International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 4 Issue 5, July-August 2020 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Self Reconfigurable Protocol among Vehicles with Dynamic Routing

Manisha Rani[1], Jyoti Kataria[2]

[1]M.Tech Scholar, [2]Assistant Professor,
[1,2]Department of Computer Science & Engineering,
[1,2]Manav Institute of Technology and Management, Jevra, Hisar, Haryana, India

ABSTRACT

By providing access for the user to construct different virtual fields, proposed protocol accomplishes the goal of meeting the need of different applications and different network conditions. In this work, an environmental data collection scenario is taken. 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. It will provide a multi-hop routing based on shortest path in wireless networks. This protocol gives the administrator a powerful ability. 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 work shows better improvement in packet loss ratio and end to end delay values as compared to existing results. The proposed mechanism is implemented with MATLAB.

KEYWORDS: *VANET, Reconfiguration Model, Dynamic Routing, Mobility in Vehicles, MATLAB etc*

How to cite this paper: Manisha Rani | Jyoti Kataria "Self Reconfigurable Protocol among Vehicles with Dynamic Routing" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-4 | Issue-5, August 2020, pp.1553-1563, URL: www.ijtsrd.com/papers/ijtsrd33208.pdf

IJTSRD33208

1. INTRODUCTION

Vehicular system can be actualized utilizing the portable specially appointed system to make the correspondence between every vehicle so they can trade data (detected information). Detected information is utilized to illuminate drivers in different vehicles about the neighbourhood of the vehicle traffic stream or the presence of any risky movement. Another utilization of VANETs is utilized to improve traffic the board of a specific territory as stream blockage control, course streamlining and to give access of web to on-board drivers to infotainment, the exact area of stopping accessibility, video-gushing and sharing and so forth. In this section, we clarify an outline of the VANETs, their highlights, applications and design. At that point, we group VANET by their applications and capacities. VANETs are advancing extremely quick and proficiently to be to the truth yet every development has some restriction and imperfections to uncover and that turns into the significant region of research. 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 extra ordinarily 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 everyday 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 materialness to improve our lives. They help us by stretching out our capacity to precisely screen, study, 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. The Vehicle-to-Vehicle (V2V) sense the information and transmit to satellite related is appeared in figure.

Assume information is detected by the vehicular hub inside the sensor field. Since the transmission scope of radio for every sensor is short, A from the outset, passes detected information to the neighbour hub B. In this model, this information might be directed by the way A-B-Sink-C. Since sink is as of now associated with the Internet, it can convey detected information to the client straightforwardly from sink. Vehicular sensor hubs in VANETs can likewise self-sufficiently process and helpfully dissect detected information inside systems with the goal that they can improve the calculation to diminish the excess information caught and saw inside a VANET and convey just fundamental information to the client through sink hub. Besides, WSNs can powerfully adjust its topology. After the sending of vehicular hubs in a sensor field, they self-rulingly discover the neighbour hubs and start speaking with one another in

different manners, ordinarily utilizing multi-bounce interchanges.

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, 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 a version 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.

A. 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).

I. **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.

II. **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.

III. **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.

IV. **Communication Environment:** Providing correspondence between vehicle-to-vehicle and vehicle-to-roadside are started with the assistance of directing calculations.

B. Attacks in VANET

There are different security assaults to which the VANET systems are defenceless against. These assaults have enormous effect on the system as well as lead to death toll also. Following are a portion of the security assaults which can be propelled on VANETs.

I. **Denial of Service Attack:** The Denial of Service (DoS) assault is performed at which a specially appointed system is inaccessible. This could be accomplished by flooding the sensor connect with unordinary and undesired solicitation so the present system assets are kept being used and couldn't make any genuine solicitation. This won't ready to access that specific sensor hub, asset or message. Another method for executing this assault is by smashing the all correspondence channels.

II. **Distributed Denial of Service:** This is likewise a sort of DoSor definitely a variation of DoS assault that have more than one assailant who attempts to dispatch the RREP on the injured individual hub. The assault is executed with the assistance of numerous sensor hubs and an immense measure of assets are procured by various sensor hubs situated at different positions. The primary rationale of DDoS assault is to negate with the accessibility of hub as a security prerequisite.

III. **Sybil Attack:** This kind of assault attempts to copy the hubs that are shaped utilizing unlawful and unscrupulous characters and when a sensor hub sends the message to other sensor hubs utilizing various personalities it got the ideal data. Subsequently unique sensor hubs have diverse impression about a similar sensor hub. Sybil assault is thoroughly relying upon the fact that it is so natural to shape personalities, whether the sensor organize considers all the sensor hubs comparative or they have any sort of unique finger impression. There is a scope of methods accessible to battle this assault like factual and likelihood approach is one of them.

IV. **Alteration Attack:** When any interloper changes their information and attempts to refresh it these kinds of assault is propelled. The changed information will consequently advance to the assailants arrange. Another approach to execute these sorts of assaults are deferring the message that must be sent in and on a similar sensor organize.

V. **Black Hole Attack:** Black gap assault is executed when the hub denies taking an interest in the sensor arrange startlingly and that could be the sensor hubs drop out of the sensor organize. This assault additionally utilizes the whole information to be sent to a sensor hub that doesn't exist at all in the sensor organize that subsequent in tremendous loss of significant information.

VI. **Malwares:** In VANETs malwares can prompt divert beside regular activity of the system to unconscious tasks. This may happen when the product refreshed an inappropriate refresh and introduce the undesirable arrangement of code into the framework.

VII. **Wormhole Attack:** These sorts of an assault that have the two real sensor hubs that isn't in one another's range and needs to transmit data through the passage. The gate crasher sensor hub lies in transmission scope of both the real sensor hubs in a sensor organize. The genuine hubs convey by means of the interloper sensor

hub inside the passage and may have the entrance to burrow.

The remainder description of paper is as per the following; Section II examines the surveyed work done by various authors in this field. Section III presents the proposed methods used during this study. The results are presented in section IV. The conclusion and its future scope is described in Section V.

2. LITERATURE SURVEY

This area introduces an audit on different procedures in VANET where fluffy systems are displayed and utilized for directing reason. Shamshir band et al. (2014) [27] proposed a model that forestalls the sensor organize from assailants by stopping the aggressor, sink hubs and the base station, creators utilized a novel Game-based FQL, agreeable game theoretic guard framework. Proposed calculation joins the helpful game hypothesis and fluffy Q-learning frameworks properties so that, the participation can be expanded between the sink hub (for recognition) and base station (reaction). The Game-FQL model is a triple-player game technique, giving solid protection against a solitary assailant hub. It has been resolved that continuous communication supports collaboration between sink hubs and different hubs. Deka et al. (2015) [8] proposed a framework that there are numerous guard strategies accessible in the exploration network and numerous procedures have been proposed to give better resistance against interruption. Creators secured a general review of different methodologies and furthermore examined current safeguard issues and difficulties. Proposed inquire about paper portrays the safeguard structures, control instruments and foundation designs to mount a decent protection. Creators additionally covers a portion of the IDS and IPS for the verifying the remote sensor organize. Sunil Kumar et al. (2015) [29] proposed the distinctive support learning methods that assessed concerning noxious hub recognition with and without comprehension. The proposed new Greedy Q cognizance calculation and Soft SARSA Cognitive calculation are likewise assessed by changing the parameters like learning rate, organize reward focuses and number of preparing cycles. Balan et al. (2015) [3] proposed a strategy not just recognizes the assault, it likewise distinguishes the range and expansion of assault. This proposed calculation gives the novel answer for this issue recognizes the assault with a lot of precision by utilizing the fluffy rationale calculation. Proposed framework additionally contains IPS instrument strategy that contains and gets their contribution from fluffy set and gives the protected information transmission over the sensor arrange. IPS additionally watches the traffic of dark opening and dark gap assaults. The yield of proposed model obviously depicts that the strategy distinguishes the assault in a viable and dependable way when contrasted with existing technique. Rupareliya et al. (2016) [22] proposed a plan that uses a Bayesian channel for the security reason. To distinguish and avert the noxious hubs, Watchdog technique is utilized however there are likely possibilities that a bogus positive may happen during the identification procedure. So to sift the odds through Bayesian channel is utilized that will check whether the identified sensor hub is really a malignant or not. From the exploratory plan creators presumed that, Bayesian channel is sufficient to diminish the bogus positive location proportion in guard dog strategy. Chaudhary et al. (2016) [4] proposed a novel interruption discovery framework (IDS) in light of neuro-fluffy classifier in parallel structure for parcel dropping assault in versatile impromptu systems. As far as IDS design, we have depicted two kinds of models dependent on neuro fuzzy classifier, for example neighbourhood, and appropriated and helpful. The proposed structures of IDS give the yield in type of 0 or 1 where 0 shows the ordinary example and 1 exhibits the irregular example so that in this paper, yield 1 methods malevolent hubs are introduced in the system. In future, we are concentrating to distinguish all sort of assaults in MANETs condition.

Prathima et al. (2017) [21] proposed SDACQ: Secured Data Aggregation for Coexisting Queries in Wireless Sensor Networks that coordinates multi-inquiry accumulation with additively homomorphic encryption. SDACQ performs confirmed question scattering by which no bogus inquiry is infused into the system. The exploratory investigation and execution examination of proposed model shows that SDACQ distinguishes replay assault and incapable to total malignant commitments. SDACQ likewise verifies the sent sensor hubs that may acquire a little deferral. Pandey et al. (2017) [18] proposed a novel framework to deal with the Denial of Service (DoS) assaults in the remote sensor arrange (WSN). Proposed model recognizes the hubs that are troublesome and complex to distinguish and forestall. Proposed calculation utilizes the follow back strategies to avert the DoS and undesired flooding of information to stop the sensor organize. There are two fundamental parts of follow back model that are accessible for example initial one is to distinguish the conceivable assailant and after that identify the pernicious bundles. Proposed model lessens the odds of getting assaulted by suspicious hubs and increment the authentic approaching traffic among sender and collector hubs. Abdel-Azim et al. (2017) [1] proposed a streamlining procedure of fluffy based IDS that is acquainted with distinguish and counteract the delayed consequence of assaults, for example, dark gap assault. It is proposed to see the impact of the streamlining on the quality of existing framework. To play out their exploration they utilized the shape, number, and position of the enrolment work for each fluffy set. Proposed calculation computerizes the procedure and upgrades the deciding the participation work for the fluffy motor for rule age. The fundamental danger of dark opening assault is that it harmed the sensor organize traffic by transmitting the phony and incessant RREP messages over and over.

Poonia et al. (2017) [20] proposed the security of MANET that is one of the basic segments for an association. Creators have dissected both the direct and issues of security dangers in adaptable Ad-Hoc arranges with best proposed game-plan discovering system. This hypothesis work gives the report along results achieved from the investigation coordinated on the AODV convention in extraordinarily named framework. Consequently, the execution of AODV can be overhauled by using balanced AODV, which uses banner power and reputation-based arrangement. Nayyar et al. (2018) [17] proposed a framework that work on an effective information spread methodology which improves the vehicle network as well as improves the QoS between the source and the goal. It uses properties of firefly improvement calculation in a joint effort with the fluffy rationale. The proposed methodology is inspected and rather than the current situation with the-workmanship draws near. In future the proposed

methodology will be additionally stretched out to oblige various situations by following provincial, roadway, sub-urban and urban conditions. Kaur et al. (2019) [12] depicted the neuro-fluffy framework for the discovery of assaults on vehicle by reproducing it in VANET. Existing calculation additionally centers in vehicle to vehicle correspondence without confirming the source, vehicles transmit the information to collector hub. The current neuro-fluffy framework additionally give no information collection that expands the peculiarity and bounty of information to be transmitted over an unbound course, which may cause a portion of the hubs forever detached from the remote sensor arrange. This may diminish the productivity of the VANETs in light of the fact that the sending systems track each sensor's individual area for the best possible inclusion of the VANETs.

From study, a beneficial data dispersing approach was proposed which upgrades the vehicle to vehicle accessibility just as improves the QoS between the source and the objective. The proposed system was examined rather than the present circumstance with the-workmanship draws near. The sufficiency of the proposed system was appeared concerning the significance. It gets cultivated in the parameters specifically, package disaster extent, end-end delay, typical download deferral and throughput in connection with the present philosophies.

3. DESCRIPTION OF PROPOSED SYSTEM

Presently the recipient hub gets this as the first informational index accepting that it is real detected information and prepared for what it's worth, without approving the legitimacy of sensor hubs. This procedure prompts doubt and all the more basically, to close down the system. So utilizing this data, we can find that current framework has just assault recognition ability, no noxious hub location and no encryption. These issues need desperate consideration of analysts for development to keep away from the data from getting captured by the faulty hubs and abuse of data.

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. 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. The proposed model will use the restriction strategy for the availability of the hubs inside the bunches in the way where they will expend 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 graphics, 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. In real, the genuine framework displayed a steering convention for VANET, which can be progressively reconfigured by the remote manager. It could accomplish the objective that receive to various applications and distinctive system conditions. This convention would give the manager of the WSN a ground-breaking capacity. With this extraordinary capacity, the chairman could change the steering convention remotely to embrace various applications and diverse system conditions. So as to get this capacity however our steering convention, they bolstered a few directions for the director to change the directing convention running on the sensor organize stage. The hubs would change their directing convention when they got the directions.

To give the directions a chance to become an integral factor on the hubs, they gave a lot of components. With these directions and components, this steering convention was enriched with the incredible capacity of adjusting to various applications and distinctive system conditions. At the system level, the natural information assortment application is described by having an enormous number of hubs ceaselessly detecting and transmitting information back to a lot of base stations that store the information utilizing customary techniques. These systems by and large require exceptionally low information rates and amazingly long lifetimes. In commonplace utilization situation, the hubs will be equally dispersed over an open-air condition. This separation between contiguous hubs will be negligible yet the separation over the whole system will be critical. Natural information assortment applications ordinarily use tree-based directing topologies where each steering tree is established at high-capacity hubs that sink information. When the system is designed, every hub occasionally tests its sensors and transmits its information up the directing tree and back to the base station. For some situations, the interim between these transmissions can be on the request for minutes. Run of the mill announcing periods are relied upon to be somewhere in the range of 1 and 15 minutes; while it is workable for systems to have fundamentally higher detailing rates. The ordinary condition parameters being checked, for example, temperature, light power, and moistness, don't change rapidly enough to require higher detailing rates. Notwithstanding enormous example interims, ecological observing applications don't have exacting inertness necessities. Information tests can be deferred inside the system for moderate timeframes without essentially influencing application execution. When all is said in done the information is gathered for future investigation, not for constant activity. So as to meet lifetime necessities, every correspondence occasion must be unequivocally planned.

A. Flow Chart of Proposed System

I. 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.

II. 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.

III. 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.

IV. Provide Head & Initiator

After the sending of the sensor hubs, there is a Head hub determination by surveying strategy. In a sensor arrange, the essential sensors are straightforward and play out the detecting task, while some different hubs, regularly called the heads, are all the more dominant and spotlight on interchanges and calculations.

V. Environmental Data Collection

All nodes are speaking with one another based on most brief way determined. At that point head check the status of every hub and gathers the natural information from sensor hubs. All hubs gather information like temperature or any calamity influence from condition.

VI. Communication between Head & Nodes

For this, there is an immediate correspondence between head and hubs. Head gets some information about 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.

VII. 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 as shown in Fig 1.

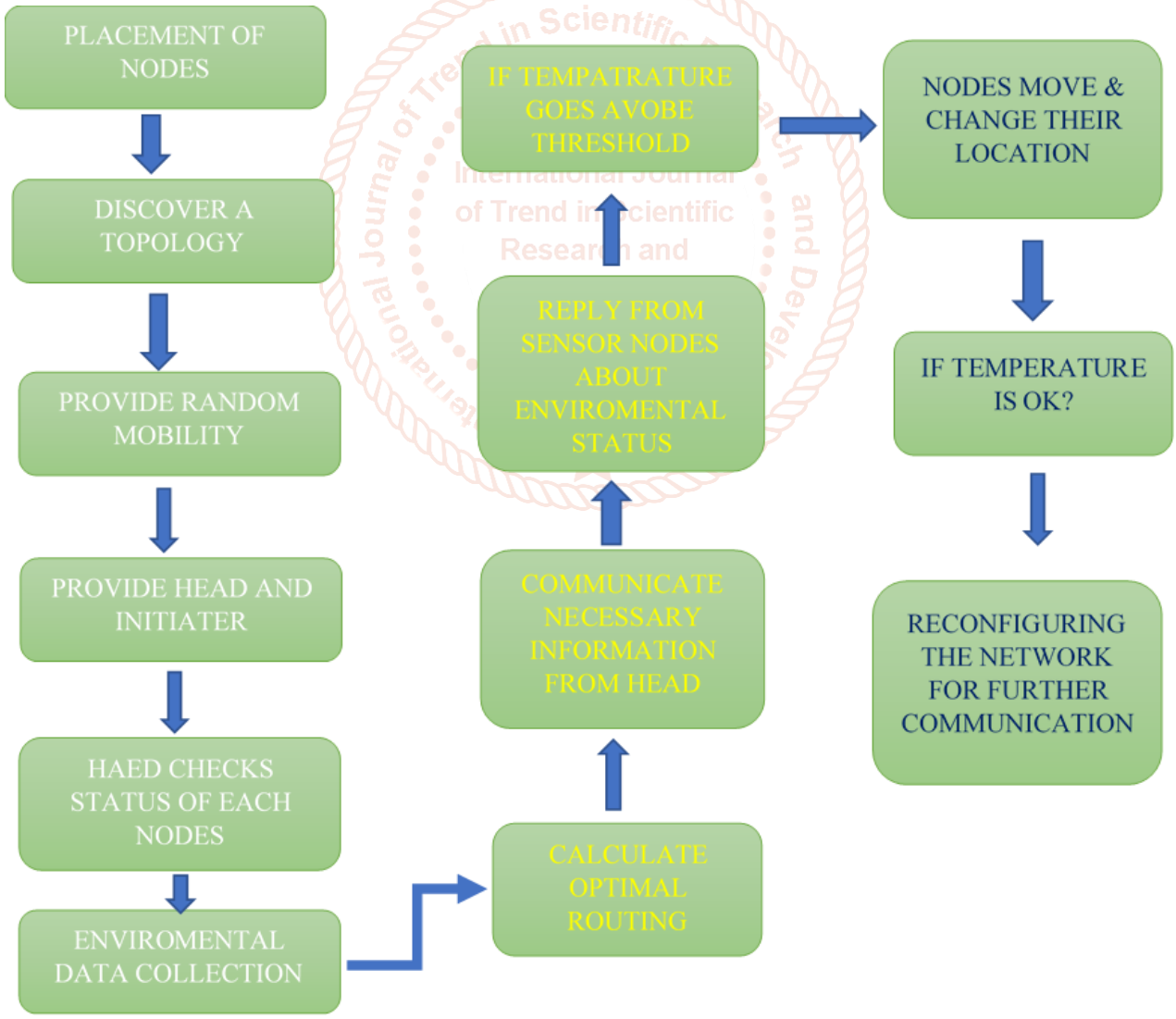

Fig 1: Proposed System Model of Reconfiguration System

4. RESULTS & DISCUSSION

This work presents a VANET system with attack detection and control by self-reconfiguration protocol. In computing graphical user interface is a type of user interface that allows users to interact with electronic devices using images rather than text commands. A GUI represents the information and actions available to a user through graphical icons and visual indicators such as secondary notation, as opposed to text-based interfaces, typed command labels or text navigation. The actions are usually performed through direct manipulation of the graphical elements. For this, it uses the GUI toolbox in MATLAB. The existing work implementation is shown in Fig.-2 below.

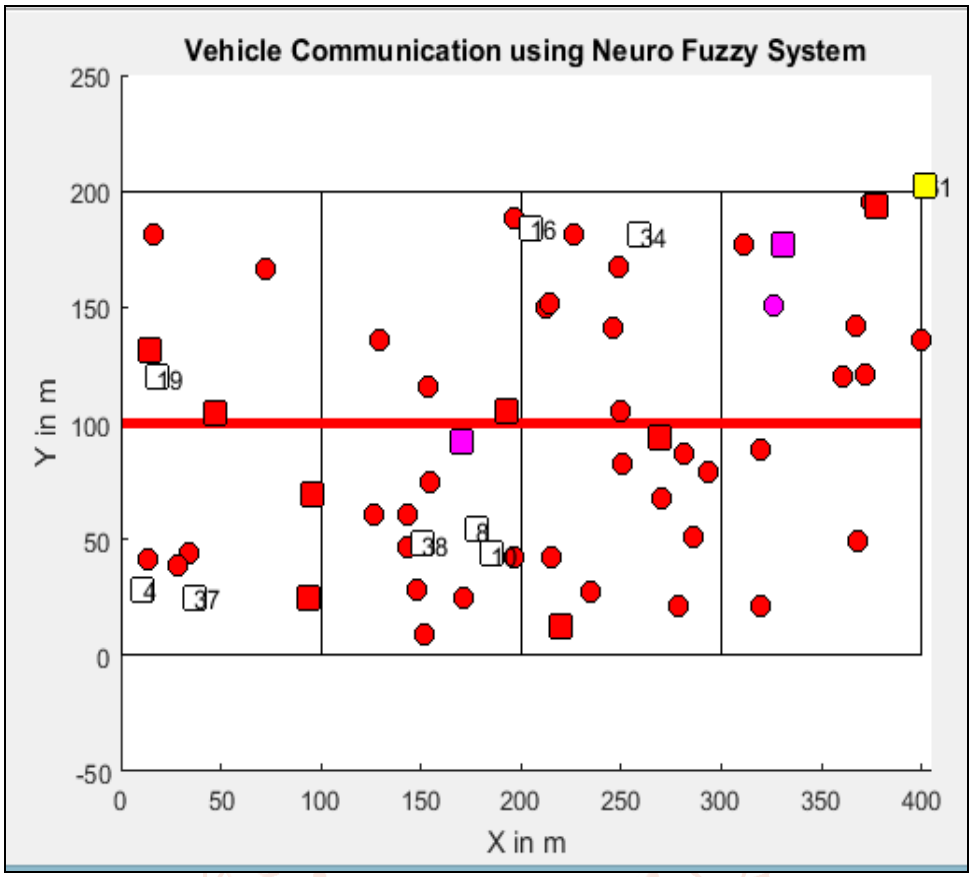

Figure 2: Existing VANET System using Neuro Fuzzy Method

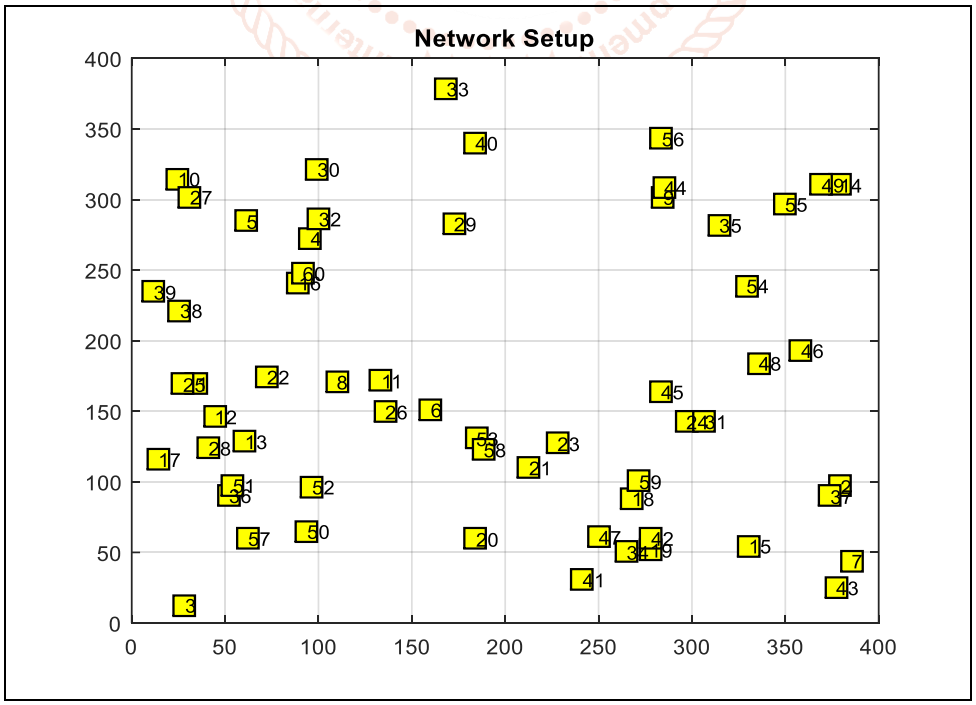

Figure 3: Placement of Vehicle in Network

The above figure 3, 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.

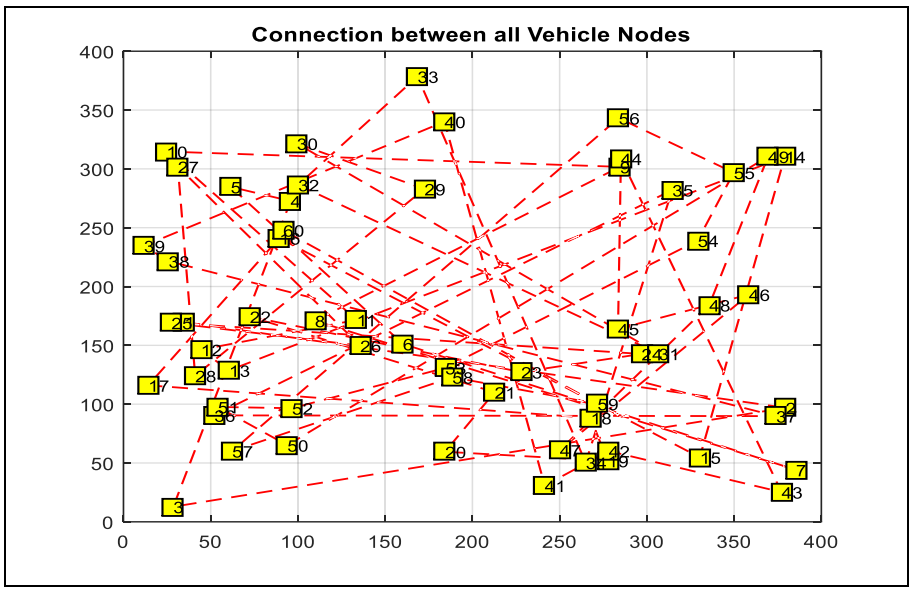

Figure 4: Mobility in Nodes

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.

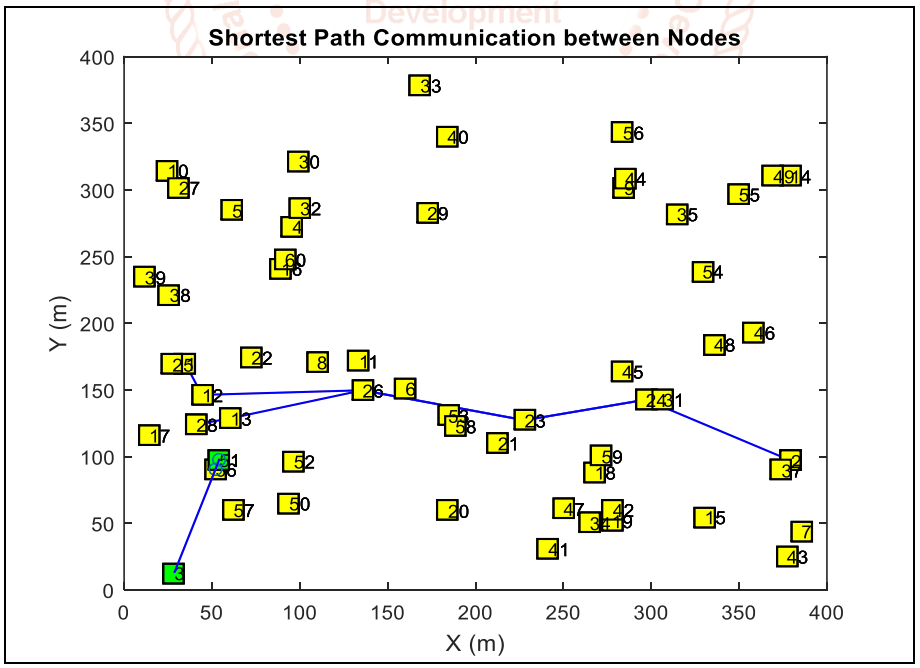

Figure 5: Message Transfer by Head to All Vehicle

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 comprises 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.

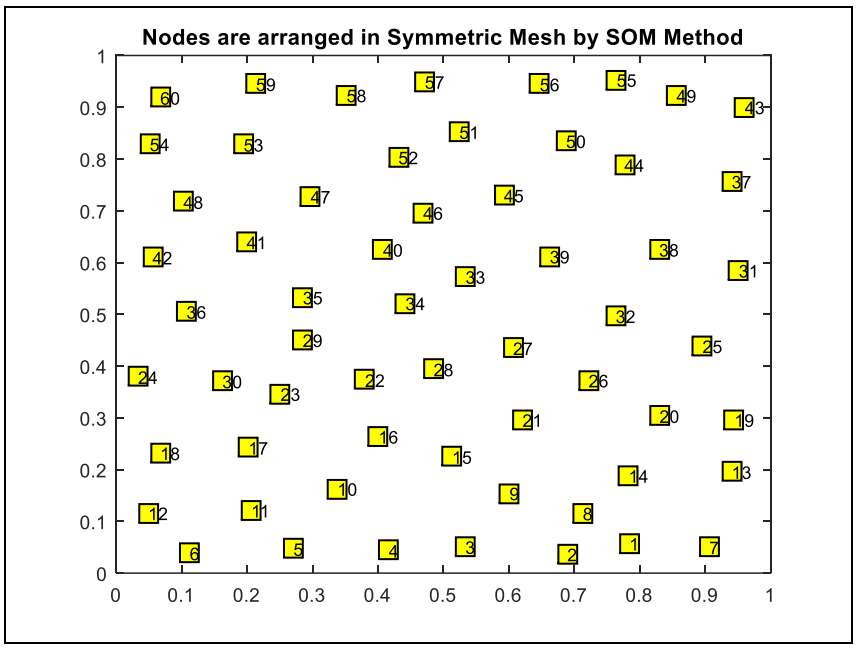

Figure 6: Vehicle Arranged in Sequential Manner

The sensor network application that are being envisioned will be deployed over large numbers of sensor nodes. Often these networks will be deployed in inhospitable and inaccessible terrain. A sensor network composed of many autonomous nodes, exposed to the elements and communicating via unreliable wireless technology is vulnerable to failure. Nodes may fail either from lack of energy or from physical destruction and new nodes may join the network. The communication between the nodes may be disrupted by noise in parts of the network and environment. A sensor network can be made robust enough to face these challenges if it is able to reconfigure itself. Once the network has been deployed in the field, reconfiguration for the most part applies to software reconfiguration. This involves reconfiguring the software components executing on individual nodes or in parts of the network to alter their behaviour in response to the changing environment. The application executing on other sensor nodes would be reconfigured to compensate for the loss of data from the obstructed sensors.

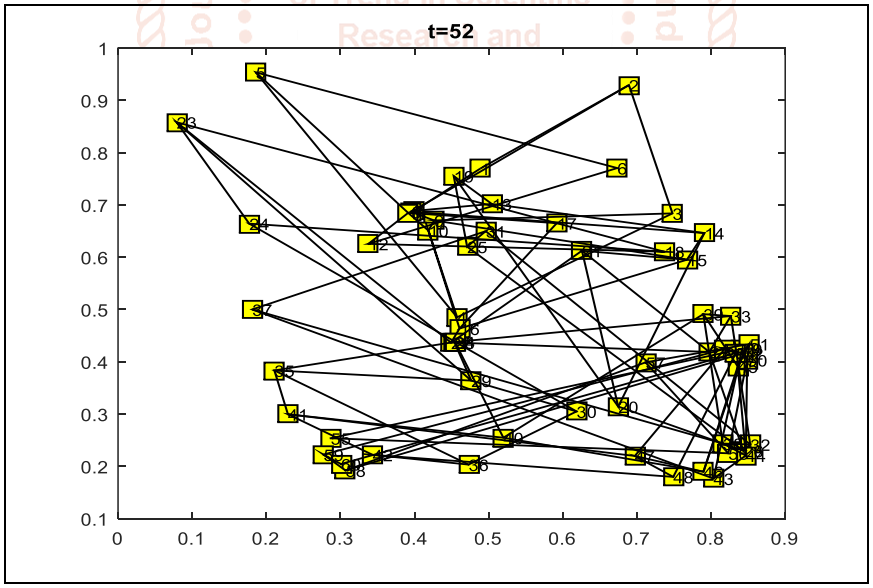

Figure 7: Reconfiguring the Network on Demand

A. Performance Analysis of System

Reconfiguration is intended to adapt the software's components such that it can operate in a changing context. The quicker the middleware responds to a change, the lesser the application is interrupted and the more time the application spends in an optimal configuration. This work presents an approach for dynamic reconfiguration of vehicle in vehicular networks and compares the performance of proposed system with existing ANFIS system. The proposed system provides better response in terms of end to end delay and packet loss rate as compared to existing work as shown in Fig 8 and 9 respectively below.

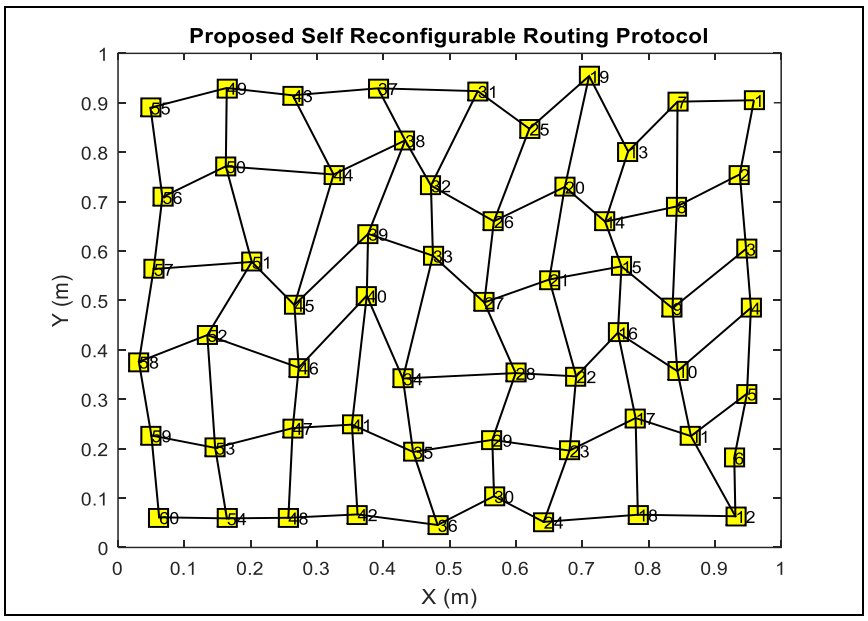

Figure 8: Self Reconfiguring Network Output

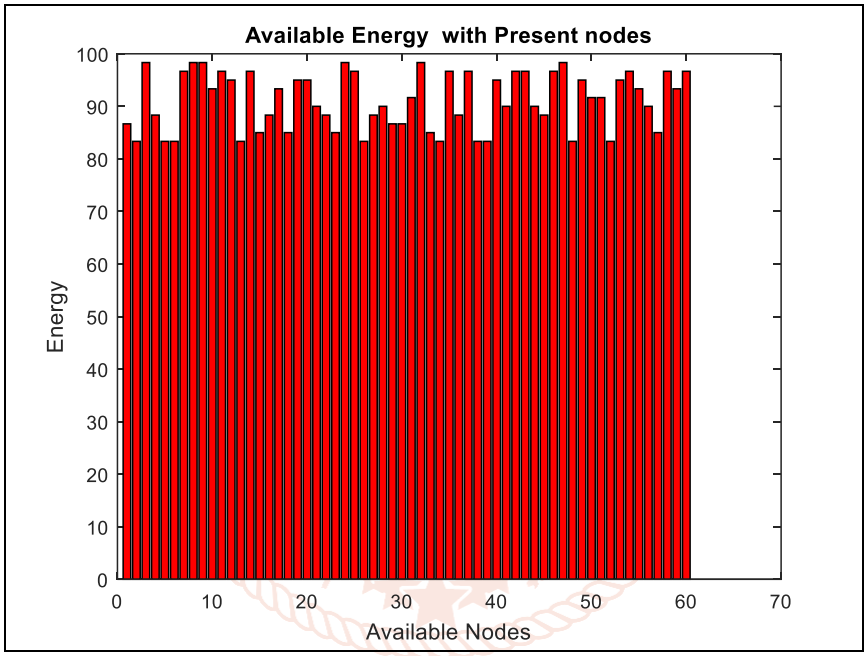

Figure 9: Available Energy in System

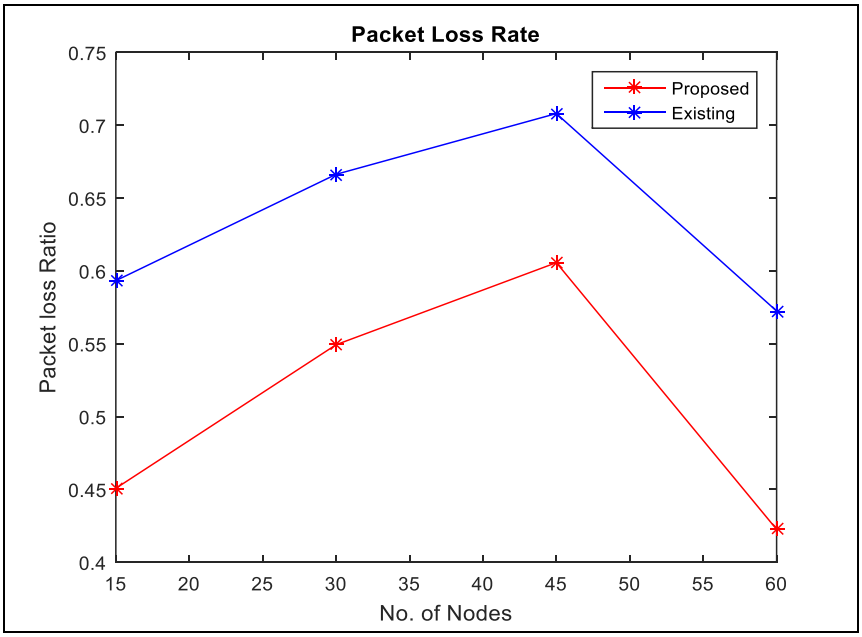

Figure 10: Performance Comparison of Packet Loss Rate

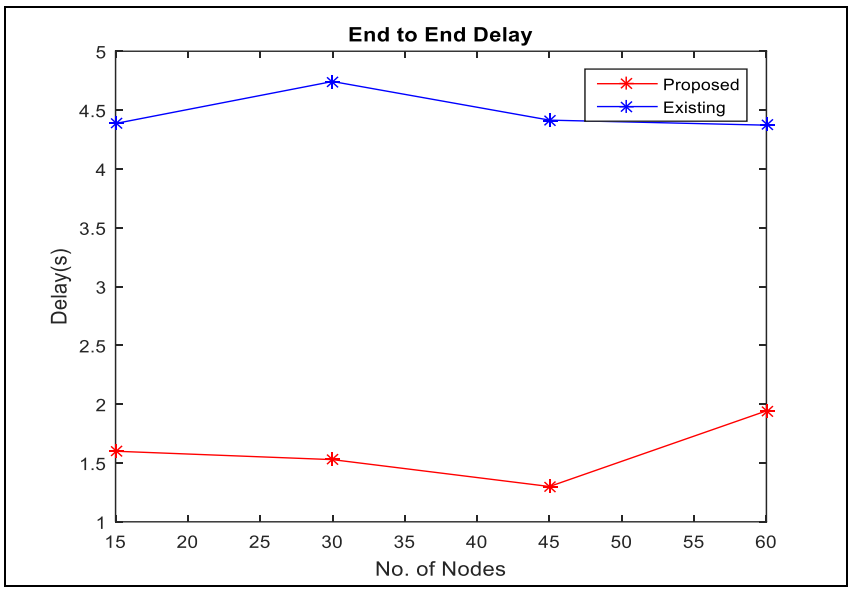

Figure 11: Performance Comparison of End to End Delay

5. CONCLUSIONS

This work presents an approach for dynamic reconfiguration of vehicle in vehicular networks and compares the performance of proposed system with existing ANFIS system. All scenarios of the dynamic reconfiguration infrastructure have been evaluated. The need for reconfiguration architecture for sensor network applications is apparent from the results of even a simple environmental monitoring algorithm. The time required for a particular network to reconfigure its components is around 30 to 40 seconds, which is very less when compared to the cost of manually stopping and restarting the application with the correct components. In vehicular network applications running over a long duration, the ability to reconfigure the components, resulting in a change in the behaviour of the application, in response to external stimuli and in such a short time is of special significance. The automatic reconfiguration of components expressed in a user-friendly modelling environment on a base station in response to changing operating conditions in the field. Reconfiguration is performed when the QoS attributes exceed a set threshold. These thresholds may be different for different application domains. Also, energy is saved by using dynamic reconfiguration system. In this, shortest distance is calculated between each node so that an optimal routing is performed in network and also direct communication between head to nodes is also provided. The proposed system provides better response in terms of end to end delay and packet loss rate as compared to existing work.

In Future Scope, QoS for applications in WSNs needs to explored and appropriate algorithms need to be devolved.

REFERENCES

[1] M. Abdel-Azim, H. E. D. Salah & M. Ibrahim (2017). "Black Hole attack Detection using fuzzy based IDS", International Journal of Communication Networks and Information Security, 9(2), 187.

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

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

[4] A. Chaudhary, V.N. Tiwari, & A. Kumar (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] M. Chaqfeh, & A. Lakas (2016). "A novel approach for scalable multi-hop data dissemination in vehicular ad hoc networks", Ad Hoc Networks, 37, 228-239.

[6] R. C. Chen, Y.F. Haung, & C.F. Hsieh (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] A. Chinnasamy, S. Prakash, & P. Selvakumari (2013). "Enhance trust-based routing techniques against sinkhole attack in AODV based VANET", International Journal of Computer Applications, 65(15), 0975-8887.

[8] R. K. Deka, K. P. Kalita, D. K. Bhattacharya, Kalita & J. K. (2015). "Network defense: Approaches, methods and techniques", Journal of Network and Computer Applications", 57, 71-84.

[9] I. Goni, & A.Lawal (2015). "A Propose Neuro-Fuzzy-Genetic Intrusion Detection System", International Journal of Computer Applications, 115(8).

[10] G. Samara, W. AH, Al-Salihy, Sures & R. "Security issues and challenges of vehicular ad hoc networks (VANET)", In New Trends in Information Science and Service Science (NISS), 2010 4th International Conference Gyeongju, IEEE, 393–398.

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

[12] J. Kaur, T. Singh, & K. Lakhwani (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), IEEE, 191-197.

[13] J. A. Khan, & N. Jain (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] V. Kumar, S. Mishra, & N. Chand (2013). "Applications of VANETs: present & future", Communications and Network, 5(01), 12.

[15] M. Mahdi Alqahatani, GM Mostafa, M. (2018). "Trust modeling in wireless sensor networks: state of the art".

[16] M. Mittal, L. K. Saraswat, C. Iwendi & J. H. Anajemba (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 (IoT-SIU), 1-5.

[17] S. Nayyar, A. Suman, & P. Kumar (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] C.E. Perkins & E.M. Royer (1999, February). "Ad-hoc on-demand distance vector routing", Second IEEE Workshop on Mobile Computing Systems and Applications IEEE, 90-100. .

[20] D. Poonia & M. K. Sharma, "Detection and Prevention of Denial of Services Attack based on Signal Strength and Reputation Mechanism".

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

[22] Rupareliya, J., Vithlani, S., Gohel & C. (2016). "Securing VANET by preventing attacker node using watchdog and Bayesian network theory", Procedia computer science, 79, 649-656.

[23] 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.

[24] Saggi, Mandeep & Sandhu, Ranjeet (2014). "A Survey of Vehicular Ad Hoc network on Attacks & Security Threats in VANETs".

[25] Sampigethaya, K., Huang, L., Li, M., Poovendran, R., Matsuura, K. &S ezaki, K. (2005). "CARAVAN: Providing location privacy for VANET", Washington Univ Seattle Dept of Electrical Engineering.

[26] S. Sanyal, N. Das & T. Sarkar (2015). "Survey on host and network-based Intrusion Detection System", ActaTechnicaCorviniensis-Bulletin of Engineering, 8(1), 17.

[27] S. Shamshirband, Anuar, N. B., M. L. M. Kiah, V. A. Rohani, Petković, D., Misra, S., & A.N. Khan (2014). "Co-FAIS: cooperative fuzzy artificial immune system for detecting intrusion in wireless sensor networks", Journal of Network and Computer Applications, 42, 102-117.

[28] S. Shamshirband, A. Patel, N. B. Anuar, M. L. M. Kiah & A. Abraham (2014). "Cooperative game theoretic approach using fuzzy Q-learning for detecting and preventing intrusions in wireless sensor networks", Engineering Applications of Artificial Intelligence, 32, 228-241.

[29] G. Sunil kumar, J. Thriveni, K. R. Venugopal, C. Manjunatha, & L. M. Patnaik (2015). "Reinforcement based Cognitive Algorithms to Detect Malicious Node in Wireless Networks", International Journal of Computer Applications, 109(16).

[30] P. Tyagi & D. Dembla (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.