iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 9 **Issue:** VII **Month of publication:** July 2021

DOI: https://doi.org/10.22214/ijraset.2021.36785

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue VII July 2021- Available at www.ijraset.com

Random Mobility based Network to Handle Attacks in Vehicular System

Pooja[1], Yashika Sharma[2]
[1]*M.Tech Scholar,* [2]*Asst Professor, Doon Valley Institute of Engg & Technology, Karnal*

Abstract: ***This paper focuses on improved mobility based routing to handle attacks in VANET. It provides study of reconfiguration concept in vehicular system. All vehicles are moving with random speed and controlled by neuro fuzzy system. It provides improvement in mobility based routing to improve performance in VANET. Due to this, it focuses on improved mobility based routing that helps to prevent attacks in system. The proposed system is compared with actual system in terms of performance parameters. All simulations are be presented in MATLAB tool.***
Keywords: VANET, Reconfiguration system, Packet Delivery Ratio, Energy Management etc.

I. INTRODUCTION

VANETs are communication networks, where communication between vehicles takes place wirelessly, and vehicles act as nodes in the network. VANETs turn all participating vehicles into a wireless router to connect and create a network. The primary goal is to increase road safety [1]. In VANETs without central base station vehicles can talk with neighbouring vehicles. The thought of this straight conversation of information to direct protection messages to one-to-one or one-to-many vehicles through the wireless link. These messages are generally small in the segment and have a very little life to reach a target. The architecture of VANET is shown in Fig 1.1 below.

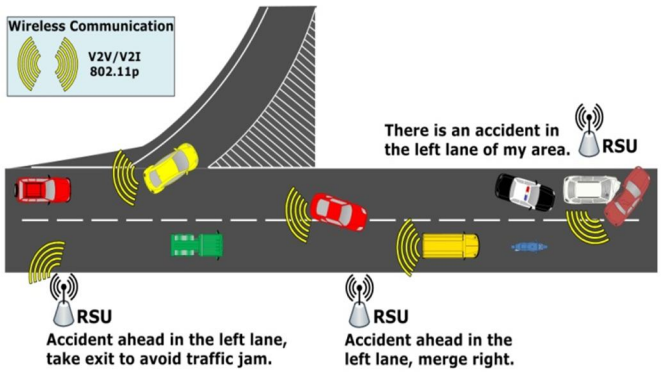


Fig 1: Vehicular Ad-hoc Network with WSN [1]

In the market of quick move of PCs the preparing power are improved out of the blue anyway the worth and size of PCs have extraordinarily diminished which motivates the use of PCs significantly. The most recent innovations have made colossal advancement in PCs design period and furthermore upgrade the use of individual and expert PCs frameworks in our every day exercises. As of late, financially, the individual work stations having sensors implanted in them and selected very well on account of costs-cutting and decrease in size of PCs. Vehicular Adhoc Networks have been getting a lot of consideration as of late because of their significant immaterialness to improve our lives. They help us by stretching out our capacity to precisely screen, study, and control items and situations of different scales and conditions, for example, wellbeing, business, comfort and beneficial arranged. Enormous no. of vehicles in a field is associated with a sink hub to transmit data about the occasions.

In remote correspondence and inserted smaller scale detecting advances, the headways support the utilization of WSNs today in numerous conditions to recognize and checking delicate data. Such conditions incorporate outskirt insurance, hazardous situations, wellbeing related territories, and savvy house control and some more. VANETs are here to recognize and follow the tanks on a war zone, following the faculty in a structure, measure the traffic rate on a street, screen ecological poisons, identify fire and downpour, distinguish an assault or mishap at any area. Vehicular sensors add to data creation about the geological area.

Presently, regardless of whether the VANETs are beginning to turn into a reality in this world, yet there are a few impediments, for example, change in topology arbitrarily, limitations in control, restricted computational assets like power, blunder inclined medium, vitality effectiveness, assaults recognition and aversion, vehicle-to-web or web to-vehicle. Assault identification and aversion is a significant issue of the VANET which requests specialist's abilities to get a path in diminishing the assaults before occurring by vehicles itself. VANETs comprises no. of vehicles sensor hubs scattered all through in a specific topographical zone to screen the earth of the region.

The remainder of the paper's association is as per the following; Section II examines the role of sensor nodes in VANET etc. Section III provides the major study provided by different authors. Section IV presents the major gaps identified during this study. Section V presents the conclusion and its future scope.

.

II. CHARACTERISTICS OF VANET

VANETs can be portrayed based on their workplace, highlights, stockpiling, battery and so on some of which may harmonize with Mobile Adhoc Networks (MANETs). Various distinctive contending frameworks plans must be considered and considered for Vehicular systems. To guarantee their prosperity, ordinary VANETs utilize the WAVE (Wireless Access for Vehicular Environment), that is a novel methodology for committed correspondence between vehicle-to-vehicle (V2V) and vehicle-to-roadside (V2R) with high unwavering quality). Fig 1.3 is the case of vehicular system in which all vehicles are communicating with each other.

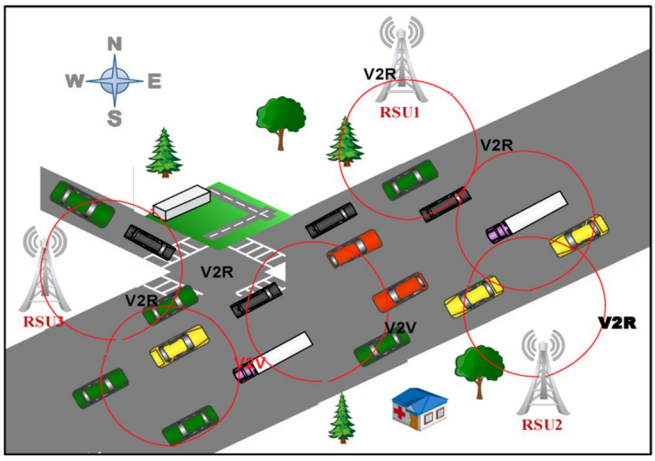


Fig 2: VANETs Communication [3]

1) *Highly Dynamic Topology:* The decision to move into any course makes the VANET a profoundly powerful topology and furthermore proposes that the system region isn't limit restricted.
2) *Frequent Disconnected Network:* Highly powerful nature of VANETs additionally causes the rapid vehicular sensor hubs to detach structure the system. Also, requires the rehashed prerequisite of absence of roadside sensor unit to execute according to the structure necessities.
3) *Mobility Modelling and Prediction:* Predicting the vehicle development and ebb and flow position is a test for the scientists for certain occasions yet VANETs are outfitted with sensor gadgets that give the careful and exact area. Specialists likewise consider the speed of the vehicle to anticipate the required with the goal that a productive model can be manufactured.
4) *Communication Environment:* Providing correspondence between vehicle-to-vehicle and vehicle-to-roadside are started with the assistance of directing calculations.
5) *Hard Delay Constraints:* Reducing the message postpone time is exceptionally basic part of VANET correspondence, normally at the time crisis. This isn't adequate to convey the message with rapid information rates yet with higher unwavering quality and higher exactness rate is likewise significant.
6) *Interaction with Onboard Sensors Nodes:* Sensor hubs are required to shape the system among vehicles and roadside remote sensors. They are the method of correspondences between them. Sensors hubs are answerable for perusing the information identified with vehicle speed, heading. In this way, these sensors hubs are utilized for interface arrangement or way development, and in directing conventions.

III. PROPOSED WORK

In the recent years, there have been growing interest and research efforts in the area of vehicular ad hoc network, because it offers enhanced safety and enriched travel comfort. Safety is one of the major goals in VANETs, since it enhances safety, reduce accidents and improve traffic conditions. This literature survey represents advancement in research that aims to strengthen security. In this survey proposal, security issues in VANETs have been presented. Security requirements are the main concern in VANETs and these requirements should be taken into consideration to enable the implementation of secure VANETs infrastructure for the efficient communication between parties. In VANETs, there are a number of security issues and for these security issues there should be well known security standard protocols and different kind of security techniques. Among multiple types of attacks, the main aim of the present study will be Sybil attack, which is a well known attack.

During their examination they found that QoS can be corrupted while attack occurred on any vehicle. However, every vehicle detected the information and transmitted it to neighbor node. This will build the handling power and decreases the transmission capacity. Another issue in the current framework is sharing information with no security. The main idea of the Sybil Attack is that two vehicles rarely pass through a few different RSUs far apart from each other at the same time. The RSU issues digital timestamps to each vehicle that passes through it. A traffic message is sent out by any vehicle, containing several time stamps corresponding to the previously passed RSUs. Therefore, if multiple traffic messages consist of a very similar series of timestamps, they might be suspected as Sybil messages originated from a single-vehicle. This approach is economic, since it does not use computational expensive public key infrastructure.

In existing work, a merged technique to prevent multiple Attacks in VANETs is presented. A two phase security based mechanism is proposed to give reliable solution in identifying and blocking the Sybil attacked nodes to secure the information. Existing framework proposes a procedure to convey the message from vehicle-to-vehicle easily of transmission rate. To accomplish this current framework missed the malignant hubs and other significant factor that may make the lethal mistake entire framework without actualizing the current framework.

Existing framework is constrained to assault identification on a VANET. During the information transmission between vehicles or VANET, existing framework missed to confirming the legitimacy of sensor hubs and another they are not scrambling the information before sending it to another sensor or sink hub. At the point when sensor hub detected information in a remote sensor arrange, there are exceptionally high odds of getting same information from crossed-areas that may prompt plentiful information and information oddity. To conquer the current framework downside, we proposed a framework that uses the three calculations to avoid the assault by confirming the VANET hubs soon after arrangement in the VANETs. To decrease the information preparing by proposing the information total system with encryption of detected information before transmitting to sink hub.

In this work, it proposes a novel secure vehicle-to-vehicle correspondence calculation utilizing neuro-fuzzy engineering. There are numerous defects in VANETs like security conveyance of information, unwavering quality, constrained battery control, ideal way arrangement, information conglomeration issue and some more. In this way, we are centred our examination around evacuating the security imperative by applying the encryption and utilizations the information collection strategies to dispose of the repetitive information parcels by melding the excess information bundles into one. This lessens the handling intensity of every hub and sets aside less effort to transmit the information bundles from youngster hub to the parent hub.

The proposed model will use the restriction strategy for the availability of the hubs inside the bunches in the way where they will expand the most minimal vitality and runs for the more drawn out periods expanding the both proficiency and lifetime of the VANETs. The proposed model will offer the controlled way arrangement procedures to shape the way between two precise graphic, which will assist us with forming the most limited and direct ways. The presentation of the proposed model will be estimated utilizing the parameters of transmission delay, vitality utilization, lifetime and system load.

The proposed model will be created utilizing the MATLAB with all fundamental info and yield parameters. The presentation of the proposed model will be altogether broke down subsequent to gathering the outcomes from the proposed model usage. The acquired outcomes would be contrasted with the current outcomes so as to appraise the presentation hole between the current and proposed plot. At that point the last end will be shaped based on the presentation assessment and correlation of the proposed plan.

A. Placement of Nodes

In above figure, the initial step depicts the sensors vehicles are being sent in a hazardous situation. Vehicle Nodes are arbitrarily spread over the zone. Every sensor vehicle has a sensor ID appeared alongside it. It will be utilized to address any sensor all through the procedure. Here we take huge number of sensors so that proposed plan will assess effectively. No two hubs cover one another.

B. Discover a Topology

In normal utilization situation, the hubs will be uniformly disseminated over an open air condition. This separation between adjoining hubs will be negligible yet the separation over the whole system will be noteworthy. They make an irregular topology at first.

C. Communication Between Head & NodeZ

For this, there is an immediate correspondence between head and hubs. Head gets some information about condition conditions, and afterward hubs answer back to head about status. For this, there is no loss of information on the grounds that there is immediate exchange of bundles from head and all hubs.

D. Sybil Attack

There is a provision of detection and prevention from Sybil attack in Network. if Attack occurred, it communicates to nearby vehicle nodes and also RSU. It helps to store the attacked location. Due to this, it chooses the another path by shortest path algorithm and helps to prevent from attack.

E. Fire Concern

Presently if temperature goes above edge because of any catastrophe impact, the hubs sense information and advises to the head and starts moving from their areas. At that point they gather to some other area and when the catastrophe levelled out then head arranges the hubs to repositioning or reconfigure their areas inside least time. This reconfiguration is finished without anyone else's input reconfigurable convention utilized. The hubs are moving to same areas after control of disaster.

F. Performance Parameters

1) *Packet Delivery Ratio*: It is defined as the ratio of no. of packets delivered successfully to destination by total number of packets transferred in system.
2) *End to End Delay*: It refers to the time which is to be taken for a data to be transferred from source to destination. It is combination of transmission delay and propagation delay.

IV. RESULTS & DISCUSSION

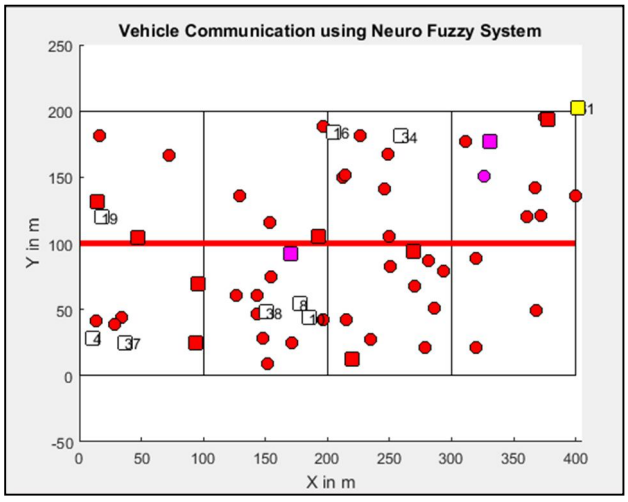


Figure 3: Existing VANET System using Neuro Fuzzy Method

This work provides the concept of mobility based vehicular networks that got affected by some multiple attacks like Sybil etc. Due to this, it may affect the performance of network. After this, it uses the concept of neuro fuzzy for system improvement. The results are shown below:

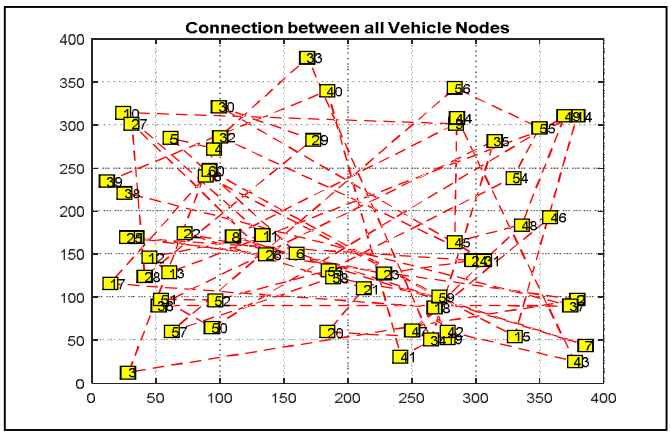


Figure 4: Connection Network between Vehicle Nodes

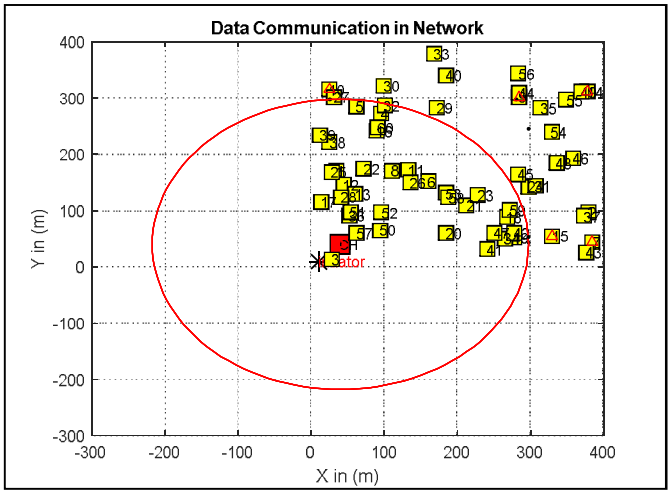


Figure 5: Message Transfer by Head to All Vehicle

Natural information assortment situation has a place with information. Sensor hubs conveyed in such applications are relied upon to work i(sense/gather/communicate) at normal premise and for longer timeframe. In such applications, information is gathered from enormous number of sent hubs for a while or year to discover the pattern and their conditions. The system structure of such application comprise of countless hubs, detecting and communicating information to the sink consistently.

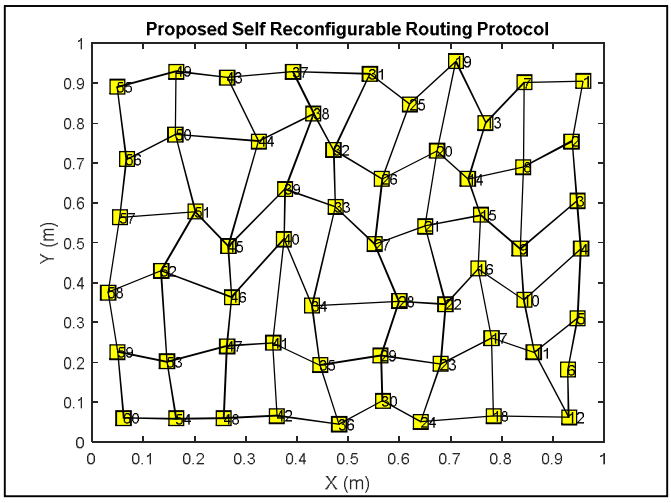


Figure 6: Self Reconfiguring Network Output

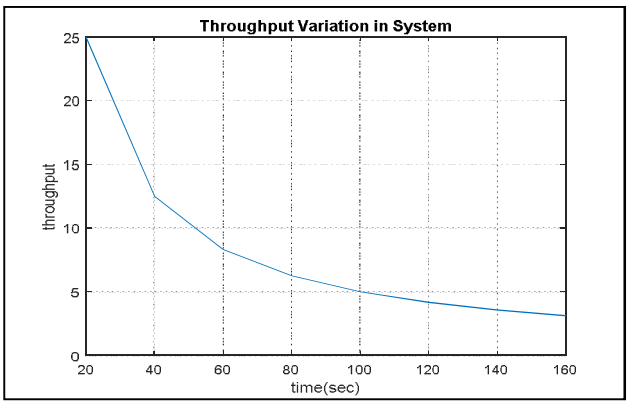


Figure 7: Throughput Variations in System

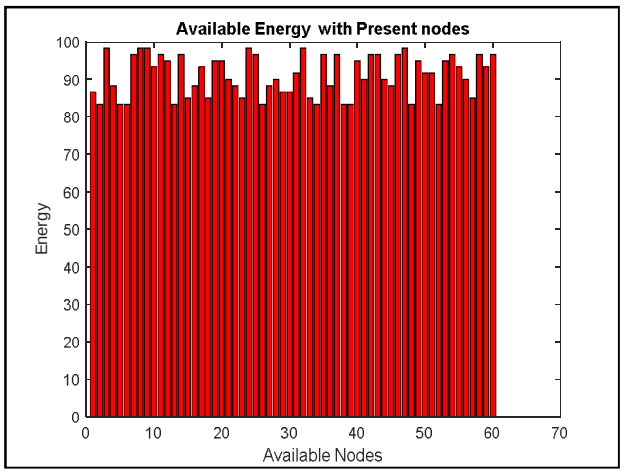


Figure 8: Available Energy in System

This work presents a methodology for dynamic reconfiguration of vehicle in vehicular systems and contrasts the exhibition of proposed framework and existing ANFIS framework. The system throughput is the primary boundary that is utilized to mirror the system ability. It is the measure of traffic that is leaving the "System". We measure these insights in bits every subsequent unit.

V. CONCLUSION

This postulation presents a methodology for dynamic reconfiguration of vehicle in vehicular systems and contrasts the exhibition of proposed framework and existing ANFIS framework. All situations of the dynamic reconfiguration foundation have been assessed. In this work, all vehicle are speaking with one another. A head is accommodated giving the directions to all vehicle. Reconfiguration is performed when the QoS qualities surpass a set limit. These edges might be distinctive for various application areas. The proposed framework gives better reaction as far as start to finish postponement and bundle misfortune rate when contrasted with existing work.

In future, it provides a concept to reduce error with improvement in technology in reconfiguration system.

REFERENCES

[1] Chaudhary, A., Tiwari, V. N., & Kumar, A. (2016). "A New Intrusion Detection System Based On Soft Computing Techniques Using Neuro-Fuzzy Classifier For Packet Dropping Attack In Manets", International Journal of Network Security, 18, 514-522.

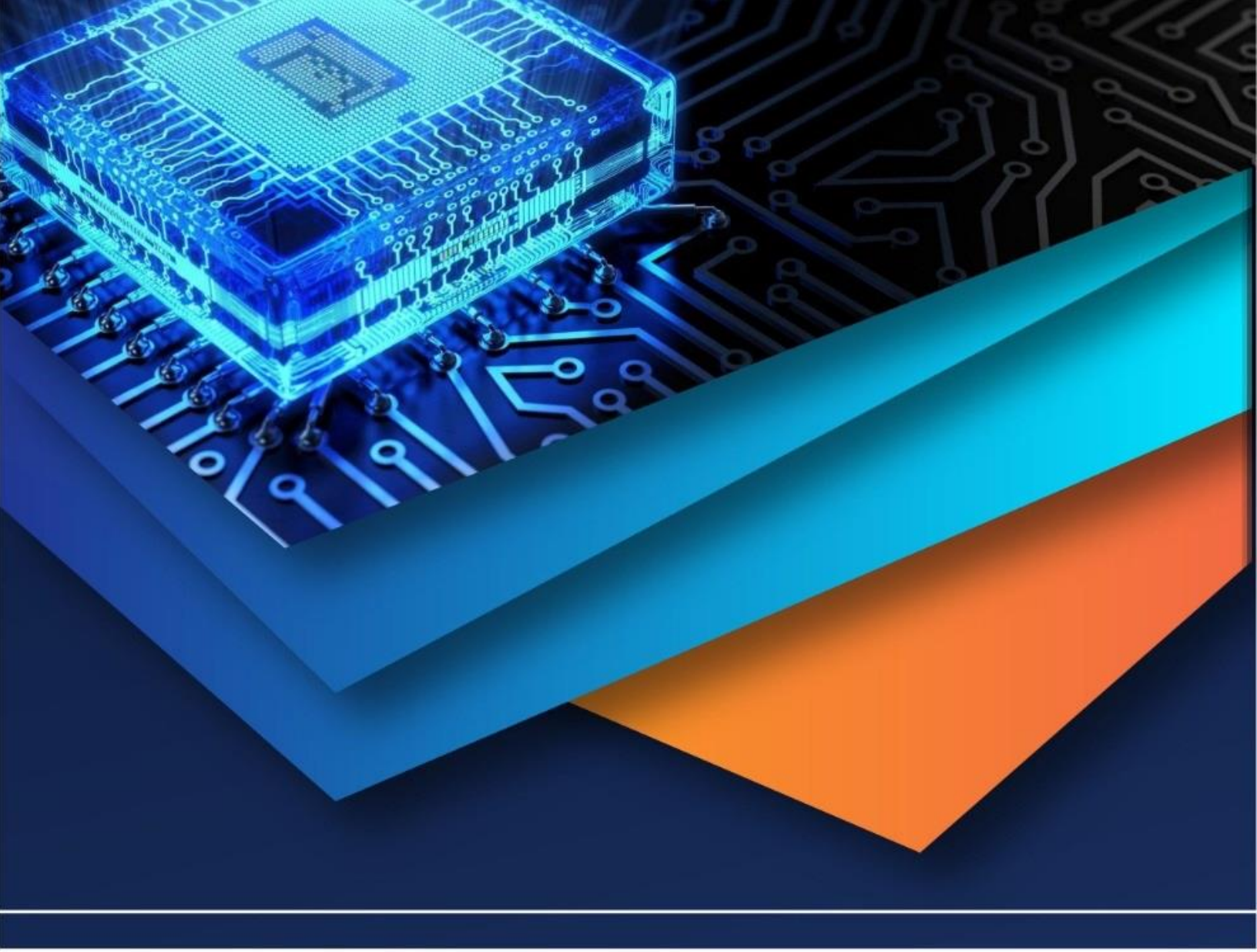
[2] Prathima, E. G., Venugopal, K. R., Iyengar, S. S., &Patnaik, L. M. (2017). "SDACQ: Secure Data Aggregation for Coexisting Queries in Wireless Sensor Networks", International Journal of Computer Science and Network Security (IJCSNS), 17(4), 205.

[3] Hasrouny, Hamssa, et al. "VANET Security Challenges And Solutions: A Survey." Vehicular Communications 7 (2017): 7-20.

[4] Tyagi, P., &Dembla, D. (2017). "Performance Analysis And Implementation Of Proposed Mechanism For Detection And Prevention of Security Attacks In Routing Protocols of Vehicular Ad-Hoc Network (VANET)", Egyptian informatics journal, 18(2), 133-139.

[5] Safi, Q. G. K., Luo, S., Wei, C., Pan, L., & Chen, Q. (2017). "PIaaS: Cloud-oriented secure and privacy-conscious parking information as a service using VANETs", Computer Networks, 124, 33-45.

[6] Pandey, P., Jain, M., &Pachouri, R. (2017). "DDos Attack On Wireless Sensor Network: A Review", International Journal of Advanced Research in Computer Science, 8(9).
[7] Abdel-Azim, M., Salah, H. E. D., & Ibrahim, M. (2017). "Black Hole attack Detection using fuzzy based IDS", International Journal of Communication Networks and Information Security, 9(2), 187.
[8] Poonia, D., & Sharma, M. K. , (2017) "Detection and Prevention of Denial of Services Attack based on Signal Strength and Reputation Mechanism", International Journal of Communication Networks and Information Security, 202-207.
[9] Mahdi Al Qahatani, M., & GM Mostafa, M. (2018). "Trust modeling in wireless sensor networks: state of the art", International Conference on Automation, Computational and Technology Management, pp. 191-197.
[10] Nayyar, S., Suman, A., & Kumar, P. (2018). "Adaptive neuro-fuzzy system based attack detection techniques for VANETs", International Journal of Computer Science Eng., 6(3), 57-64.
[11] Mittal, M., Saraswat, L. K., Iwendi, C., &Anajemba, J. H. (2019). "A Neuro-Fuzzy Approach for Intrusion Detection in Energy Efficient Sensor Routing", In 2019 4th International Conference on Internet of Things: Smart Innovation and Usages, pp. 1-5.
[12] Kaur, J., Singh, T., & Lakhwani, K. (2019). "An Enhanced Approach for Attack Detection in VANETs Using Adaptive Neuro-Fuzzy System", In International Conference on Automation, Computational and Technology Management, pp. 191-197.
[13] Syed S, Prasad B., (2019), " Merged technique to prevent SYBIL Attacks in VANETs", IEEE, pp. 01-06.
[14] Mao Ye, Lin Guan, (2020), " MPBRP- Mobility Prediction Based Routing Protocol in VANETs", IEEE, pp. 01-07.
.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY