Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 45 No. 2 (2024)

Enhanced 5G Networks Application for Accessing Ontology Based RPL Traffic Mutation Network Environment

Mrs. Sharmila G.[1], Ajay kumar I. [2], Keerthivasan B.[3], Pradeep T.[4]

[1,2,3,4]*Department of Computer Science and Engineering*

[1,2,3,4]*Manakula Vinayagar Institute of Technology, Puducherry, India.*

***Abstract*:**

An ontological structure Using a variety of resources and embedded devices for wireless communication, 5G networks aim to enable ontology-based communication across wide networks. For 5G-based networks to link and maximize their efficiency, thousands of low-cost, low-power devices embedded gadgets are required. Computational testing of the RPL routing protocol's effectiveness in a highly dynamic automobile context forms the basis of the full assessment. The implication of this discovery is that even in huge mobility-based VANETs, the proposed CAGQ technology outperformed earlier methods and offered adequate transmission execution. Thousands of cheap, low-power embedded devices need to be quietly and efficiently connected to one another in order for 5G to be effective. For wireless networks (WSNs), evaluating a node's trust has a positive impact on the security of an object's communication with that node in a trust-based cluster-head selecting process.

Keywords—CAGQ,RPL,WSN,Trafficfuzzer

1.Introduction

An LTE network is made up of radio frequencies that may be constantly planned and tailored to make use of the best local wireless channels. This kind of radio automatically searches the wireless spectrum for available channels and modifies its broadcast or reception settings to support several wireless connections at once. Among these criteria are "waveform, protocol, operating frequency, and networking". This functions autonomously inside the communications environment,
exchanging environmental data with other radios (CRs) and the networks to which it is connected. A continuous recorder (CR) "reads the radio's outputs it" and "continuously monitors itself."at a specific frequency range at one location. This process is one kind of dynamic spectrum management. In response to operator commands, the engine can set radio-system parameters.

Joseph Mitola III first introduced the idea of radio in a 1998 language at Stockholm's KTH, a Royal Institute of Technology. Then, in 1999, Mitola and Gerald Q. Maguire, Jr. released their study. Later on, Mitola described this cutting-edge radio transmission technique. Radio is believed to be the ultimate goal of the development of software-defined radio platforms: a fully reconfigurable wireless transceiver that can instantly alter its transmission settings.

2.Related Work

Beyond merely growing, the fifth generation of mobile broadband allows for larger machine-type interactions, ultra-reliable and very low-latency connections, and more mobile bandwidth [1]. It relies on a hazy, changing, and heterogeneous environment that requires a lot of precautionary measures and testing work to be done. By developing and injecting network situations into a target, which may be a 5G primary service (such as AMF or SMF) or a Regional network (like gNodeB), this makes it possible to evaluate 5G components by replaying and altering 5G technology network traffic. The accompanying programme offers very flexible offline and online

network packet manipulation in both the data and control planes.A single processor core can replay 5G communications at up to 9.56 Gbps, according to an experimental evaluation the tool conducted against open-source 5G equipment.. Altered traffic also gets accepted by the target servicesMany new testing objectives and obstacles will emerge when 5G mobile networks transition to a service-based architecture (SBA). First, the deployment of network functional virtualization (NFV) and software-defined networking (SDN) makes feasible a new set of technologies that come with 5G, including network slicing (NS), mobile computing at the edge (MEC), and virtualisation of network functions (NFV).These need to be analysed from both functional and non-functional perspectives in order to assess the system's sanity using metrics like data throughput performance, latencyscalability, strength.

An[6] rising number of connected devices can be supported by Fifth Generation (5G) networks, which are designed to offer value-added services with improved performance, including high dependability, low latency, high data rates, and capacity. A shared infrastructure that spans several sites and domains and is regulated by various business stakeholders allows for the automated and flexible provisioning and management of resources and services, which is what makes 5G networks possible. This creates new risks and vulnerabilities that have not yet been thoroughly investigated and moves towards a complex 5G ecosystem made possible byNetwork Function Virtualization (NFV) andnumerous corporate partnerships. Deriving a 5G telecommunication business model powered by5G enabling technologies, we thus examine the intricacy of the 5G ecosystem in this survey. We employthis business strategyto determine.

We[7]examine the protocol format and discover an efficient security detection technique by studying the5G core network's NGAP protocol. In this study, we apply the Fuzzing approach to identify security vulnerabilities in the 5Gcorenetwork's NGAP protocol. A partition weight table-based selection mutation algorithm is suggested to increase the effectiveness of fuzzing. The NGAP protocol is tested in a 5G core network to identify any security flaws using our newly suggested algorithm and fuzzing technique. By counting the variationsamples and determining the increase in the probability of triggering anomalies inthe partition weight table, we can finallydemonstrate the effectiveness of the mutation algorithm selection process.

3.Proposed Work

In the proposed system,we suggest routing attacks in the RPL based 5G networks Becoming crucial in number of 5G applications.To address routing attacks,by applying several solutions in the security of the network formation.It is proposed using machine learning techniques,intrusion detection system.The algorithm used here is reinforcement learning.We rectify the security issues in the 5G network and devices is feasible by simple integration and resource constrained in the smart devices.Existing security solutions have minor drawbacks in the previous used RPL network protocol.The created node will be selected based on the neighbor node communication strength and each vehicle's formation may change the latency and distance between the two nodes.

The node creates call back to get demands at each location that is currently present at most to the neighbor node. The current node returns the demand of the network formation by adding capacity constraint structure. And the specified location gets the service time by the efficiency of security solutions like BEER ,EAR ,Q Routing etc. The travelling time between the vehicular communication between the two locations of the present nodes and acts global span constraint. The number of packets delivered during the communication of the RPL network protocol and energy consumption of each packet delivered over time is calculated by the reinforcement learning.

Optimized Link State Routing Protocol is referred to as OLSR. Every node regularly floods the status of its links in this way. Every node relays link state data that it has received from nearby nodes. Every node records the link state data that it receives from other nodes.Routing via Link State Every node has the ability to obtain the entire network topology and can expand a spanning tree.It makes use of MultiPoint Relaying, a method to lessen message flooding (MPR). This is when each network node N chooses a group of nearby nodes to act as multipoint relays, or MPR(N), retransmitting control packets from N- Control packets from N are processed by neighbors who are not in MPR(N), but they are not sent. MPR(N) is chosen so that (one-hop neighbors) of MPR(N) cover all two-hop neighbors of N.

4.Methodology

4.1 Reinforcement Learning

The study of how intelligent creatures should act in a certain environment to optimise the idea of cumulative reward is known as reinforcement learning (RL), a branch of machine learning. Reinforcement learning constitutes one of the three core paradigms of machine learning, along with supervised and autonomous learning. Unlike supervised learning ,reinforcement learning does not involve the presentation labelled of input/output pairs of suboptimal.

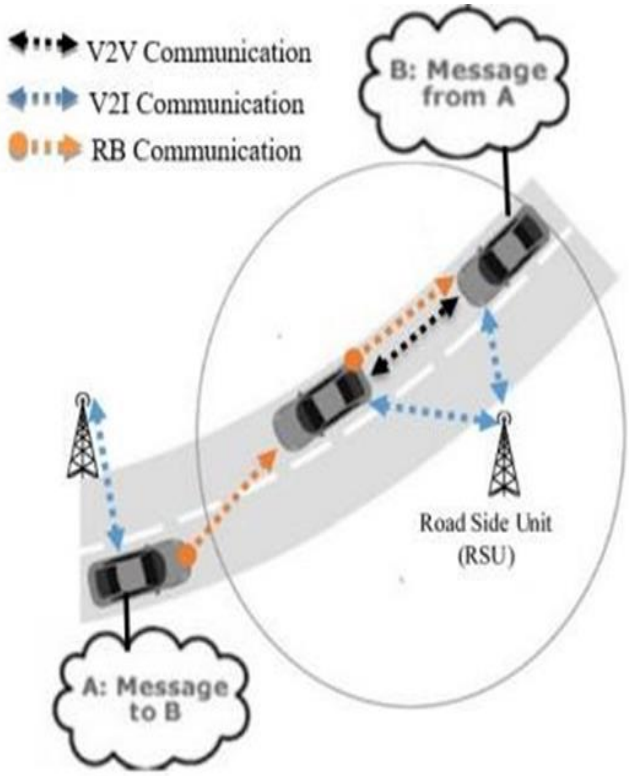

Fig 1Ad-hoc network

activities that need to be rectified directly. In the fig.1 Ad-hoc network shows the V2V communication between the two nodes A and B by sending messages.The Road Side Unit(RSU) makes the communication messages from A to B and vehicular communication travels by receiving acknowledgement from the network formation nodes..Exploration of unknown areas and utilisation of already-known information are instead balanced.As many reinforcement learning methods for this scenario employ dynamic programming approaches, the environment is typically described as a Markov decision procedure (MDP).[2]Primarily, reinforcement learning algorithms target large MDPs when exact methods become unfeasible and do not presuppose knowledge of an exact mathematical model of the MDP. This is how they vary from traditional dynamic programming techniques.

4.2 System Architecture

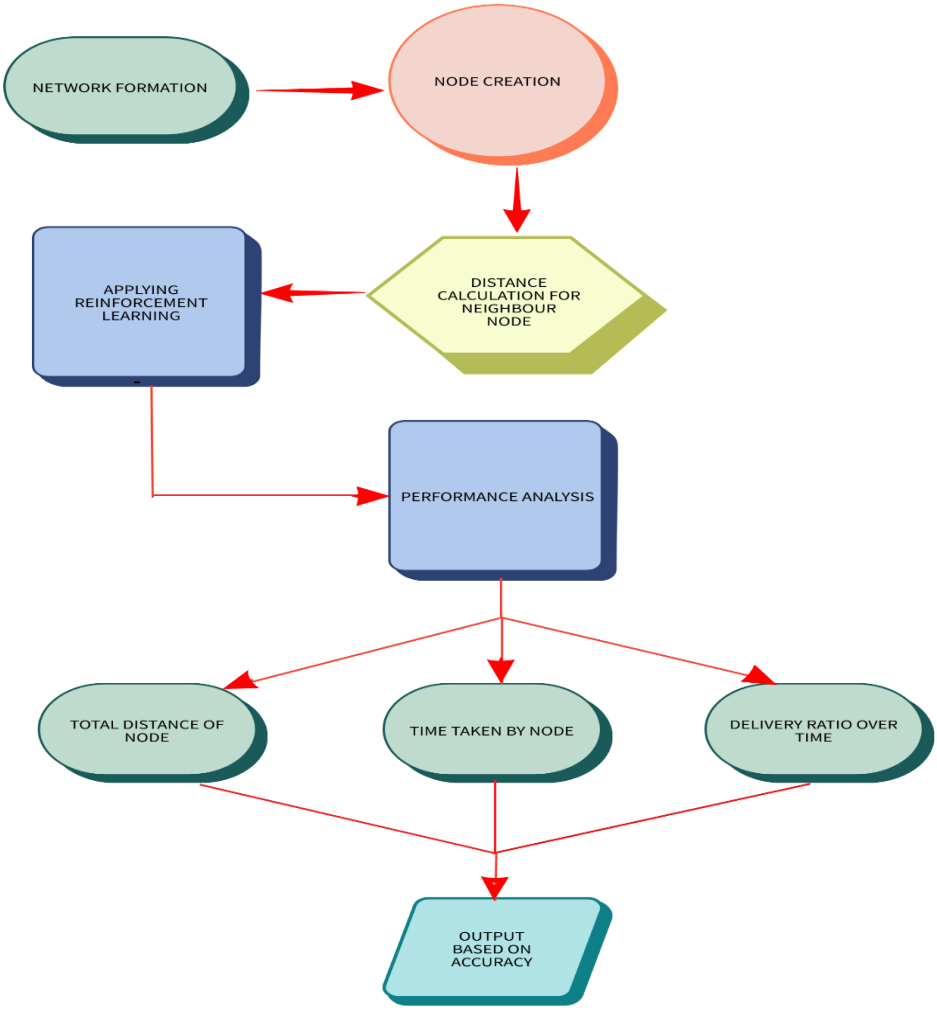

Fig2 RPL routing protocol for smart buildings

In the system architecture,the network formation is created using RPL network protocol.In this there are 50 nodes are taken into consideration to form a network framework.Node creation taken place from initial phase of the network to destination phase of the network.By taking Neighbor node into account to calculate the distance vector by using Eucliden formula.After calculating distance vector then the neighbor node distance will be generated.Applying Reinforcement algorithm,it makes the data routing technique to overcome the traffic mutation by RPL network.The shortest path between the nodes for the vehicular communication is calculated.Data transmission makes way easier for loading data for the communication of each vehicle's node based on the distance between the neighbor nodes.Finally, the performance metrics is performed by mainly focuses on distance vector,time taken by the node,delivery ratio over time.

4.3 DISTANCE

One of the primary variables used to find the shortest path is the cost or distance involved with a certain path. These must to be considered as crucial inputs in any algorithm that is created. Even though it goes with common sense, a shorter road could be more costly, so the correct decision needs to be made based on other factors that affect optimality.

4.4 LATENCY

The latency or delay noticed by a packet as it travels from its source to its destination can be increased through

optimal routing. When thinking about network routing, take into consideration the latency of cloud provider services in different global cities. In order to reduce delays caused by inefficient routes, network packets must have an ideal route. Remember that these network latencies could fluctuate over time and not always stay the same.

There are many distinct kinds of shortest path strategies: rule-based, model-based, dynamic, adaptive, deterministic, free of models, etc. Evaluation criteria for these strategies include complexity, calculating demands, time/delays, memory requirements, optimality, power consumption, and more. The majority of these techniques base their choices on a cost-latency trade-off.

5. Perfomance Analysis

5.1 NODECREATING

This module was created to create nodes and put over thirty nodes at specific distances from one another. middle area where the mobilitynode is located. Everynode is aware ofwhere it is with relation tothesink. Transmit packets must be received bythe access point, which must then acknowledge the transmitter.

5.2 ROUTINGOVERHEAD

The percentage of total data packets transported to destinations compared to the total number of control packet(which comprise RREQ, RREP, RERR, and Hello). Every hop counts as one transmission for the control packets sent over several hops. Because the neighbor list included in the RREQ packet bythe DPR and OLSR protocols is larger than that of the original AODV, we utilize the size of RREQ packets rather than the number ofRREQ packets in order to maintain fairness. Researchers studying vehicle wireless networking have discovered that message broad casting presents a tempting alternative due in part to its inexpensive cost and in part to its ability to handle huge numbers of data packets.

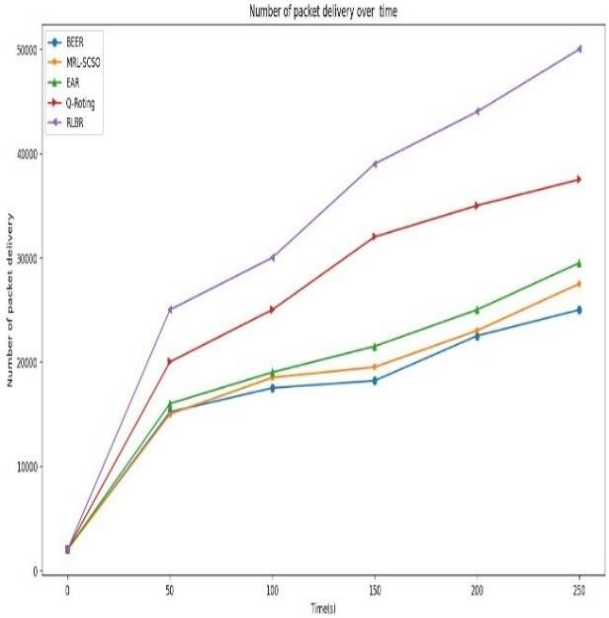

Fig3 No. of packet delivery over time

The Fig 3 graph explains number of packet delivery in the y axis and time taken by the network communication in the x axis.It defines the network packet delivery ratio over time to overcome the loss of packet delivery during vehicular communication

5.3DATAROUTING

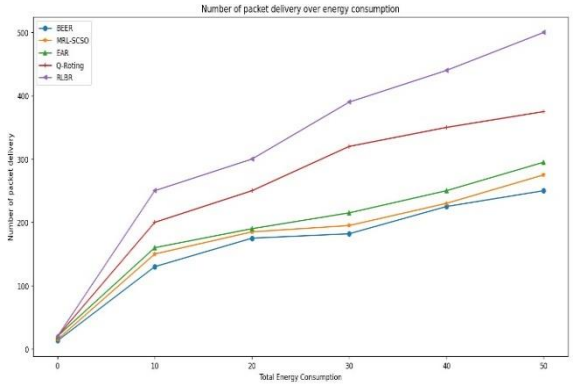

Fig 4 No. of packet delivery over energy consumption

To fig 4 transport packets to their destination, the source node routes them via a more reliable node. The graphicalresultsareused toanalyzetheperformance. Thefollowing isalist of attacks that werepart ofthis phase.

The above graph describes the number of packet delivery in the y axis and energy consumption in the x axis .It calculates the number of packet delivery over energy consumption by comparing the other network protocols with RLBR routing protocol.

5.4 PASSIVEATTACK:

Here,an attacker gainsaccesstoanetwork'saggregator node, compromisesit, examinesit,listens,and gets important data from it in an attempt to determine which nodes—such as base stations or sink nodes—have greater significance in the topology. The newly compromised node might be utilized by the attacker to launch other malicious assaults.

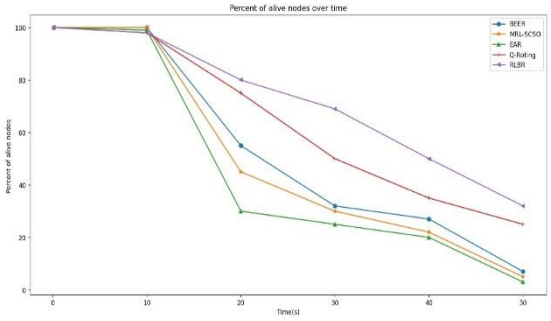

Fig 5 Percent of alive nodes over time

WSNs Fig 5 should be able to shield communications from unwanted access in order to safeguard nodes (confidentiality).

this graph calculates the number of present alive nodes over time during the vehicular communication per second. RLBR improves alive nodes in the network than other compared network protocols.

6. Results And Discussion

ForroadsidesensordatacollectionbyautomobilesinVANET-WSNfordrivingsafety,theroutingprotocolis the main focus of the research.The NetworkProtocol for Less Power and Lossy Networks (RPL), which is tree-based,takescareofourroutingneedswithease.Unfortunately,RPLneedstobeupdatedtocopewiththe verydynamicarchitectureofVANET-WSNbecauseitwasdesignedforstaticwirelesssensornetworks.For thefirsttime,wequantifyRPL(GI-RPL)usingGeographicalInformation(GI),whichenablesRPLtohappen rapidly. Wealsooffer severaltechniquestotuneRPLin VANET-WSN.Todemonstratetheperformanceof GI-

RPL,webuiltasimulationusingCoojaandcomparedtheoutcomeswithanothermodifiedRPL.

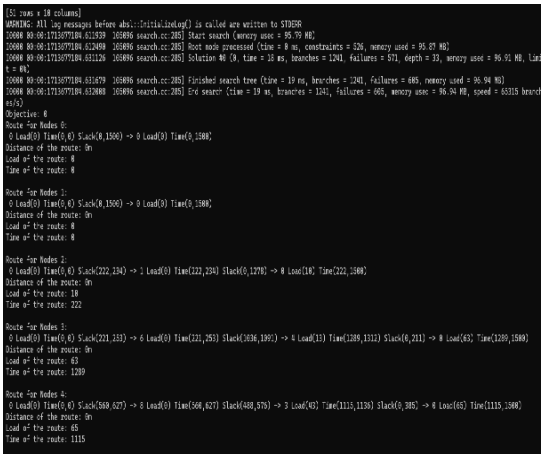

Fig 6 Execution

The Fig 6resultsofthesimulationshowthatGI-Lhasashortdelay,afairoverhead,andahighpackagedelivery ratio.OurFutureisoperational,Trafficdataisanalysedforreliability(datatrust)utilisinginformationsensed and gathered from various cars.

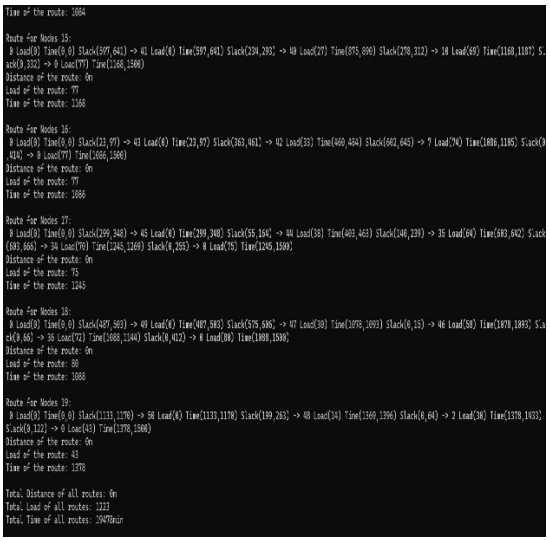

Fig 7 Execution

The Fig 7 trustworthiness of vehicle nodes is assessed in two ways.Put differently, a vector made up of two elements represents the level of reliability that is given to each node. The two aspects of node trust are functional trust and suggestion trust, which gauge a node's probabilityofperformingitsfunctionalityandthevalidityofitssuggestionstoothernodes,respectively.The node routes through the initial node from the previous node to calculate the distance between the vehicular nodes and the lifetime of the node calculated efficiently.The RLBR shows improvement compared to other network protocols.TheresultsofthesimulationshowthatGI-RPLhasashortdelay,afairoverhead,andahighpackagedelivery ratio.OurFutureisoperational,Trafficdataisanalysedforreliability(datatrust)utilisinginformationsensed and gathered from various cars.

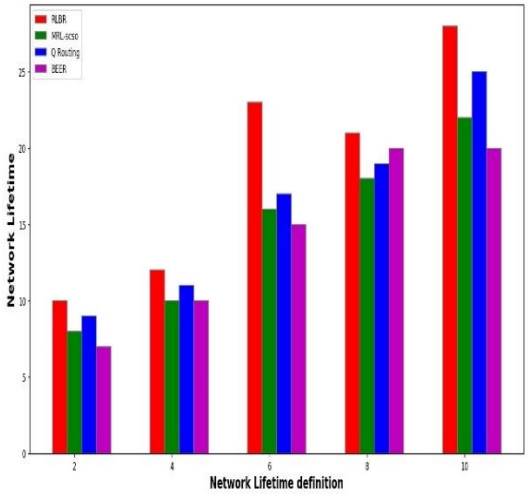

Fig 8 Network lifetime

In this Fig 8 graph, it compares the values between the network protocols to show off the network lifetime definition.RLBR shows efficiency in network lifetime compared to other network protocols.

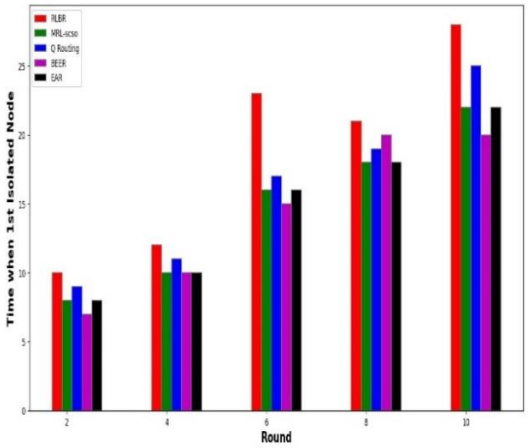

Fig 9 Time when 1st isolated node

this Fig 9 graph calculates the time when the node is isolated per round(indicates communication between the vehicles)

7.Conclusion

The routing system for roadside sensor data collecting by automobiles in VANET-WSN for driving safety is the main focus of the research. The tree-based RPL easily satisfies our routing requirements.But RPL was designed for static wireless sensor networks; therefore, it needs to be adjusted to function with the highly dynamic architecture of VANET-WSN. For the first time, we use Geographical Information (GI) as the RPL measure (GI-RPL), allowing RPL take place rapidly. We additionally offer multiple ways to tune RPL in VANET-WSN. To demonstrate the performance of GI-RPL, we ran a simulation using Cooja and compared the outcomes with those of another modified RPL. The results of the simulation show that GI-RPL has a short delay, a fair overhead, and a high package delivery ratio. Our Future Is Working: Information sensed and gathered from several vehicles is used to assess traffic data for reliability (data trust). The trustworthiness of vehicle nodes is assessed in two ways. Stated differently, a vector with two elements indicates the dependability level assigned to each node.The two aspects of node trust are functional trust and suggestion trust, which gauge a node's probability of executing its functionality and the validity of its recommendations to other nodes, respective.

References:

[1] IEEE Standard for Information Technology Telecommunications and Information Exchange Between Systems Local and Metropolitan Area Networks Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Wireless Access in Vehicular Environments, IEEE Standard 802.11, Nov. 2022.

[2] E.C.Eze, S.-J.Zhang,E.-J.Liu,andJ.C.Eze,``Advancesinvehicularad-hocnetworks(VANETs): Challenges android-map for future development," Int. J. Auto. Comput., vol. 13, no. 1, pp. 1_18, 2022.

[3] B. Mokhtar and M. Azab, ``Survey on security issues in vehicular ad hoc networks," Alexandria Eng. J., vol. 54, no. 4, pp. 1115_1126, 2015, doi: 10.1016/j.aej.2015.07.011.

[4] K. Govindan andP. Mohapatra, ``Trust computationsandtrust dynamics inmobile adhocnetworks: A survey," IEEE Commun. Surveys Tuts., vol. 14, no. 2, pp. 279_298, 2nd Quart., 2022, doi: 10.1109/SURV. 2011.042711.00083.

[5] Z. Yan, P. Zhang, and A. V. Vasilakos, ``A survey on trust management for Internet of Things," J. Netw. Comput. Appl., vol. 42, pp. 120_134, Jun. 2022.

[6] S. A. Soleymani et al., ``Trust management in vehicular ad hoc network: A systematic review," EURASIP J. WirelessCommun. Netw., vol. 2021, no. 1, p. 146, Dec. 2015.

[7] N. Karthik and V. S. Ananthanarayana, ``A hybrid trust management scheme for wireless sensor networks," Wireless Pers. Commun., vol. 97, no. 4, pp. 5137_5170, Dec. 2019.

[8] S. Goli-Bidgoli and N. Movahhedinia, ``Determining vehicles' radio transmission range for increasing cognitive radio VANET (CR-VANET) reliability using a trust management system," Comput. Netw., vol. 127, pp. 340_351, Nov. 2017.

[9] P. Agarwal and N. Bhardwaj, ``A review on trust model in vehicular ad hoc network," Int. J. Grid Distrib. Comput., vol. 9, no. 4, pp. 325_334, 2016.

[10] . U. Khan, S. Agrawal, and S. Silakari, ``Detection of malicious nodes (DMN) in vehicular ad-hoc networks," Proc. Comput. Sci., vol. 46, pp. 965_972, Jan. 2015