centralized system owned by the government. The V2V a real time data is exchange between vehicles via sensors regarding the traffic condition in the road's vehicle broadcast 300 ft to warn other near vehicle about the traffic conditions which minimizes the accidents.

*Corresponding author. Email: m.almaiah@ju.edu.jo

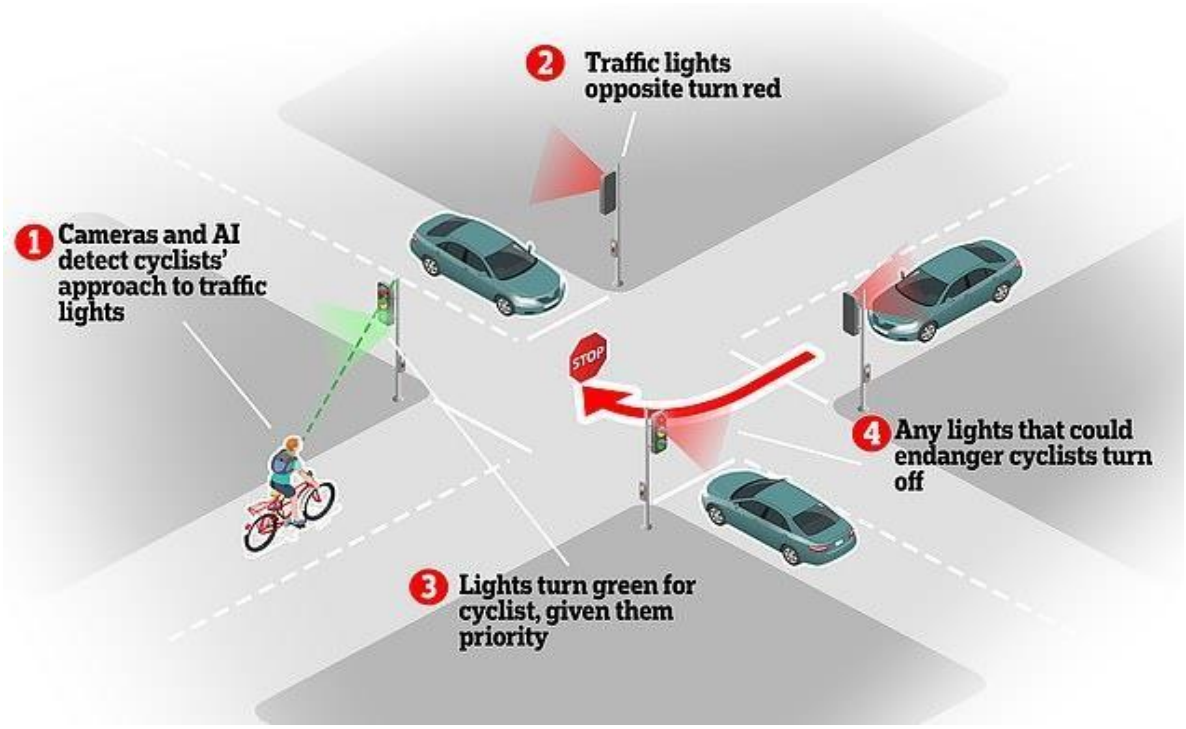


Figure 5: Smart Traffic lights working procedures

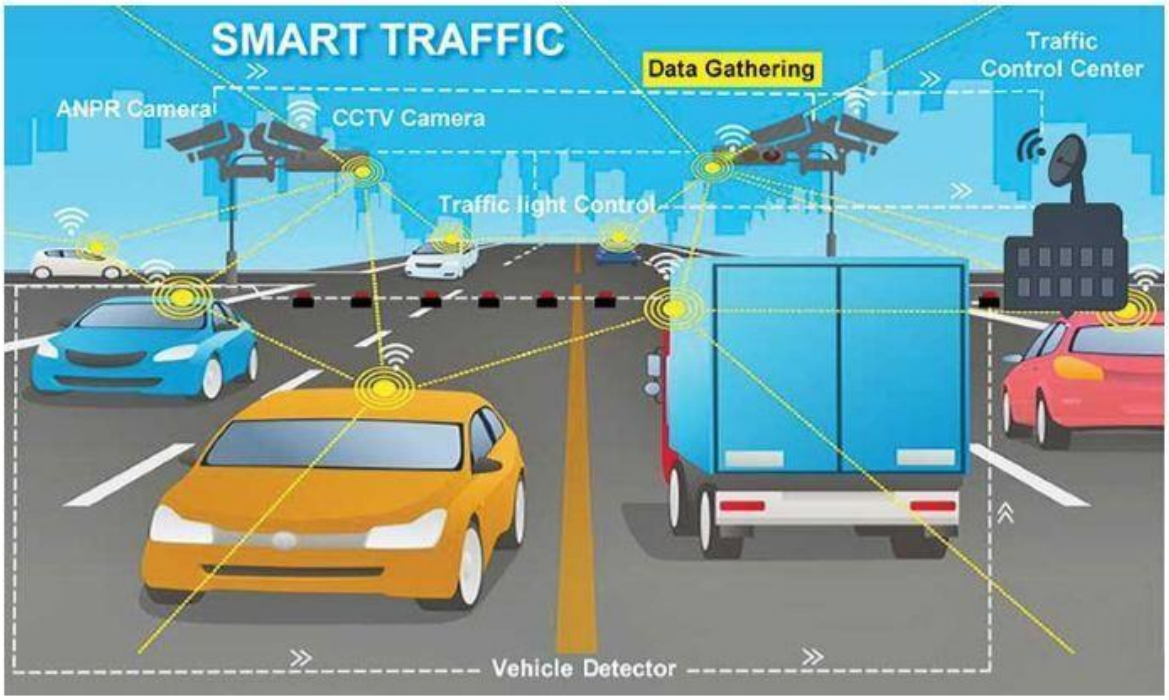


Figure 6: V2V Traffic data exchange

4.3 Autonomous Platoon Formation for VANET

Platoon is an automated driverless mechanism where s one vehicle is selected as a leader for a platoon group and the other vehicles join the platoon group to follow the leader driving instructions. The main purpose of automated platoon is to increase the capacity and safety in roads while decreasing the accident and the traffic. The automated platoons are part of the Intelligent

*Corresponding author. Email: m.almaiah@ju.edu.jo

Transportation System and as mentioned the automated platoons system is designed to manage vehicles and the traffic mutinously which ensures traffic and accidents avoidance. One of the important components of the autonomous platoon is the adaptive cruise control where the speed is set based on the leader data and the distance between the vehicles also, this data is exchanged between the leader and vehicles and the vehicle them sleeves via VANET. The platoon leader is vehicle with a human driver for ensuring the safety and stability of the platoon group the rest of the vehicles that follow the leader are called the followers. The whole platoon moves in the same lane as the leader, and they exchange the location information with the help of the GPS injected sensor in each vehicle.

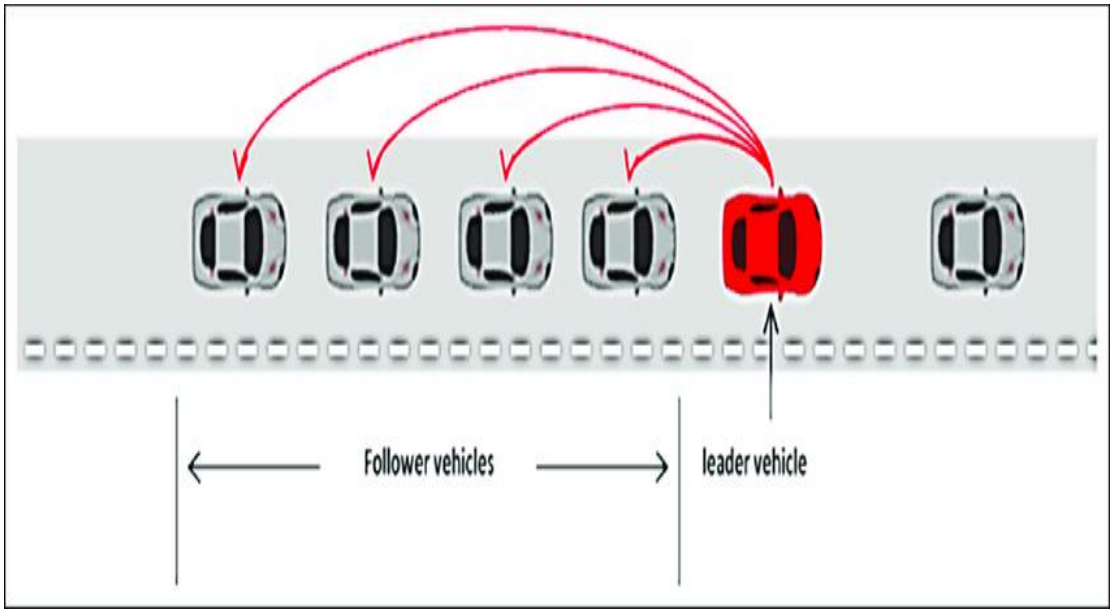


Figure 7: A group of vehicles in a platoon

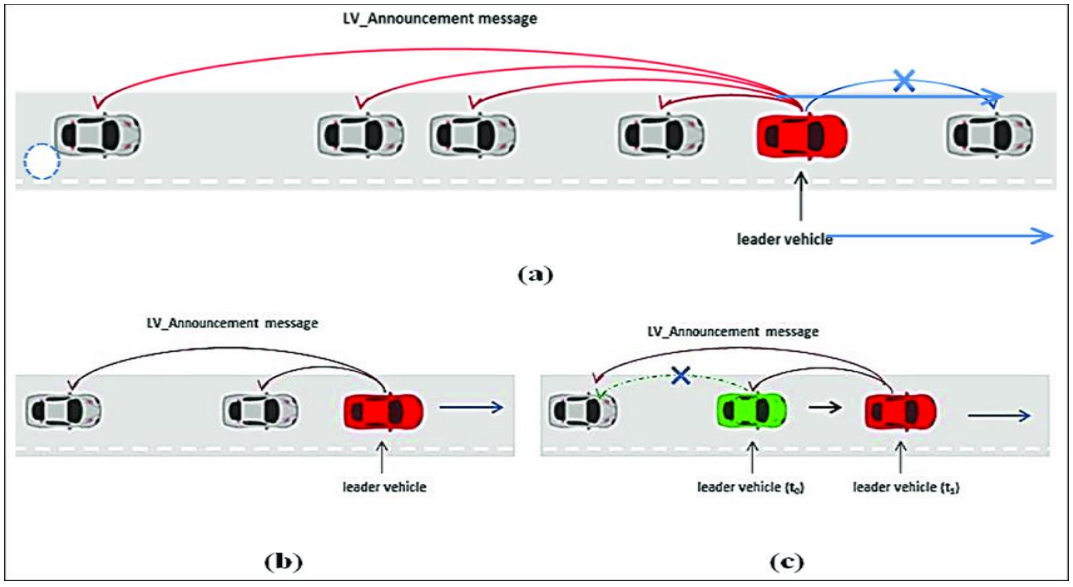


Figure 8: Procedure of platoon formation (a) leader vehicle selection, (b) platoon formation, (c) platoon merge

*Corresponding author. Email: m.almaiah@ju.edu.jo

4.4 VANET Future Applications and Trends

There are many projects and research going in VANET Cooperative Mobility based on ITS - EU standards for Intelligent Transportation Systems, these applications can be classified into three main categorizes Active Road Safety, Cooperative Traffic Efficiency and Global Internet Services. The Active Road Safety applications constants on accidents prevention and driver awareness where the driver will be notified and alarmed if there is any action is needed to be taken or the vehicle itself take the needed action. The Cooperative Traffic Efficiency Applications focus on enhance the road safety and reduce the environmental emissions also, achieving zero random traffic accidents with the help of coexist technologies as autonomous platoon. The Global Internet Services can be exploited for entertainment services as video streaming shared among platoon followers' vehicles or the road seen can be shared via the leader cameras with the follower's vehicles these services will attract drivers to join platoon groups.

5. Conclusion

Vehicular Ad-hoc Networks (VANETs) have emerged as a transformative technology in modern transportation systems, enabling seamless communication between vehicles and infrastructure. This study has explored the fundamental aspects of VANETs, including their architecture, communication models, applications, and challenges. The findings indicate that VANETs play a critical role in enhancing road safety, traffic management, and emergency response, making them essential components of Intelligent Transportation Systems (ITS) and smart city initiatives. Despite their significant potential, the deployment and adoption of VANETs face several challenges. High mobility and dynamic topology, inherent to vehicular environments, introduce difficulties in maintaining stable communication links. Additionally, data security and privacy concerns remain major obstacles, as VANETs are highly susceptible to cyber threats such as message tampering, spoofing attacks, and unauthorized access. The reviewed studies highlight ongoing research efforts aimed at overcoming these challenges through blockchain-based security models, AI-driven intrusion detection systems, and decentralized authentication mechanisms. The integration of VANETs with emerging technologies such as 5G, edge computing, and artificial intelligence (AI) has the potential to further enhance network efficiency, scalability, and reliability. The shift toward hybrid communication models, incorporating technologies like LoRa, 5G-V2X, and satellite IoV, can address limitations related to network coverage and connectivity in high-speed environments. Furthermore, the adoption of machine learning-based trust management systems can improve the overall security and reliability of VANET communications, ensuring safer and more efficient vehicular interactions.

Looking ahead, further research is required to optimize VANET protocols, enhance cybersecurity measures, and develop cost-effective deployment strategies. Collaborative efforts between academia, industry, and government agencies will be crucial in standardizing VANET technologies and ensuring their successful integration into smart transportation ecosystems. As technology advances, VANETs will continue to evolve, paving the way for fully connected, autonomous, and intelligent vehicular networks that contribute to safer and smarter road systems worldwide. By addressing current limitations and embracing technological advancements, VANETs have the potential to revolutionize transportation infrastructure, improve urban mobility, and create a more secure and efficient driving experience for all road users.

Funding

No funding.

Author contributions

Conceptualization, H.A.; methodology; A.A; formal analysis, A.A.; investigation, H.A.; resources, A.A.; writing original draft preparation, A.A.; writing—review and editing, H.A., A.A. All authors have read and agreed to the published version of the manuscript.

Conflicts Of Interest

The authors declare no conflicts of interest.

Data Availability Statement

The data that support the findings of this study are available from the corresponding author upon reasonable request.

Use of Generative Artificial Intelligence

The authors declare that no generative artificial intelligence tools were used in the preparation of this manuscript.

References

[1] Lottermann, C., Botsov, M., Fertl, P., Müllner, R., Araniti, G., Campolo, C., ... & Molinaro, A. (2015). Vehicular ad hoc networks: Standards, solutions, and research.

[2] Artimy, M. M., Robertson, W., & Phillips, W. J. (2009). Vehicular ad hoc networks: an emerging technology toward safe and efficient transportation. *Algorithms and Protocols for Wireless and Mobile Ad Hoc Networks*, 405.

[3] Su, D., & Ahn, S. (2016). Autonomous platoon formation for VANET- ENABLED vehicles. 2016 International Conference on Information and Communication Technology Convergence (ICTC). doi:10.1109/ictc.2016.7763478

[4] Ferrari, G., Medagliani, P., Di Piazza, S., & Martalo, M. (2007). Wireless sensor networks: Performance analysis in indoor scenarios. *EURASIP Journal on Wireless Communications and Networking*, *2007*(1), 081864.

[5] Fotohi, R., Firoozi Bari, S., & Yusefi, M. (2020). Securing wireless sensor networks against denial-of-sleep attacks using RSA cryptography algorithm and interlock protocol. *International Journal of Communication Systems*, *33*(4), e4234.

[6] Huanan, Z., Suping, X., & Jiannan, W. (2021). Security and application of wireless sensor network. *Procedia Computer Science*, *183*, 486-492.

[7] Yang, T., Zhai, F., Xu, H., & Li, W. (2022). Design of a secure and efficient authentication protocol for real-time accesses of multiple users in PIoT-oriented multi-gateway WSNs. *Energy Reports*, *8*, 1200-1211.

[8] Butt, S. A., Diaz-Martinez, J. L., Jamal, T., Ali, A., De-La-Hoz-Franco, E., & Shoaib, M. (2019, July). IoT smart health security threats. In *2019 19th International conference on computational science and its applications (ICCSA)* (pp. 26-31). IEEE.

[9] Deebak, B. D., & Al-Turjman, F. (2020). A hybrid secure routing and monitoring mechanism in IoT-based wireless sensor networks. *Ad Hoc Networks*, *97*, 102022.

[10] Fotohi, R., Firoozi Bari, S., & Yusefi, M. (2020). Securing wireless sensor networks against denial-of-sleep attacks using RSA cryptography algorithm and interlock protocol. *International Journal of Communication Systems*, *33*(4), e4234.

[11] Almaiah, M. A., Hajjej, F., Ali, A., Pasha, M. F., & Almomani, O. (2022). A novel hybrid trustworthy decentralized authentication and data preservation model for digital healthcare IoT based CPS. Sensors, 22(4), 1448.

[12] Almaiah, M. A., Ali, A., Hajjej, F., Pasha, M. F., & Alohali, M. A. (2022). A lightweight hybrid deep learning privacy preserving model for FC-based industrial internet of medical things. Sensors, 22(6), 2112.

[13] Babaeer, H. A., & Al-Ahmadi, S. A. (2020). Efficient and secure data transmission and sinkhole detection in a multi-clustering wireless sensor network based on homomorphic encryption and watermarking. *IEEE Access*, *8*, 92098-92109.

[14] Aliady, W. A., & Al-Ahmadi, S. A. (2019). Energy preserving secure measure against wormhole attack in wireless sensor networks. *IEEE access*, *7*, 84132-84141.

[15] Kalivar, P., Jaballah, W. B., Conti, M., & Lal, C. (2020). LiDL: Localization with early detection of sybil and wormhole attacks in IoT Networks. *Computers & Security*, *94*, 101849.

[16] Ding, J., Zhang, H., Guo, Z., & Wu, Y. (2021). The DPC-based scheme for detecting selective forwarding in clustered wireless sensor networks. *IEEE Access*, *9*, 20954-20967.

[17] Safaldin, M., Otair, M., & Abualigah, L. (2021). Improved binary gray wolf optimizer and SVM for intrusion detection system in wireless sensor networks: M. Safaldin et al. *Journal of ambient intelligence and humanized computing*, *12*(2), 1559-1576.

[18] Jha, S. K., Gupta, A., & Panigrahi, N. (2021). Security threat analysis and countermeasures on consensus-based time synchronization algorithms for wireless sensor network. *SN Computer Science*, *2*(5), 409.

[19] Arshad, A., Hanapi, Z. M., Subramaniam, S., & Latip, R. (2021). A survey of Sybil attack countermeasures in IoT-based wireless sensor networks. *PeerJ Computer Science*, *7*, e673.

[20] Paiila, P. B., Julie, E. G., & Robinson, Y. H. (2022). FBDR-Fuzzy based DDoS attack Detection and Recovery mechanism for wireless sensor networks. *Wireless Personal Communications*, *122*(4), 3053-3083.

[21] Bendale, S. P., & Prasad, J. R. (2018, November). Security threats and challenges in future mobile wireless networks. In *2018 IEEE global conference on wireless computing and networking (GCWCN)* (pp. 146-150). IEEE.

[22] Wang, C., Wang, J., Shen, Y., & Liu, X. (2018). An accurate Sybil attack detection based on fine-grained physical channel information. *Sensors*, *18*(3), 878. https://doi.org/10.3390/s18030878

[23] Osanaiye, O., Alfa, A. S., & Hancke, G. P. (2018). A statistical approach to detect jamming attacks in wireless sensor networks. *Sensors*, *18*(6), 1691. https://doi.org/10.3390/s18061691

[24] Yang, G., Dai, L., & Wei, Z. (2018). Challenges, threats, security issues and new trends of underwater wireless sensor networks. *Sensors*, *18*(11), 3907. https://doi.org/10.3390/s18113907

[25] Adil, M., Almaiah, M. A., Omar Alsayed, A., & Almomani, O. (2020). An anonymous channel categorization scheme of edge nodes to detect jamming attacks in wireless sensor networks. *Sensors*, *20*(8), 2311. https://doi.org/10.3390/s20082311

[26] Fattah, S., Gani, A., Ahmedy, I., Idris, M. Y. I., & Hashem, I. A. T. (2020). A survey on underwater wireless sensor networks: Requirements, taxonomy, recent advances, and open research challenges. *Sensors*, *20*(18), 5393. https://doi.org/10.3390/s20185393

[27] Shafiei, H., Khonsari, A., Derakhshi, H., & Mousavi, P. (2014). Detection and mitigation of sinkhole attacks in wireless sensor networks. *Journal of computer and system sciences*, *80*(3), 644-653.

[28] Huan, X., Kim, K. S., & Zhang, J. (2021). NISA: Node identification and spoofing attack detection based on clock features and radio information for wireless sensor networks. *IEEE Transactions on Communications*, *69*(7), 4691–4703. https://doi.org/10.1109/TCOMM.2021.3071448

[29] Yuan, Y., Huo, L., Wang, Z., & Hogrefe, D. (2018). Secure APIT localization scheme against Sybil attacks in distributed wireless sensor networks. *IEEE Access*, *6*, 27629–27636. https://doi.org/10.1109/ACCESS.2018.2835527

[30] Ahutu, O. R., & El-Ocla, H. (2020). Centralized routing protocol for detecting wormhole attacks in wireless sensor networks. *IEEE Access*, *8*, 63270–63282. https://doi.org/10.1109/ACCESS.2020.2983438

[31] Numan, M., Subhan, F., Khan, W. Z., Hakak, S., Haider, S., Reddy, G. T., Jolfaei, A., & Alazab, M. (2020). A systematic review on clone node detection in static wireless sensor networks. *IEEE Access, 8*, 65450–65461. https://doi.org/10.1109/ACCESS.2020.2983091

[32] Liu, G., Peng, B., Zhong, X., & Lan, X. (2020). Differential games of rechargeable wireless sensor networks against malicious programs based on SILRD propagation model. *Complexity, 2020*, Article 5686413. https://doi.org/10.1155/2020/5686413

[33] Xu, Y., & Liu, F. (2017, December). Hybrid key management scheme for preventing man-in-middle attack in heterogeneous sensor networks. In *2017 3rd IEEE International Conference on Computer and Communications (ICCC)* (pp. 1421-1425). IEEE.

[34] Bhatt, R., Maheshwary, P., Shukla, P., Shukla, P., Shrivastava, M., & Changlani, S. (2020). Implementation of fruit fly optimization algorithm (FFOA) to escalate the attacking efficiency of node capture attack in wireless sensor networks (WSN). *Computer Communications, 149*, 134–145. https://doi.org/10.1016/j.comcom.2019.09.007

[35] Liu, G., Peng, B., Zhong, X., & Li, Z. (2020). Attack-defense game between malicious programs and energy-harvesting wireless sensor networks based on epidemic modeling. *Complexity, 2020*, Article 3680518. https://doi.org/10.1155/2020/3680518

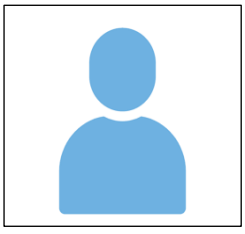
[36] Altulaihan, E., Almaiah, M. A., & Aljughaiman, A. (2024). Anomaly detection IDS for detecting DoS attacks in IoT networks based on machine learning algorithms. *Sensors, 24*(2), 713. https://doi.org/10.3390/s24020713

[37] Modares, H., Salleh, R., & Moravejoshargeh, A. (2011, September). Overview of security issues in wireless sensor networks. In *2011 third international conference on computational intelligence, modelling & simulation* (pp. 308-311). IEEE.

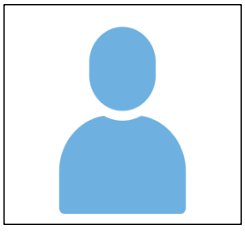
[38] Periyanayagi, S., & Sumathy, V. (2018). Swarm-based defense technique for tampering and cheating attack in WSN using CPHS. *Personal and Ubiquitous Computing, 22*, 1165–1179. https://doi.org/10.1007/s00779-018-1162-1

[39] Huang, D.-W., Liu, W., & Bi, J. (2021). Data tampering attacks diagnosis in dynamic wireless sensor networks. *Computer Communications, 172*, 84–92. https://doi.org/10.1016/j.comcom.2021.03.007

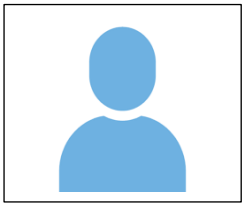
[40] Ali, A., Almaiah, M. A., Hajjej, F., Pasha, M. F., Fang, O. H., Khan, R., Teo, J., & Zakarya, M. (2022). An industrial IoT-based blockchain-enabled secure searchable encryption approach for healthcare systems using neural network. *Sensors, 22*(2), 572. https://doi.org/10.3390/s22020572



Haitham Albinhamad Department of Computer Networks and Communications, King Faisal University, Al-Ahsa 31982, Saudi Arabia. He has published over 115 research papers in highly reputed journals such as the Engineering and Science Technology, an International Journal, Education and Information Technologies, IEEE Access and others. Most of his publications were indexed under the ISI Web of Science and Scopus. His current research interests include Cybersecurity, Cybersecurity-Risk Assessment and Blockchain.



Abdullah Alotibi Department of Computer Networks and Communications, King Faisal University, Al-Ahsa 31982, Saudi Arabia. He has published over 115 research papers in highly reputed journals such as the Engineering and Science Technology, an International Journal, Education and Information Technologies, IEEE Access and others. Most of his publications were indexed under the ISI Web of Science and Scopus. His current research interests include Cybersecurity, Cybersecurity-Risk Assessment and Blockchain.



Ali Alagnam Department of Computer Networks and Communications, King Faisal University, Al-Ahsa 31982, Saudi Arabia. He has published over 115 research papers in highly reputed journals such as the Engineering and Science Technology, an International Journal, Education and Information Technologies, IEEE Access and others. Most of his publications were indexed under the ISI Web of Science and Scopus. His current research interests include Cybersecurity, Cybersecurity-Risk Assessment and Blockchain.

Dr. Mohammed Almaiah is an Associate Professor in the Department of Computer Science at University of Jordan. Almaiah is among the top 2% scientists in the world from 2020 up to now. He is working as Editor in Chief for the International Journal of Cybersecurity and Risk Assessment. He has published over 115 research papers in highly reputed journals such as the Engineering and Science Technology, an International Journal, Education and Information Technologies, IEEE Access and others. Most of his publications were indexed under the ISI Web of Science and Scopus. His current research interests include Cybersecurity, Cybersecurity-Risk Assessment and Blockchain.

Dr. Said Salloum is a highly qualified professional with a strong educational background and extensive experience in computer science. He earned his PhD in Computer Science from the University of Salford, UK. Currently, he serves as an Assistant Professor in the School of Computing at Skyline University

College. Previously, he worked as a Senior Enterprise Architect at the University of Sharjah's Computer Centre, where he led the strategic design and implementation of advanced technology solutions to support teaching, research, and administrative functions.