Novel Algorithm for Enhancing Bitrate in MANET for Topology Based Routing Protocol

Munisha Devi, Nasib Singh Gill

Abstract: ***Mobile computing is rapidly growing due to powerful, cheaper and smaller devices in a smart environment. By creating smart devices with mobile communication abilities, the idea of being connected anytime, anywhere and anyhow has become reality. Group of smart devices creates a mobile network (Ad Hoc Network) while communicating directly and wirelessly. When mobile nodes move, the topology changes frequently and dynamically, at that time security or some network management mechanism is required. By reviewing the functional mechanism, advantages, and disadvantages of previous routing protocols, new routing protocols can be designed for MANET and performance evaluation of different protocols is very important for the designing of a new mechanism. Various routing protocols have been designed for MANETS but these are not sufficient for all the needed requirements in MANET environment. Comparisons analysis of different protocols have been conducted in these networks using different scenarios, however, they are still not sufficient to make decisions as to which protocol is better for a specific scenario, that's why lot of research is still being conducted, in the design implementation and enhancement of novel protocols in network. This paper presents various securities and safety-related issues of MANET systems, and also advocate the requirement of enhancing routing protocols. MANET protocol has been enhanced to increase the bitrate of active protocol in mobile network and performance comparison carried out between the existing and proposed approach.***

Index Terms: ***Smart city, Security requirements, MANET, Routing Protocol, AODV.***

I. INTRODUCTION

Wireless networks can be divided into two types of infrastructure-based and infrastructure-less networks. The first one (infrastructure-based) are those which relies on access points or base stations (relies on fixed infrastructure). Example of this type is cellular networks or wireless local area networks. These networks have base station which helps in routing or transmitting the data that is transmitted from the particular node to target nodes. On the other hand second category (infrastructure-less) have no centralized access points as we can see in figure1. There is a collection of various nodes which can be tablets, laptops, etc. and we can say that there is not any fixed infrastructure as base station or access point, unlike the picture where each node will have to contact via that particular base station or access point [1].

Revised Manuscript Received on October 15, 2019

Ms. Munisha, Pursuing Ph.D., Department of Computer Science & Applications, M. D. University, Rohtak, India

Dr. Nasib Singh Gill, Professor, Department of Computer Science & Applications, M. D. University, Rohtak, India

So the ad-hoc network belongs to infrastructure-less network category. In these networks there is a group of various wireless-enabled nodes, which can contact one another and there is no based station or access points. When nodes are in the proximity of one another they can contact (communicate) with one another and they can create a topology, and when these nodes move due to the mobility, the topology changes over time.

These wireless structures are also called as multi-hop networks because they not need any certain infrastructure hence if a node needs to communicate or transmit some data to goal node, it needs help of the intermediate nodes. Intermediate nodes behave as peer nodes and these peer nodes participate in transferring data packets from initial to goal node. These wireless structures are self-configuring and self-organizing. If there is a group of various nodes and these nodes are put together, they will be able to create the network by themselves and different nodes will start to communicate.

In multi-hop, if the goal or target node is not in the communication range of the initial node then the initial node will have to take help of the intermediate nodes. So if it is not a single hop transmission from the source to destination node but it goes through a number of intermediate nodes consequently we have multiple structures the packets are sent through multiple hops from the source to the goal node. So these networks are useful in various situations like different types of emergency or during any relief operations. In the history disaster incidents, when the internet infrastructure, network infrastructure and building infrastructure, collapse than it was very difficult for the rescue team to be able to communicate with one other because whatever was existing it doesn't exist anymore. So in order to efficiently communicate between the various victims and rescue workers it's very important to have some kind of a system or mechanism by which the communication can be restored and structure can be set up fast. So ad-hoc networks become useful in these scenarios and it is very easy to set up such network in remote areas or desert areas where there is not any certain infrastructure [2]. So not much planning can be afforded to set up these networks. So that is why these networks prove to be very useful. Ad-hoc networks depend on deployment and topology. These networks can be divided into two types. One is known as the homogenous and another is a heterogeneous network. Homogenous network, contain different nodes which have similar characteristics and similar specifications.

An example of this type is smartphones which have very similar abilities and specifications, on the other hand, in heterogeneous ad-hoc networks the nodes may not be of the same type and may not all have similar specifications.

They have different capacities. An example would be a network that is formed of PC, Tablets, and Smartphones [3].

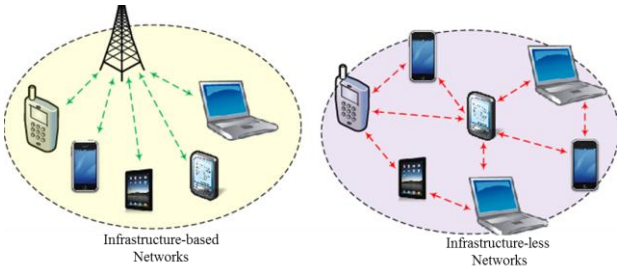

Fig1: Infrastructure based and infrastructure-less networks

History of Ad Hoc Networks: The idea of Ad Hoc Networks is not new, it comes into existence in 1970 with the DARPA project, called as Packet Radio Network Project. The aim was to enable contacts (communication) in a battlefield among various wireless devices so that different ports and terminals contact with one another. But the main issue was that even though this concept proves to be useful but the gadgets used were very large in size, and also portability issue was also there. Even though the project was popular, but there was not much that was done since 1970. In the 1980s this project again looked upon, and the wireless devices become portable and consequently the idea that was demonstrated in the packet radio networks was becoming more beneficial for us in communication in various scenarios, scenarios of relief operations & disasters, where there is no fixed infrastructure and it is not very easy to set up infrastructure because nothing already exists and it is very hard to set up such a network [4].

Characteristics of Packet Radio Networks: These networks consist of various dedicated mobile stations, wireless terminals, and mobile radio repeaters. These repeaters transmit data from one repeater to others until the data reaches the host. So the benefit of having such a network is that this network is self-organizing, rapidly deployable, and self-initializing, and there is no need of administration problems or network management issues. But there are various draw bags also. For example although it is very attractive to have this type of network but the main issue with respect to medium access so when you have several such nodes and there is no access point or centralized coordinator, which can help the different nodes to get access to the common medium then medium access control becomes a big issue. Similarly the traditional problems of routing, flow control, error control, and so on and so forth including in a transport issue these become challenging in this kind of networks and in fact without addressing these problems in the newer context of PRNET with existing solutions with other kinds of wireless networks the internet becomes very inefficient.

II. LITERATURE SURVEY

In the paper [5] the author described that routing protocol can also be categorized according to route computation: Precomputed (proactive/ table-driven) and On-Demand Routing. In precomputed as the name indicates, the nodes are computed in advance. The main benefit of Proactive routing is that there is no latency problem (the route is already available) but because of changing topology, there is a strong possibility that predefined routes never be used. Another issue is that dissemination of routing data consumes lot of bandwidth while networking topology and link-state change rapidly. The main benefit of reactive routing is that it saves bandwidth [6]. While exchanging routing data, supporting to only those goals nodes to which the routers require to send data traffic, but here the problem is latency in transmission.

Performance evaluation of protocol is done by R. Balakrishna et.al. [7]. Comparison is done between both AODV and AOMDV protocols. The comparison was based on various parameters. The proposed algorithm of AOMDV was better than the basic AODV algorithm in term of finding the alternative path while currently used path link breaks down. But the main limitation of the work was more routing overhead and less throughput.

Manoj Kumar et.al [8] evaluated the performance of various protocols DSR, DSDV, and AODV for a mobile ad-hoc network having thirty number of nodes. Network performance is evaluated taking various parameters like throughput, data traffic received, data traffic sent, control traffic received, control traffic sent and number of retransmission attempts, on OPNET simulator. Simulation time 20 minutes and data rate 2mbps were taken. AODV shows better performance over the two algorithms. The limitation was smaller number of nodes were taken for the experiment.

Arafatur Rahman et.al. [9] Report the simulation analysis and performance evaluation of different routing algorithm. The zone routing protocol (ZRP), optimized link State Routing Protocol (OLSR), dynamic MANET on-demand (DYMO) routing, Ad Hoc on-demand distance vector (AODV) have been taken for performance evaluation. AODV and ZRP show close result through graphs and OLSR was the worst one. DYMO performed worst in case of jitter and end to end delay. ZRP and OLSR performed well in case of end to end delay.

Agrawal et.al. [10]provides a detailed simulation-based performance study for various metrics like the end to end delay, packet delivery transmission, network load with DSDV protocol using network simulator. The performance was evaluated using various mobility models as Manhattan mobility model, Gauss Markov, reference point group and random waypoint mobility model having different speed and network load. In paper [11] the authors have shared their five-year working experience in Ad Hoc Network environment. They worked in a real environment, they included tested software package and also included several implementations.

The author shared different potential dangers and issues faced by them during their work. They also mentioned various issues that require special attention to make mobile network usable and implementable in Real-world.

Previously multi-hop wireless routing and medium channel access were the main issues associated with a mobile network. The research on MANET shows that security is the main problem providing secured information between mobile nodes in a smart environment [12]. The existing security methods of wired networks can't be used in mobile networks. The issues including Limited physical security, resource-constrained capacity, distributed Corporation, highly dynamic topology, wireless medium. It is important to protect the network functionality to transmit message between mobile nodes through multi-hop ad-hoc forwarding. The data packets transmitting between the mobile nodes should be consistent with the protocol specification [13]. For exchanging routing information in wireless environment, sometimes trust relationship is used by routing protocols among participating nodes and hence the currently used protocol trust on neighboring nodes but it is possible that the trust model unintentionally permit malicious attacker to enter in-network, for example, replaying old routing data or by including erroneous routing data or inefficient routing can cause malicious attacker to enter in system. Hence routing protocols should be robust against any kind of attacks [14, 15].

III. CLASSIFICATION OF WIRELESS NETWORK

Wireless networks can be divided in to various kinds of networks as shown in the figure. In WANET (wireless ad-hoc network), various nodes are fixed but these nodes can contact others in ad-hoc manner. The first one is MANET (mobile ad hoc networks) where all or some nodes are mobile and topology changes frequently. It is actually heterogeneous system. Here nodes may or may not move. This network has self-CHOP characteristics, where C describes configuration, H stands for Heal & O stand for Optimize and P stands for protection. These properties characterized these networks. Here link changes continuously and frequently due to mobility present in network. The nodes act as router to transmit other nodes data in any mobile multi-hop networks [16, 17].

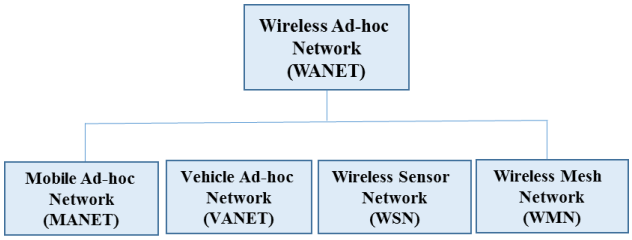

Fig 2: Classification of wireless Ad- hoc network

Another category is *VANET*. Here networks are formed by different vehicles moving on the road. Here different vehicle, want to communicate with one another and each of these vehicles has some electronic equipment, which is known as an onboard unit (OBU). And this OBU has the capability to communicate to the roadside access point. And these access points are set up on the roadside. So these vehicles can communicate with each other. In figure3, we have double-headed yellow color arrows which signify that there is contact between the different vehicles. And the black color denotes that the vehicle can communicate to the roadside units. So we have two types of communication, one vehicle to vehicle and another vehicle to roadside units. So VANET is important because these provide spontaneous information exchange mechanism between these different vehicles so that the vehicle can communicate to one another.

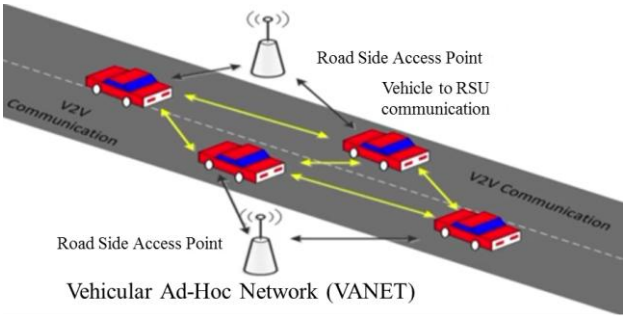

Fig 3: Vehicular Ad- hoc network

These networks offer different applications. When some unfortunate incident took place, immediately information about the accident is conveyed to all other vehicles by the particular vehicle following the accidental vehicle, the other things are with respect to different comforts that can be offered to drivers of the vehicles and they can be offered various services while driving. There are two types of communication, one is V2V (inter-vehicle communication) and other is V2i (vehicle to infrastructure communication). Communication between them is very important. Here networks are co-operative in driving, media streaming, and in Information sharing.

Comparison between mobile ad-hoc networks and Vehicular ad-hoc networks: MANET look similar to VANETs but in fact, they are different, because in MANET nothing is predictable or we can say that traffic pattern can't be imagined but in case of VANET traffic pattern is fairly predictable. In MANET moving pattern of nodes is "random" but in VANET it totally constrained by road. In both network topology changes but mobility is low in case of MANET as compared to VANET. Node lifetime in case of mobile ad-hoc networks depends on power resources but in VANET it depends on lifetime of vehicles. Multi-hop routing is present in MANET but multi-hop routing is weakly available in VANET. In terms of cost of deployment, VANET is highly expensive to deploy compare to MANET. Their range also varies.

Another category of ad-hoc networks is WSN *(wireless sensor networks)*, here nodes have different sensors and these nodes able to sense the different phenomenon that is occurring around them and the sensed data is sent to base station and so base station remotely the different phenomena that occur around the sensors that deployed on the field can be monitored. These networks can be divided into two categories, one is stationary and the other one is mobile category. The sensors Nodes are very small in size. Different applications of these sensors are: used for different types of applications like soil makeup measurement, lighting condition measurement, noise level, humidity level, temperature measurement, etc.

Another category is WMN (*wireless mesh networks),* it is somewhat like MANET but there is a backbone of access points which are connected in mesh-like fashion and as we know mesh topology is important to maximize the reliability of transmission in a network, for example, if some link fails in the system then other links help in transmitting data from one place to other. There are different types of application scenarios transportation, building automation, Metropolitan Area Networking, enterprise networking, home networking, and broadband, so on.

Here is an example of the ad-hoc network is connected via an IP backbone to the internet.

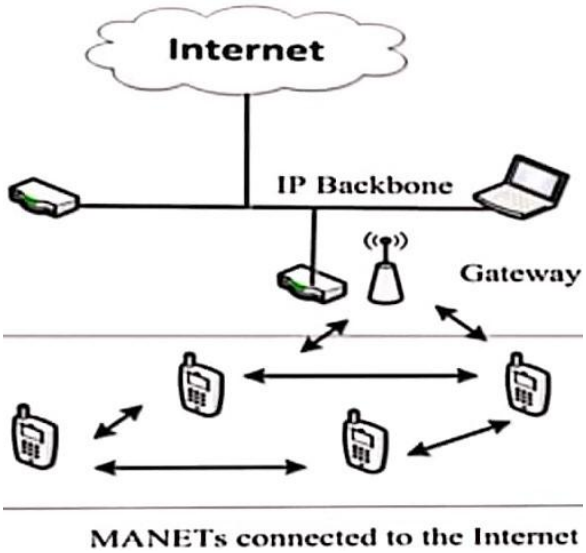

Fig 4: MANETs connected to the internet

IV. CONSTRAINT IN AD HOC NETWORKS

There is a different constraint in Ad Hoc networks.

Energy Efficiency: A very important issue in Ad-hoc network is Energy Efficiency. The nodes in the Ad-hoc Network are battery-powered. So there is no infinite battery that powers these nodes. So typically once the battery is fully charged it can last for a couple of minutes to a couple of hours. There are different ways due to which energy consumed such as transmission, computation, retransmission, and reception. Here batteries have limited life cycle, once fully charged they could not be able to last for too long. So additionally there are other issues with the batteries also. So for using the nodes in these networks, it is required to have high performance and smart batteries which will support mobility of the devices also. These batteries should have a low self-discharge rate, they should be able to operate in a wide temperature range, high energy density, and long cycle life. So the commonly used batteries in this network are nickel-cadmium, nickel-metal hydride. It is required to manage the energy at all levels of the network. So there is dire need to improve different protocols in these networks. Energy Management is a crucial issue. Power is basically energy consumed part unit time.

Cooperation in Wireless Ad Hoc Networks: It is a very important issue. Nodes communicate with each other with the help of intermediate nodes. The intermediate nodes act as relays. So these intermediate nodes have to co-operate with the source and destination nodes to transmission to be successfully completed. And all these nodes are energy-constrained. But some nodes may or may not be cooperative. So this becomes a challenge in the ad-hoc network. So there are two extremities in these networks. First is a total corporation and next extremity is total non-cooperation. In total cooperation case, if all the relay requests are accepted, then nodes will quickly exhaust limited energy and in total non-cooperation, if no relay requests are accepted, the network throughput will go down rapidly. There are additional issues in networks also such as selfishness, symbiotic dependence (nodes like to depend on one another, if one node help to relaying the packet to another node, it also expects that the other node is also going to help it in relaying packets or mutual dependence).

Dealing with Misbehaviors: These networks have nodes which have a tendency to misbehave. Marti et al. work in the direction of avoiding these misbehaving nodes. In their work, they defined misbehaving nodes as nodes that agree to cooperate with other nodes but they do not. They mentioned that intelligently identify misbehaving nodes and avert links through these nodes is very important. So in their proposed solutions, they have two components. One component is the watchdog, which runs on every node and tracks the behavior of another node. And the other one is Pathrater, which uses watchdog information for finding reliable routes. Pathrater note downs, which nodes reliable one or which node helps the packet to be delivered successfully to the intended destination. But there was a big draw bag with the proposed model. It failed in a large network and there was large overhead in resource-constrained.

Reputation: one of the ways of handling the issue of cooperation is to promote the reputation and keeping track of the reputation behavior of the nodes in the network. Reputation means that how the different nodes are behaving. If a particular node is sent a packet, keeping track whether it is forwarding it or it is dropping it in between. So if a node drops a packet means it is not reliable and its reputation level is going to down and if a node forwards its reputation level is going to go up. And at the same time, it is also important to identify the liar's nodes in these networks.

Security Challenges in Cooperation: The network is open medium which is shared by different nodes and the nodes dynamically changes positions, at the same time there is no centralized network management or not any certification authority, and because it is open medium and a node getting into the network can be malicious and can stop functioning of other nodes, these nodes are prone to attacks, interference, eavesdropping, and infiltration. Nodes can be captured, compromised, false routing information can be sent.

The main problem is that with the existing solution, one could have handled these problems, none can be assumed will have a centralized authority which can help in defending these attacks. If a node is cooperating with other nodes, it might fall victim from the malicious node.

Routing Challenges: Privacy and Security in the movement of nodes, higher rates, low bandwidth, and high rate of the conception of power at the nodes.

Device Power Management: Power is an important issue not only at the protocol level or algorithmic level but also at the device level. Devices also use power. So there are different device power management technique that has been proposed, one is advanced power management (APM) the other is advanced configuration and power interface (ACPI). But each has its own limitations.

V. SELF-ORGANIZING BEHAVIOR OF WIRELESS AD-HOC NETWORKS

Self-organization is a very important concept in building scalable systems like MANET. The primary objective of self-organization includes availability, scalability, reliability and collaboration and coordination to achieve a shared goal. It collaborates without a central entity. There are different design goal of self-organization in MANET with respect to topology maintenance & topology configuration and neighbor Discovery. Self-organization is a behavior that has been inspired by different natural phenomena and has been adopted in the network system. In self-organization behavior, there are patterns which emerge at the global level using only local information generated by the interaction between lower-level components. For example, local interaction between the nodes within the particular area and that information scales up for the overall network system. Emergent Behavior is a behavior of a complex system initiated by simple interactions between lower-level entities

Through the self-organization feature, Global behavior of the system can be observed. The benefits of self-organization include plug and play Technology. When we plug the system, the system starts operating on its own, it's a fully autonomous system. Where the new nodes which enter the system are automatically configured without needing any human intervention.

Properties of Self-Organizing Networks: Self-organized Networks have very distinct properties as mention below:
Self-configuration: Setting the system parameters without external intervention.
Self-management: It is the second property, which concerned with the maintaining current system configuration in terms of current system parameters.
Self-adaptability: It means the ability of the system to adapt to changing environmental conditions. Self-protection: It is basically the ability of a system to protect itself from the external malicious influences. In a wireless system, there could be a large number of malicious attacks. And the system should be designed in such a way that it should be able to protect itself from such kind of external malicious interferences.
Self-Healing: Self-healing property explains, whenever there is some kind of failure then the system should be able to operate in the presence of such failures and it should be able to recover from such failures.
Self-Diagnose: Next properties self-diagnose means the ability of a system to initiate self-healing and detect faults.
Self-Optimize: It is the ability of the network to configure local components optimally based on global objectives.

Two very important mechanisms for the system is self-configuring and self-organizing. This two mechanism is basically based on typical approaches known as Route Discovery Approach and Route Updating Approach. Route Discovery is very important phenomena for any kind of networks, especially for MANET. The route can be discovered as Proactive or on-demand. In Route updates, single or multiple routes are maintained between a pair of nodes. Route Discovery and route update are two important routing mechanisms also. Self-optimizing helps in improving the routes between the different nodes, with respect to energy consumption and route length.

Self-healing characteristic is also very important in ensuring fault tolerance in MANET. So there are two types of fault tolerance, one is masking fault tolerance, it ensures that the system continues to keep its functionality in the presence of faults. Other is known as masking fault- tolerance, it guarantees that when faults stop occurring, the system converges to the configuration from where it continues to function. Self-healing system and adaptive systems are considered closely related. Adaptive means whenever there is some kind of abnormality or problem arises, the system would be able to adapt to it, and continuously perform its function the way it does.

VI. EXPECTED PROPERTIES OF ROUTING PROTOCOLS

When mobile nodes move, the topology changes frequently and dynamically, at that time security or some network management mechanism is required. By reviewing the functional mechanism, advantages, and disadvantages of previous routing protocols, new routing protocols can be designed for MANET and performance evaluation of different protocols is very important for the designing of a new mechanism. Various routing protocols have been designed for MANETS but these are not sufficient for all the needed requirements in a MANET environment. Properties that should be expected from a routing protocol are given below.
Distributed Operation: We have distributed environment, so protocol should be design in a distributed manner in order to increase reliability. The mobile system being self-organizing and autonomous network, the algorithm should be able to maintain the distributed environment.
Unidirectional Links: The environment in which nodes of MANET operate, is very error-prone. There are different physical factors because of which the links can behave unidirectional at different points of time, instead of being bi-directional. So this basically adds complexity gradually in the network.
Energy Efficiency: Energy is very crucial in this network. And the routing protocol that is proposed for these networks has to be energy efficient. The nodes in these networks, required to have high performance and smart batteries which will support mobility of the devices also. These batteries should have a low self-discharge rate, they should be able to operate in a wide temperature range, high energy density, and long cycle life. So the commonly used batteries in this network are nickel-cadmium, nickel-metal hydride.

It is required to manage the energy at all levels of the network. So there is dire need to improve different protocols in these networks. Energy Management is a crucial issue.

Security and Quality of Service: Security is another issue. These networks are very much vulnerable to various type of security attacks and consequently, the routing protocol that is proposed should keep it in an account. Routing Protocol should be aware of quality of service so that a real-time application might rely on it.

Freedom from Loops: Looping of data packets give considerable overheads in term of power connection and bandwidth. So it is better than the route chosen is acyclic.

Optimization of Metrics: The battery power and bandwidth are the main metrics in mobile networks besides delay and end to end throughput, the widely used performance metrics in wired and wireless networks. The designer must optimize the various metrics.

- Minimum number of hops (shortest path)
- Least congested path (load balancing)
- Bandwidth (minimum overhead)
- Minimum end to end delay
- Minimum packet lost
- Maximum end to end throughput
- Maximum packet delivery ratio.

Efficient utilization of bandwidth: If the routing algorithm provides excessive controlled traffic, the present system bandwidth will be used by control traffic. It may affect the communication performance of the network. As the bandwidth of a mobile system is comparatively limited, the lakh of control overhead becomes an essential design factor.

VII. EXPERIMENTAL RESULTS & ANALYSIS

We carried out a simulation on mobile Ad Hoc Network by using ns2. It gives a highly modular platform for wireless and wired simulations supporting different routing types, traffic, protocols, network elements. It contains the NAM (network animator) tool. NAM is used for visualization. Trace graph tool is used for plotting graph & it is supported by Mac OS, UNIX, and Linux.

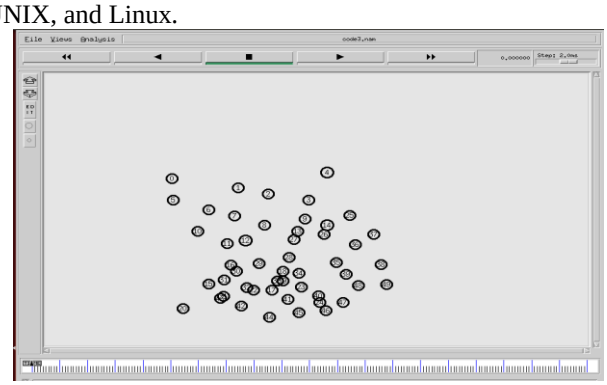

Fig.5: Nodes creation in mobile Ad-hoc network

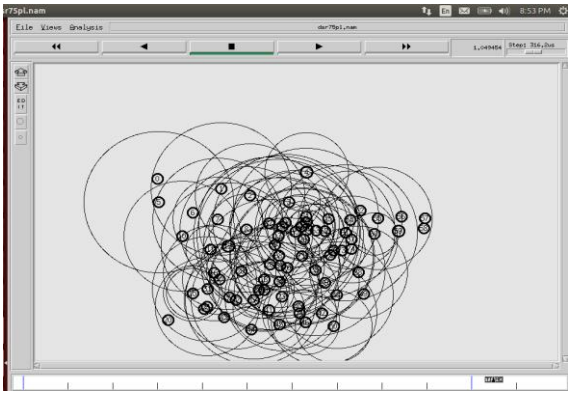

Fig.6: Data transmission range between nodes in network

Transmission Range: Nodes in wireless networks send data only up to a defined (limited) transmission range as shown in the figure. This provides multi-hop functionality. Data transfer rate is calculated by measuring the amount of data transmitted between two nodes in a specified time period. In a smart environment, high data transfer rate permits net to be used for complex tasks such as online streaming. Data transfer rate improve the performance of our task. Nodes creation and data transmission between them is shown in figure 5 and 6 respectively.

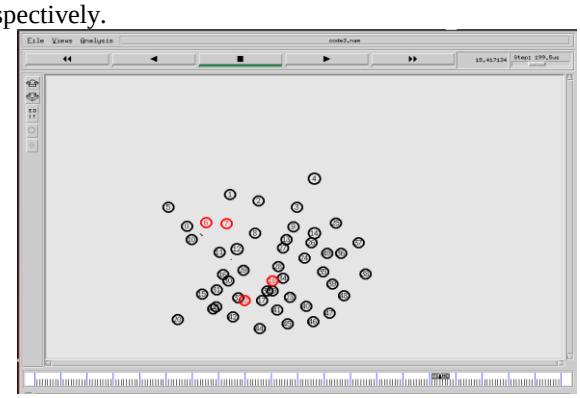

Fig.7: Packet transmission and Mobility of nodes

Mobility of Nodes: We make programs with a fixed number of nodes and specific parameters are used to configure these wireless nodes in network. The initial position of the nodes is fixed. Mobility is provided to nodes with fixed speed and mobility of nodes changes with time to time. We have created mobile nodes in two ray ground Model. Nodes alter their position over time, they often have to update their position estimates to avoid inaccuracy as a result of older position estimates. Packet transmission and mobility of nodes are shown in the above figure 7.

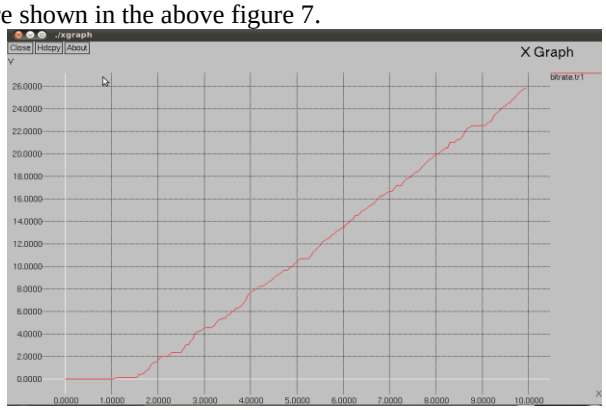

Fig.8: Bitrate of Existing Approach

Bitrate: Bitrate describes a speed, the speed at which data (bits) can be transmitted in the network or it can be defined as the amount of data transmitted per second. The bit rate of the existing and proposed AODV shown in the below figure. And the enhanced bit rate of the proposed algorithm is shown through comparison of both.

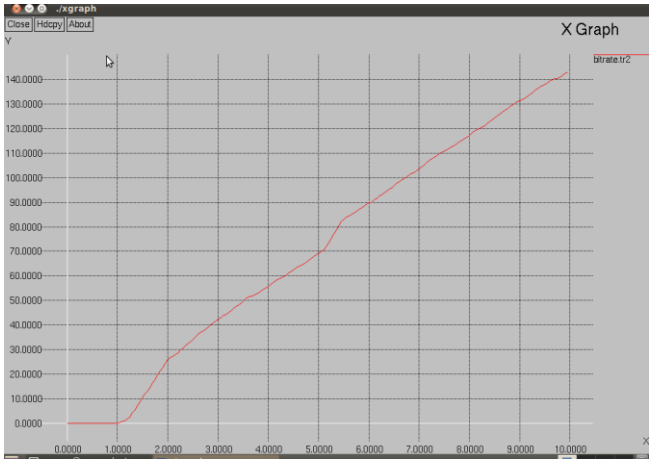

Fig.9: Bitrate of Proposed Approach

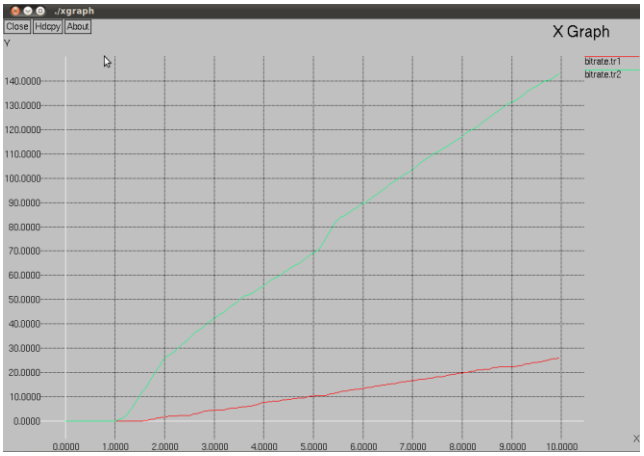

Fig.10: Comparison of Bitrate in both Existing (red) and Proposed Approach (green).

Comparative analysis of bitrate is shown in the above Fig10. X and Y-axis represent the time and bitrate of communication respectively. As we can see, the bitrate has been improved after the implementation of the proposed algorithm.

VIII. CONCLUSION

Ad-hoc networks play a vital role in the mobile environment, but at the same time designing and deploying an Ad Hoc network is very challenging and we have also seen that there are different types of ad-hoc networks and challenges in each of different types of ad-hoc networks are also different. When we concerned about self-configuring and self-organizing behavior of MANET, there are different **issues** for MANET that should be kept in mind.

Here we do not have a centralized coordinator like any access point or base station, which can help the different nodes communicate between them, so it becomes a challenging problem in MANET. Cooperation is a very important issue in an ad-hoc network, without successful cooperation between the different nodes in the networks, the network not going to survive at all. Enhancement of the protocols has become essential in order to strengthen the smart network. The proposed work in the present paper is about to maximize the Bitrate of the reactive protocol in the mobile network. The implementation is done in a mobile network with the AODV protocol. The proposed work may be enhanced in the future and may be implemented with some other protocol. Future work can be on energy consumption on a large scale in the mobile network.

REFERENCES

1. J. Karlsson, L. S. Dooley, and G. Pulkkis, “Secure Routing for MANET Connected Internet of Things Systems”. 2018 IEEE 6th International Conference on Future Internet of Things and Cloud (FiCloud), (2018), 114–119. https://doi.org/10.1109/FiCloud.2018.00024.
2. M. Devi, and N. S. Gill. “Mobile Ad Hoc Networks and Routing Protocols in IoT Enabled Smart Environment: A Review”.*Journal of Engineering and Applied Sciences*,14(3),(2019),802-811.
3. Alameri, I. A. "MANETS, and internet of things: the development of a data routing algorithm." *Engineering, Technology & Applied Science Research* 8, no. 1 (2018): 2604-2608.
4. Ping Yi, Yue Wu, and Futai Zou and Ning Liu, “A Survey on Security in Wireless Mesh Networks”, *Proceedings of IETE Technical Review*, Vol. 27, Issue 1, Jan-Feb 2010.
5. V. V. Mandhare, and R. C. Thool. “Improving QoS of Mobile Ad-hoc Network Using Cache Update Scheme in Dynamic Source Routing Protocol”. *Procedia Computer Science*, 79, (2016),692–699. https://doi.org/10.1016/j.procs.2016.03.090.
6. M. Devi, and N. S. Gill. “Comparison Analysis of MANET Routing Protocols to identify their Suitability in Smart Environment.” International Journal of Engineering & Technology, 7 (4) (2018) 4844-4849
7. R. Balakrishna, U.Rajeswar Rao, N.Geethanjali N,“Performance issues on AODV and AOMDV for MANETS”, *International Journal of Computer Science and Information Technologies(IJCSIT)*, vol. 1,no.2 , pp. 38-43, 2010.
8. Kumar Manoj, Parmanand, S. C. Sharma & S.P. Singh, “Performance of QoS Parameter in Wireless Ad hoc Network (IEEE 802.11b)”, in Proceedings of the World Congress on Engineering and Computer Science 2009 (WCECS 2009), Vol 1, October 20-22, 2009, San Francisco, USA.
9. Md. Arafatur Rahman and Farhat Anwar, Jannatul Naeem and Md. Sharif Minhazul Abedin, “A Simulation Based Performance Comparison of Routing Protocol on Mobile Ad-hoc Network (Proactive, Reactive and Hybrid)”, International Conference on Computer and Communication Engineering (ICCCE 2010), Kuala Lumpur, Malaysia, pp. 1-5, Aug. 2010.
10. D. P. Agrawal and Qing-An Zeng, “Introduction to wireless and Mobile Systems,” Brooks/Cole, 2005.
11. P. M. Jawandhiya and S. S. Asole, “Performance analysis of mobility models using routing protocols, traffic models and provides an outcome as to which routing protocol is better,” in *2016 International Conference on Recent Advances and Innovations in Engineering, ICRAIE 2016*, 2017, pp. 0–4.
12. S. Hou, M. Wu, W. Liao, and D. Wang, “Performance comparison of AODV and DSR in MANET test-bed based on Internet of Things,” in *2015 IEEE 82nd Vehicular Technology Conference, VTC Fall 2015 - Proceedings*, 2016, pp. 3–7.
13. V. V. Mandhare and R. C. Thool, “Improving QoS of Mobile Ad-hoc Network Using Cache Update Scheme in Dynamic Source Routing Protocol,” in *Procedia Computer Science*, 2016, vol. 79, pp. 692–699.
14. M. Imran and M. A. Qadeer, “Evaluation Study of Performance Comparison of Topology Based Routing Protocol, AODV and DSDV in MANET,” in 2016 International Conference on Micro-Electronics and *Telecommunication Engineering (ICMETE)*, 2016, pp. 207-211.
15. G. N. Anil, “Semantic Probabilistic Modelling of novel routing Protocol with Implication of Cumulative Routing Attack in Mobile adhoc network,” 2012, vol. 9, no. 1, pp. 340-349.
16. M. Devi, and N. S. Gill. “Novel Algorithm for Enhancing MANET Protocol in Smart Environment”. International Journal of Innovative Technology and Exploring Engineering,8(10),(2019),1830-1835.

17. M. Devi, and N. S. Gill. "Performance Evaluation of Dynamic Source Routing Protocol in Smart Environment". International Journal of Advanced Trends in Computer Science and Engineering, 8(2), March – April 2019, 333-338.

AUTHORS PROFILE

Ms. Munisha has passed Master of Technology from Maharshi Dayanand University, Haryana, India in 2014. She is currently pursuing Ph. D under the supervision of renowned academician and researcher – Professor Nasib Singh Gill of M. D. University. She has published more than 15 research papers in reputed National and International Journals and Conference Proceedings including IEEE. Her main research work focuses on MANETs, IoT, Network Security and Privacy, Big Data Analytics and Data Mining.

Dr. Nasib Singh Gill is at present senior most Professor of Department of Computer Science & Applications, M. D. University, Rohtak, India and is working in the Department since 1990. He has earned his Doctorate in Computer Science in the year 1996 and carried out his Post-Doctoral research at Brunel University, West London during 2001-2002. He is a recipient of Commonwealth Fellowship Award of British Government for the Year 2001. Besides, he also has earned his MBA degree. He has published more than 260 research papers in reputed National & International Journals, Conference Proceedings, Bulletins, Edited Books, and Newspapers. He has authored seven books. He is a Senior Member of IACSIT as well as a fellow of several professional bodies including IETE and CSI. He has been serving as Editorial Board Member, Guest Editor, Reviewer of International/National Journals and a Member of Technical Committee of several International/National Conferences. He has guided so far 8 Ph.D. scholars as well as guiding about 7 more scholars presently in the areas – IoT, Information and Network Security, Computer Networks, Measurement of Component-based Systems, Complexity of Software Systems, Decision Trees, Component-based Testing, Data mining & Data warehousing, and NLP.