JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

# A DYNAMIC SELF-RECONFIGURATION PROTOCOL FOR DISASTER MANAGEMENT USING VANET

**Priyankush Sharma, Dr. Sukhvinder Kaur**
M. Tech Scholar, Professor and HOD
Department of Electronics and Communication Engineering
Swami Devi Dayal Institute of Engineering &Technology, Barwala, Panchkula (Haryana)

**Abstract - Vehicular Adhoc Network is a self-organized network that consists of a large number of low-cost and low powered vehicular devices, called nodes, which can be deployed in harsh environment; sensor nodes are prone to have faults. It is thus desirable to detect and locate faulty sensor nodes to ensure the quality of service of sensor networks. In this thesis, it proposes mobility based dynamic reconfiguration system in VANET. In this, all nodes will be in dynamic nature and moves randomly. All nodes will be communicating with each other as well as from head nodes. There is a direct communication between head & nodes. With this great ability, the administrator can reconfigure remotely to adopt different applications and different network conditions. Reconfiguration is performed when the QoS attributes exceed a set threshold. The proposed mechanism is implemented with MATLAB.**

***Keywords:*** *VANET, Vehicle Routing, Dynamic Reconfiguration, MATLAB etc.*

## I. INTRODUCTION

Vehicular Ad-Hoc Networks (VANETs) are essentially sensor hubs that are conveyed to make correspondence between vehicle-to-vehicles or vehicle-to-sink hub conceivable utilizing impromptu remote gadgets. These days, these vehicular specially appointed systems turned into a rising and innovation in the field of VANETs. Because of the accessibility and assortment of impromptu system applications in Intelligent Transportation Systems (ITS) they investigate a wide scale to make it progressively dependable and VANET is a specially appointed system since sensor hubs are situated in a particular region independent of engineering and order and could be interface with the base station by following the directing calculation.

As we presumably already know, VANETs are used to gather information about locations where events are likely to occur. In order to accomplish this, VANETs make use of several sensor hubs that are used to scan an area for events and, after doing so, to inform the roadside assistance unit about the location of the event. When RAU receives the reports of the occasion, it will respond with a brief physical message.

In sense-reaction applications, sensor hubs with covering detecting zones are transported in the inclusion territory to block openings. As a result, many sensor hubs (neighbouring hubs) detect the same event simultaneously and send it to the RAU, resulting in excess. In such a situation, the RAU controls this repeat by only responding to people who are entering the system territory. In this way, RAU keeps a strategic distance from any fictitious positives, such as an event that has been reported but never occurred. Another solution would be for all neighboring sensor hubs to report to one basic hub, such as a head, which would then send a message to the base station (BS) informing it of the detection of an event and receive the data that each hub verifiably detected.

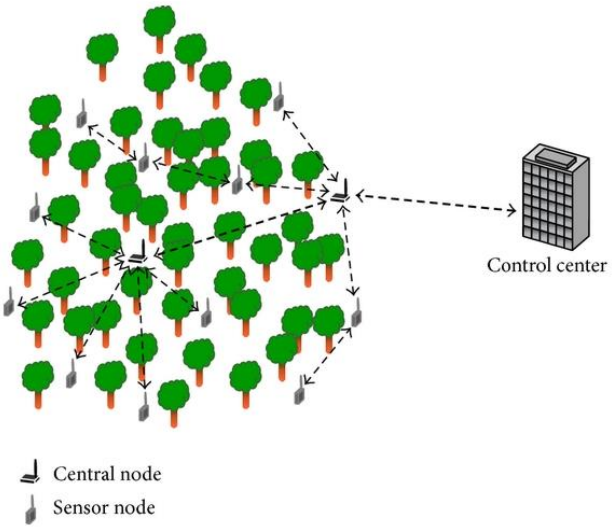


Fig 1: VANETs Communication [1]

### A. Attacks in Vanets

The VANET systems are helpless against a variety of security intrusions. These assaults have a significant impact on the system and also result in a high mortality toll. Here are some of the security attacks that can be launched against VANETs.

**1. Denial of Service Attack**

A Denial of Service (DoS) attack is launched to make a system that has been designated specifically unreachable. This could be achieved by flooding the sensor connection with unexpected and unwanted requests, which would keep the resources of the current system in use and prevent any

real requests from being sent. This is not prepared to access that particular asset, sensor hub, or message. Smashing all communication channels is another way to carry out this attack.

**2. Distributed Denial of Service**

This is another type of DoS or certainly a variation of a DoS attack in which multiple attackers attempt to send the RREP on the victim hub. Several sensor hubs are used to execute the attack, and numerous sensor hubs spread out in different locations gather a significant amount of resources. The main goal of a DDoS attack is to eliminate the hub's accessibility as a security requirement.

**3. Replay Attacks**

This kind of attack uses an intruder to replay previous communications sent to the sender and try to intercept the PC's admission. These types of attacks call for enormous resources that are available at the time of sending the message from numerous attacker centres.

**4. Sybil Attack**

This type of attack tries to duplicate sensor hubs that are created using dishonest and illegal characters, and when a sensor hub sends a message to another sensor hub using a different personality, it receives the correct information. Therefore, different sensor hubs have different perceptions of a similar sensor hub. The effectiveness of Sybil assault heavily depends on how naturally personalities are shaped, as well as whether the sensor network compares all sensor hubs equally or whether each one has a distinct finger print. A variety of strategies are available to counter this onslaught, one of which is the factual and likelihood approach.

**5. Alteration Attack**

This type of attack is launched when an intrusive modifies their information and tries to update it. The attackers' network will thereafter receive the updated information. Delaying the message that needs to be transmitted into and on the same sensor network is another way to carry out these types of assaults.

**6. Fabrication Attack**

In this type of attack, the attacker transmits made-up information to a sensor system to detect the entrance. There is a good chance that the transmitter is not who the data indicates and that the emitter is actually someone else.

**7. Black Hole Attack**

A black hole attack is carried out when a sensor hub abruptly denies being a part of the sensor network, which may result in the sensor hubs leaving the sensor network. Additionally, this attack sends all of the information to a sensor hub that doesn't exist at all in the sensor network, resulting in a considerable loss of data.

**8. Malwares**

In VANETs, malware can direct the machine to do unconscious tasks in addition to its routine work. This might occur if the product received an improper refresh and introduced an unfavourable code arrangement into the framework.

**9. Masquerading Attack**

The aggressor who has successfully shown an interest in the sensor network will use this attack. The attacker tries to gain in by pretending to be another vehicle hub and using a false persona. This could be done and used for masking through message generation, replay attacks, or adjustment assaults.

**10. Tunnelling Attack**

The intruder sets up a system between two remote, particularly appointed sensor systems using an extra channel between them in an effort to get access to the sensor network. This creates a passageway, which is referred to as. Two distant systems' sensor hubs have an idea of being neighbours and communicate through the route.

**11. ID Disclosure Attack**

This attack has the ability to obtain data and characters that can be misused from the sensor hub, and as a result, its precise location becomes entirely visible to the entire vehicular impromptu system. At this time, a stranger can send malware to any objective sensor hub and neighbours. These malicious programmes are naturally replicating their IDs, and they are now introducing themselves as the computer's neighbours. When the malware tries to approach the intrusive neighbour, it believes that the attacker has captured its character in the vicinity of the target sensor hub.

**12. Wormhole Attack**

This kind of assault uses two genuine sensor hubs that are out of range of one another and must communicate data through the opening. In a sensor organisation, the sensor hub is located in the transmission range of both real sensor hubs. The genuine hubs may have the entrance to the burrow and convey through the intruder sensor hub inside the channel.

This work is introduced as pursues. In Section II, It portrays the related work regarding this work. Zone III portrays the proposed work and importance of them. Results are shared in section IV. At closing, conclusion is clarified in Section V.

## II. LITERATURE SURVEY

This area introduces an audit on different procedures in VANET where fuzzy systems are displayed and utilized for directing reason.

Chen et al. (2010) [6] proposed a framework that means to investigate the metaphysics instruments for inconsistency discovery and light-weight Intrusion Detection System (IDS) are utilized to play out their examination. To recognize the Sybli assault, different sensor hubs are utilized. Proposed model uses the novel engineering plan of light-weight IDS that can diminish the stacking time on the sensor arrange. Proposed model accepts an assault as a module for precisely distinguishing the irregularity and later play out the ideal activity on it. Proposed framework is definitely making the system lightweight IDS since it improve the usage of IDS on WSN helpful. Goni et al. (2015) [9] proposed Neuro-fluffy Genetic Intrusion Detection System (IDS). The examination commitments on the utilization of Artificial Neural Network, Fuzzy rationale Genetic calculation and blend of any of the two were investigate and recognized a portion of their constraints. At that point we proposed Neuro-fluffy Genetic Intrusion Detection System which would be another exploration heading and are writing for the related field. The dataset that would be utilized to assess the framework were additionally quickly examined in this work. Sanyal et al. (2015) [26] proposed the Network-based and have based IDS to avert both the system from assaults that may happen inside just as outside of the WSN. There are a few developing techniques for identification of interruption however most frameworks use advanced marks to scan for assault examples of abuse. Proposed framework either consequently reacts to the bad conduct or lingerie the framework chairman to make proper move. IDS are even sense misappropriation by applying the conduct information crime scene investigation to play out the ideal errand.

Khan et al. (2016) [13] proposed half and half interruption discovery model that comprises of a lot of base-include

classifiers that utilizations fractional unique element space just as an information mining classifier. Proposed model consolidates the element choice strategy for the advancement of the location rate while applying the information mining procedure to trim down the quantity of bogus alerts like joint endeavor of abuse identification and abnormality recognition. The exploratory outcomes reason that half and half model has a superior way to deal with execution while actualizing the recognition definition with both low FPR on typical framework utilizations and high DR on vindictive projects.

Hasrouny et al. (2017) [11] concentrated on VANET security systems that are displayed in 3 sections. There are broad diagrams of VANET security qualities and difficulties just as prerequisites are directed. The ongoing security designs subtleties and security conventions are adhered to with a standard objective for example to keep up the VANET progressing. The subsequent significant issue and spotlights would be on novel characterization for avoiding the diverse digital assaults that are known in the VANET with their answer. The last approach is to think about the arrangements previously executed by the researcher's dependent on security criteria in VANET. Tyagi et al. (2017) [30] proposed a discovery calculation that recognizes the pernicious sensor hubs in any system. Steering convention executed in VANET is increasingly inclined to assaults that may transmit the undermined information to the beneficiary without confirming the toughness and unwavering quality of the sensor hub. Consequently, the need to improve the supervisory calculation is made. To execute the ideal calculation another and novel calculation is proposed and tried over VANET by steering bundles with numerous situations. Proposed framework assesses the presentation of DSR and AODV steering conventions to test their speculation over the city and parkway. Safi et al. (2017) [23] proposed a novel structure for PIaaS, a security, and protection cognizant help. The Service Level Agreements (SLAs) are appropriately in set for guaranteeing the smooth handling and correspondence postponement towards mists.

Mahdi et al. (2018) [15] proposed a general review of trust displaying in sensor hubs. Assaults and alleviations techniques in WSNs were likewise inspected. Creators sort all assaults related with trust plots in organize from various characteristics. In view of the writing, the exploration holes and the bearings of future research are outlined. Mittal et al. (2019) [16] proposed a system model that considered as conglomeration of huge volume of hubs into a littler sub-framework associated with one another (it could be straightforwardly or by implication). Proposed model at first actualized the EESR convention with ART-2 neural-net. While managing information transmission and correspondence between sensor hubs these are visit difficulties specialists needs to face and handle them with most extreme actions. The proposed model outcomes show that the system unusualness is so high and surveying the IDS needs complex computational counts to handle the issue in a skilled manner.

## III. DESCRIPTION OF PROPOSED SYSTEM

There are a few calculations accessible for the VANETs, out of which numerous has been proposed in the examination in the ongoing years. Existing framework utilizes the neuro-fluffy framework to improve the assault location in Vehicular Ad-hoc Networks (VANETs). During their examination they found that nature of administrations (QoS) can be corrupted while assault occurred on any vehicular. However, every vehicle detected the information and transmitted it to neighbor hub and may create the information plenitude and information peculiarity. This will build the handling power and decreases the transmission capacity. Another issue in the current framework is sharing information with no encryption. From various gaps and challenges identified through literature survey, it finalizes few challenges as the objectives for current work. The objective of this work is listed as follows; The main objective of this thesis is to design mobility based self-network reconfiguration system in VANET. The next objective is to use dynamically reconfigurable routing protocol with shortest path for routing in network.

.

*1. Research Methodology*

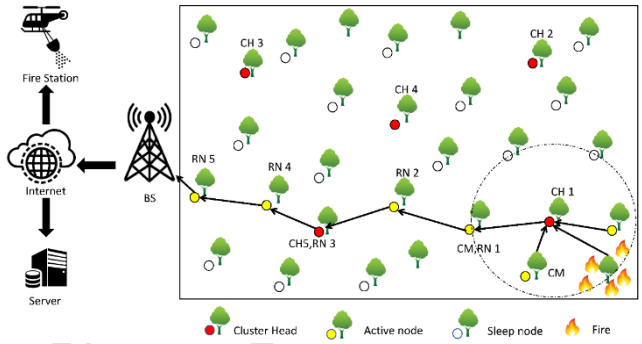


Fig 2: Nodes Deployed to Monitor Fire Disaster

Existing framework proposes a steering 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. There are a few upgrades that are proposed to conquer the current work that proposed framework point by point here. In this work, it proposes a novel secure vehicle-to-vehicle correspondence calculation utilizing neuro-fluffy 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 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 are being sent in a hazardous situation. Sensors are arbitrarily spread over the zone. Every sensor 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. Provide Random Mobility*

At that point give irregular versatility in hubs to show that all hubs are dynamic in nature. All hubs move here and there relies on their speed. We can change the speed of hubs physically.

*D. Temperature Effect*

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.

## IV. RESULTS & DISCUSSION

This work presents a VANET framework with assault recognition and control without anyone else reconfiguration convention. In registering graphical UI is a kind of UI that permits clients to cooperate with electronic gadgets utilizing pictures as opposed to message orders. GUIs can be utilized in PCs, hand-held gadgets, for example, MP3 players, convenient media players or gaming gadgets, family unit apparatuses, office, and industry hardware. The existing work implementation is shown in Fig 3 below.

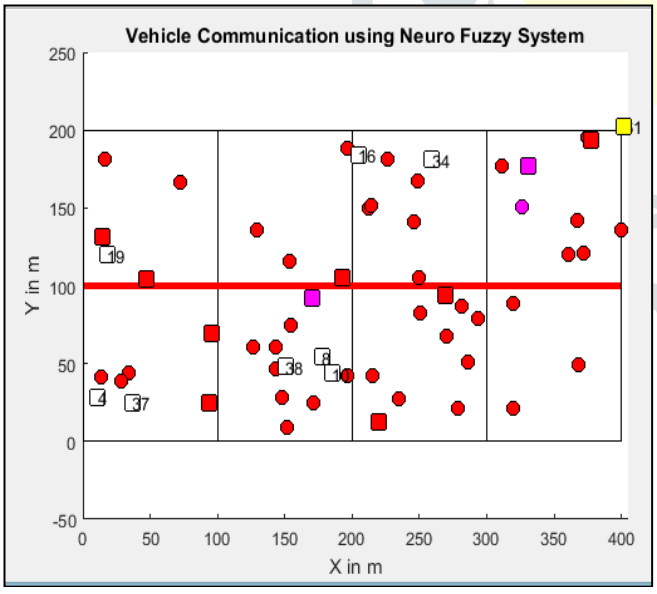


Fig 3: Existing VANET System using Neuro Fuzzy Method

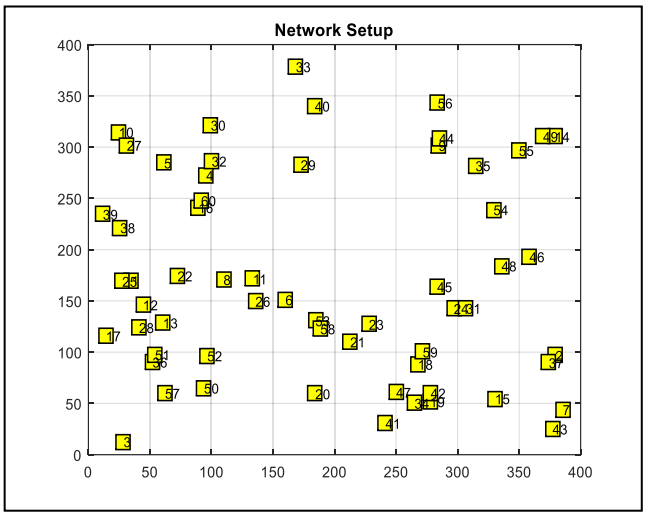


Fig 4: Placement of Vehicle in Network

The above figure 4, shows how the vehicle are being sent in a territory. Vehicles are haphazardly spread over the territory. Every vehicle has an ID appeared alongside it.

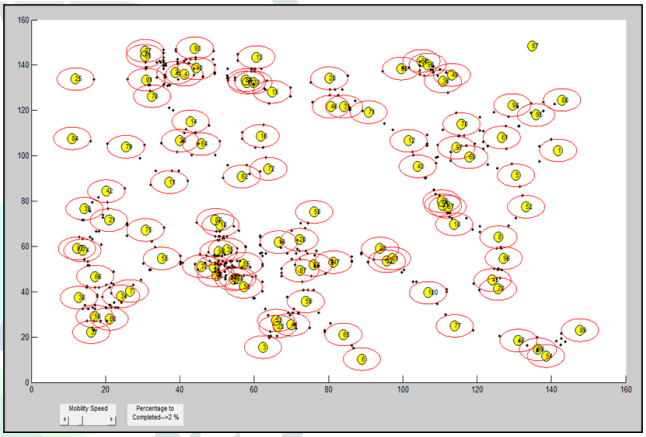

Fig 5: Mobility in Nodes

It will be utilized to address any sensor all through the procedure. Here we take enormous number of sensors so that proposed plan will assess without any problem. The data of the considerable number of hubs will be update to single hubs to which we accept as a cell director. This arrangement is a normal capacity of facilitate factors characterized in the vectors. They are arbitrary in nature. No two hubs cover one another. In run of the mill utilization situation, the hubs will be uniformly conveyed over an open-air condition.

This separation between adjoining hubs will be negligible yet the separation over the whole system will be huge. After the sending of the sensor hubs, there is a Head hub determination by surveying technique. In a sensor organize, the essential sensors are straightforward and play out the detecting task, while some different hubs, regularly called the heads, are all the more impressive and spotlight on interchanges and calculations. Essentially, the head sorts out the fundamental sensors around it into a bunch, where sensors just send their information to the head and the head does the long-extend between group interchanges. In this, a surveying plan is utilized in heterogeneous sensor systems for such applications to lessen power utilization. Surveying is a technique where the bunch heads demand every hub individually to send the information back to the group head. The motivation behind surveying is to dodge impedance from numerous hubs sending to the group head at the same time.

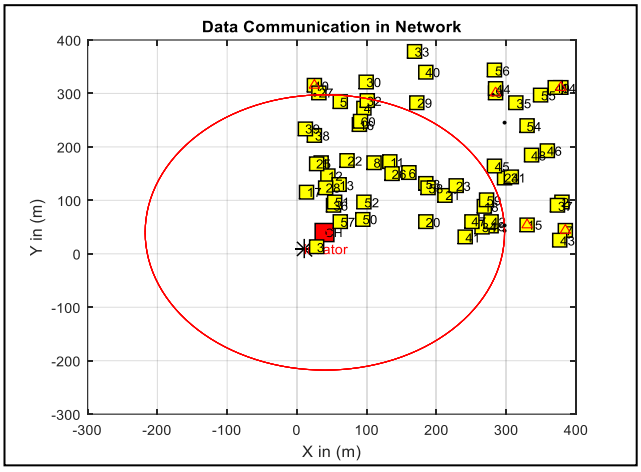


Fig 6: Message Transfer by Head to All Vehicle

On the off chance that the head doesn't send any order, these hubs will start to work. Around then, the course convention runs on the WSN stage. The steering comprises of two essential instruments: Route Discovery and Route Maintenance. Course Discovery is the system by which a hub wishing to send a parcel to a goal gets a source course. To decrease the expense of Route Discovery, every hub keeps up a Route Cache of source courses it has learned or caught. The system structure of such application comprise of countless hubs, detecting and sending information to the sink persistently. Hubs are conveyed equally in a huge region and necessities to appraise the ideal directing approach subsequent to finding system geography. In such applications as the hubs are conveyed at careful areas so the physical geography of the system stays consistent. This implies that, the ideal steering strategy for transmission can be determined outside the system rather than at hubs. Course Discovery works by flooding a solicitation through the system in a controlled way, looking for a course to some objective goal. In its most straightforward structure, a source hub endeavouring to find a course to a goal hub communicates a Route Request parcel that is re-communicated by middle of the road hubs until it arrives at goal, which at that point answers by restoring an answer bundle to sender.

Reconfiguration is expected to adjust the product's parts with the end goal that it can work in an evolving setting. The faster the middleware reacts to a change, the lesser the application is hindered and the additional time the application spends in an ideal setup. The system throughput is the principle boundary that is utilized to mirror the system capacity. It is the measure of traffic that is leaving the "System". We measure these insights in bits every subsequent unit. As we realize that throughput use to depict misfortune rate which for the most part observed on transport layer.

*A. Performance Comparison of 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 proposed framework gives better reaction regarding start to finish deferral and parcel misfortune rate when contrasted with existing work as appeared in Fig 9 and 10 separately beneath.

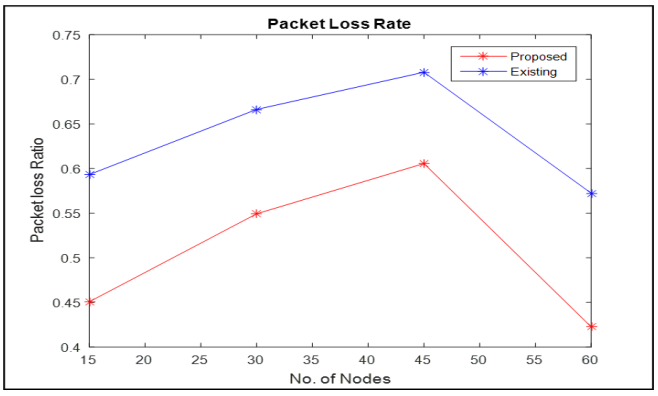


Fig 7: Performance Comparison of Packet Loss Rate

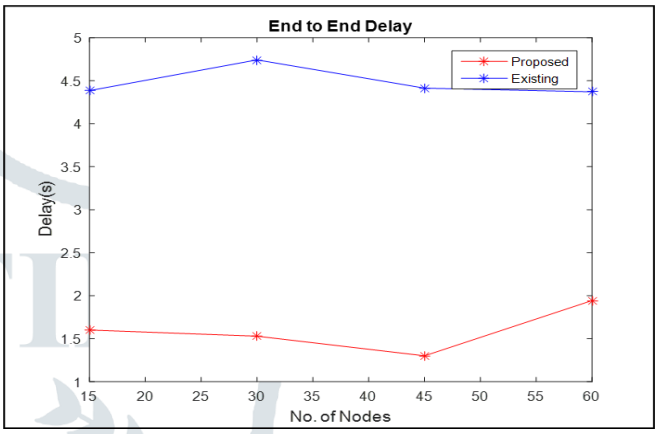


Fig 8: Performance Comparison of End to End Delay

## V. CONCLUSION

This work presents a methodology for dynamic reconfiguration of vehicle in vehicular systems and contrasts the presentation of proposed framework and existing ANFIS framework. All situations of the dynamic reconfiguration framework have been assessed. In this work, all vehicle is speaking with one another. A head is accommodated giving the directions to all vehicle. The requirement for reconfiguration engineering for sensor arranges applications is evident from the consequences of even a straightforward ecological observing calculation. The time required for a specific system to reconfigure its parts is around 30 to 40 seconds, which is less when contrasted with the expense of physically halting and restarting the application with the right segments. In vehicular system applications running over a long term, the capacity to reconfigure the parts, bringing about an adjustment in the conduct of the application, in light of outer boosts, in such a brief timeframe is of exceptional essentialness.

## REFFERENCES

[1] 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.

[2] Aneja, M. J. S., Bhatia, T., Sharma, G., & Shrivastava, G. (2018). "Artificial intelligence-based intrusion detection system to detect flooding attack in VANETs", In Handbook of Research on Network Forensics and Analysis Techniques (pp. 87-100). IGI Global.

[3] Balan, E. V., Priyan, M. K., Gokulnath, C., & Devi, G. U. (2015). "Fuzzy based intrusion detection systems in MANET", Procedia Computer Science, 50, 109-114.

[4] 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.

[5] Chaqfeh, M., &Lakas, A. (2016). "A novel approach for scalable multi-hop data dissemination in vehicular ad hoc networks", Ad Hoc Networks, 37, 228-239.
[6] Chen, R. C., Haung, Y. F., & Hsieh, C. F. (2010). "Ranger intrusion detection system for wireless sensor networks with Sybil attack based on ontology", New Aspects of Applied Informatics, Biomedical Electronics and Informatics and Communications.
[7] Chinnasamy, A., Prakash, S., &Selvakumari, P. (2013). "Enhance trust-based routing techniques against sinkhole attack in AODV based VANET", International Journal of Computer Applications, 65(15), 0975-8887.
[8] Deka, R. K., Kalita, K. P., Bhattacharya, D. K., &Kalita, J. K. (2015). "Network defense: Approaches, methods and techniques. Journal of Network and Computer Applications", 57, 71-84.
[9] Goni, I., & Lawal, A. (2015). "A Propose Neuro-Fuzzy-Genetic Intrusion Detection System", International Journal of Computer Applications, 115(8).
[10] G. Samara, W. AH Al-Salihy, and R. Sures, "Security issues and challenges of vehicular ad hoc networks (VANET)". In New Trends in Information Science andService Science (NISS), 2010 4th International Conference Gyeongju, pp: 393–398. IEEE,2010
[11] Hasrouny, Hamssa, et al. "VANET Security Challenges and Solutions: A Survey." Vehicular Communications 7 (2017): 7-20.
[12] Kaur, J., Singh, T., &Lakhwani, K. (2019). "An Enhanced Approach for Attack Detection in VANETs Using Adaptive Neuro-Fuzzy System", In 2019 International Conference on Automation, Computational and Technology Management (ICACTM) (pp. 191-197). IEEE.
[13] Khan, J. A., & Jain, N. (2016). "Improving intrusion detection system based on KNN and KNN-DS with detection of U2R, R2L attack for network probe attack detection", International Journal of Scientific Research in Science, Engineering and Technology, 2(5), 209-212.
[14] Kumar, V., Mishra, S., & Chand, N. (2013). "Applications of VANETs: present & future", Communications and Network, 5(01), 12.
[15] Mahdi AlQahatani, M., & GM Mostafa, M. (2018). "Trust modeling in wireless sensor networks: state of the art".
[16] Mittal, M., Saraswat, L. K., Iwendi, C., &Anajemba, J. H. (2019, April). "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 (IoT-SIU) (pp. 1-5).
[17] 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.
[18] 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).
[19] Perkins, C. E., & Royer, E. M. (1999, February). "Ad-hoc on-demand distance vector routing", Second IEEE Workshop on Mobile Computing Systems and Applications (pp. 90-100). IEEE.
[20] Poonia, D., & Sharma, M. K., "Detection and Prevention of Denial of Services Attack based on Signal Strength and Reputation Mechanism".