Fault Diagnosis and Implementation in Manet

Dr. Pankaj Kumar srivastava,

Professor, ISB&M School of Technology

***Abstract*—** In this paper we describe here the diagnosis the dynamic topology in a faulty environment. In this paper we have optimize that type of network in which less nodes are used to reach source to destination so that data loss are reduced. we have compare the data loss after optimize the new path to reach the source to destination. In dynamic topology nodes are free to move randomly. Mobile stations from an arbitrary topology.

Keywords-VANET, INVANET, IMANET

I. INTRODUCTION

Wireless network is a emerging as a significant aspect of Internet networking [1]. It presents a set o unique issues based on the fact that the only limit to a wireless network is the radio signal strength .There is no wiring to define membership in a network .Wireless technology has helped to simplify networking by enabling multiple computer user to simultaneously share resources in a home or business without additional or intrusive wiring. These resources might include a broadband Internet connection, network printers, data files, and even streaming audio and video. This kind of resource sharing has become more prevalent as computer users have changed their habits from using single, stand-alone computers to working on networks with multiple computers, each with potentially different operating systems and varying peripheral hardware. U.S. Robotics wireless networking products offer a variety of solutions to seamlessly integrate computers, peripherals, and data.A wireless ad-hoc network is a decentralized type of wireless network. The network is ad hoc because it does not rely on a preexisting infrastructure, such as routers in wired networks or access points in managed infrastructure wireless networks. Instead, each node participates in routing by forwarding data for other nodes, and so the determination of which nodes forward data is made dynamically based on the network connectivity. In addition to the classic routing, ad hoc networks can use flooding for forwarding the data. An ad hoc network typically refers to any set of networks where all devices have equal status on a network and are free to associate with any other ad hoc network devices in link range[2]. Very often, ad hoc network refers to a mode of operation of IEEE 802.11 wireless networks. It also refers to a network device's ability to maintain link status information for any number of devices in a 1 link range, and thus this is most often a *Layer 2* activity. Because this is only a Layer 2 activity, ad hoc networks alone may not support a routable IP network environment without additional *Layer 2*or*Layer 3* capabilities.

II. TYPE OF WIRELESS AD HOC NETWORK

Wireless ad hoc networks can be further classified by their application:

1. mobile ad-hoc networks (MANET)
2. wireless mesh networks (WMN)
3. wireless sensor networks (WSN)

A. MANET

MANETs are a kind of wireless ad-hoc networks that usually has a routable networking environment on top of a Link Layer ad hoc network. A mobile ad-hoc network (MANET) is a self-configuring infrastructure less network of mobile devices connected by wireless links. Ad hoc is Latin and means "for this purpose". Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router.

The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic [5]. Such networks may operate by themselves or may be connected to the larger Internet. In mobile ad-hoc networks where there is no infrastructure support as is the case with wireless networks, and since a destination node might be out of range of a source node transmitting packets; a routing procedure is always needed to find a path so as to forward the packets appropriately between the source and the destination. Within cell, a base station can reach all mobile nodes without routing via broadcast in common wireless networks. In the case of ad-hoc networks, each node must be able to forward data for other nodes. This creates additional problems along with the problems of dynamic topology which is unpredictable connectivity changes [6].

B. WIRELESS MESH NETWORK

A wireless mesh network can be seen as a special type of wireless ad-hoc network. A wireless mesh network often has a more planned configuration, and may be deployed to provide dynamic and cost effective connectivity over a certain geographic area.[7] An ad-hoc network, on the other hand, is formed ad hoc when wireless devices come within communication range of each other. The mesh routers may be mobile, and be moved according to specific demands arising in the network. Often the mesh routers are not limited in terms of resources compared to other nodes in the network and thus can be exploited to perform more resource intensive functions. In this way, the wireless mesh network differs from an ad-hoc network, since these nodes are often constrained by resources. Mesh networking (topology) is a type of networking where each node must not only capture and disseminate its own data, but also serve as a relay for other nodes, that is, it must collaborate to propagate the data in the network.

C. WIRELESS SENSOR NETWORK

A wireless sensor network (WSN) consists of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants and to cooperatively pass their data through the network to a main location. The more modern networks are bi-directional, also enabling control of sensor activity. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on [4]. The WSN is built of "nodes"– from a few to several hundreds or even thousands, where each node is connected to one sensor.

III.TYPES OF MANET

MANETs are of following types

3.1Vehicular Ad-Hoc Networks *(VANETs)*: This[7] type of MANET is mainly used to communicate between the vehicles and the roadside equipments or just to communicate among the vehicles. A Vehicular Ad-Hoc Network or VANET is a technology that uses moving cars as nodes in a network to create a mobile network. VANET turns every participating car into a wireless router or node, allowing cars approximately 100 to 300 metres of each other to connect and, in turn, create a network with a wide range. As cars fall out of the signal range and drop out of the network, other cars can join in, connecting vehicles to one another so that a mobile Internet is created. It is estimated that the first systems that will integrate this technology are police and fire vehicles to communicate with each other for safety purposes. We can understand VANETs as subset of MANET and best example of VANET is Bus System of any University which are connected. These buses are moving in different parts of city to pick or drop students if they are connected, make a Ad hoc Network. With the Internet becoming an increasingly significant part of our lives, the dream of a WiFi-enabled city is becoming closer and closer to reality.

3.2 Intelligent vehicular ad hoc networks **(InVANETs)**: It includes artificial intelligence that aids the vehicles to behave in intelligent manner during drunken driving, collision etc. Intelligent vehicular ad-hoc networks (InVANETs) use WiFi IEEE 802.11p (WAVE standard)and WiMAX IEEE 802.16 for easy and effective communication between vehicles with dynamic mobility. Effective measures such as media communication between vehicles can be enabled as well methods to track automotive vehicles.

InVANET is not foreseen to replace current mobile (cellular phone) communication standards. [5]InVANET can be used as part of automotive electronics, which has to identify an optimally minimal path for navigation with minimal traffic intensity. The system can also be used as a city guide to locate and identify landmarks in a new city. Communication capabilities in vehicles are the basis of an envisioned InVANET or intelligent transportation systems (ITS). Vehicles are enabled to communicate among themselves (vehicle-to-vehicle, V2V) and via roadside access points (vehicle-to-roadside, V2R). Vehicular communication is expected to contribute to safer and more efficient roads by providing timely information to drivers, and also to make travel more convenient.

***3.3 Internet Based Mobile Ad hoc Networks* (iMANET):** This type of ad-hoc network connects mobile nodes with the internet gateway node. Here the ad-hoc routing algorithms cannot be applied directly.

IV.PROBLEM FORMULATION

A node becomes faulty because of battery discharge, crash and limitation in age. An important problem in designing hosts MANET is handling failure of nodes is the distributed self diagnosis problem. In distributed self-diagnosis system each mobile node is able to diagnose the status of all nodes and knows the correct status of other nodes in the network.[7]

Each node in the system can be in one of two states faulty or fault-free. Faults can be categorized based on their duration, how it behaves after failure and occurrence of fault during diagnosis session.[9]

A.Based on the Duration

Based on duration faults can be of three types:

***4.1Transient fault*:** A transient fault can disappear without any visible event it appears in a network for short time. The recovery of transient faults from system is addressed using repeated-round techniques. A probabilistic model used for the action of faulty periods, and a fault analysis is used to obtain the optimum retry period. A transient fault is a fault that is no longer present if power is disconnected for a short time. Many faults in overhead power lines are transient in nature. At the occurrence of a fault power system protection operates to isolate area of the fault. A transient fault will then clear and the power line can be returned to service. In electricity transmission and distribution systems an automatic reclose function is commonly used on overhead lines to attempt to restore power in the event of a transient fault. This functionality is not as common on underground systems as faults there are typically of a persistent nature. Transient faults may still cause damage both at the site of the original fault or elsewhere in the network as fault current is generated.

4.2. Intermittent fault: It is problematic type of transient fault; we can't predict its appearance and disappearance in the network. An intermittent fault is occurred by several factors, some may be erect randomly, which occur simultaneously. These factors can only be identified when malfunction is occurred. Intermittent faults are difficult to identify and repair. An intermittent fault, often called simply an "intermittent", is a malfunction of a device or system that occurs at intervals, usually irregular, in a device or system that functions normally at other times. Intermittent faults are common to all branches of technology, including computer software. An intermittent fault is caused by several contributing factors, some of which may be effectively random, which occur simultaneously. The more complex the system or mechanism involved, the greater the likelihood of an intermittent fault. Intermittent faults are notoriously difficult to identify and repair "troubleshoot" because each individual factor does not create the problem alone, so the factors can only be identified while the malfunction is actually occurring. The person capable of identifying and solving the problem is seldom the usual operator. Because the timing of the malfunction is unpredictable, and both device or system downtime and engineers' time incur cost, the fault is often simply tolerated if not too frequent unless it causes unacceptable problems or dangers. For example, some intermittent faults in medical life support equipment can kill a patient. If an intermittent fault occurs for long enough during troubleshooting, it can be identified and resolved in the usual way.

***4.3 Permanent fault*:** Once it appears in network it remains until it removed and repaired by some external administrator. Permanent faults are simpler to deal.

B. Based on the Behavior

Based on behavior faults can be of two types:

***4.5 Soft Fault*:** Soft faulted units can communicate with its neighbors but with unexpected behaviors and always give undesirable response.

4.6 Hard fault: Hard faulted units cannot communicate with its neighbors. It neither sends nor receives any information from the network.

C.Based on the Occurrence

Based on occurrence faults can be of two types:

***4.7 Static fault*:** All faulty nodes be faulty from the starting of diagnosis session.
The fault-free node can't be faulty during diagnosis session.

4.8. Dynamic fault: Fault-free node may become faulty during diagnosis session. It is hard 5to diagnosis because any node may fail after it diagnosed fault-free by any fault-free node.

D. Other Faults

Another type of fault is Byzantine fault which fail the components of a system in arbitrary ways by processing requests incorrectly. It is of two types:

4.8 Omission failures: This type of failure doesn't response for a request, e.g., crash, failing to receive a request, or failing to send a response.

4.9. Commission failures: This type of failure may respond in any unpredictable way, e.g., processing a request incorrectly, corrupting local state, and/or sending an incorrect or inconsistent response to a request. Hardware Failures: Hardware failures can be described as failures that occur in mechanisms like disks or storage media. Hardware failures tend to offset other failures. It is recommended to utilize platforms that can monitor internal temperatures, as well as trigger alarms accordingly. With random access memories, error correcting codes (ECCs) can be utilized to identify and correct single errors and to identify two-bit errors.

Software Failures: Determining the reason of a system outage can be quite intricate. Virus protection defects can cause system outages. Often, incorrect system configuration can also lead to system failures.

***4.10 Network Failures*:** Any changes to the network design or topology of a layer of the protocol stack can have an impact on the entire network. It is therefore better to assess each layer when making any network changes.

E. Fault diagnosis

Fault identification is one of the important part in many protocols. When the actual behavior is deviated by system or nodes of the system, a diagnosis function started to determine which node performed abnormal behavior that is called diagnosis. Diagnosis is classified based on the occurrence of fault. It simply can be classified as static diagnosis and dynamic diagnosis.

In static diagnosis, the fault does not occur during the diagnosis session; they already appeared in the networks. In dynamic diagnosis, the faults can occur during the diagnosis session, it is difficult to handle because node can be faulty after it has been diagnosed as fault-free by other node. We considered the problem of dynamic failures of node and remove those nodes from the network. Previously all work has dealt with the static fault situation where node cannot be faulty during diagnosis period.

IV. ANALYSIS OF THE PROBLEM AND INPLEMENTATION

In this figure we can see that the node moves anywhere in lxl area .the souce node send the request .All node generates the hello message to start up the time.

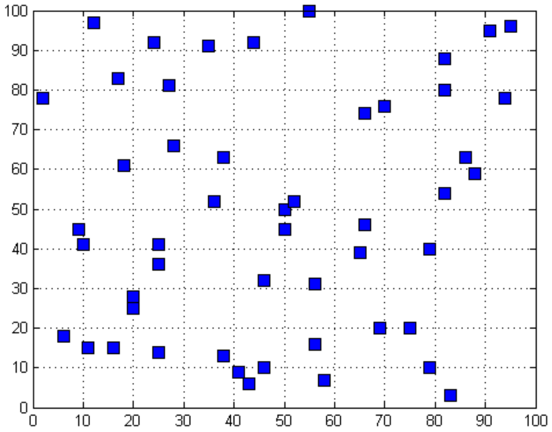

Fig.1

2. In this figure we can see that the actual path is generated between the source and the destination .The minimum number of nodes is 1and the maximum number of nodes is 50 is used when the actual path is generated. For measure the distance between the nodes we can use the formula mentioned in the proposed idea .in this sceanario nodes moves anywhere in lxl area. the nodes picked randomly to generate the path. the number of nodes effected on the transmission range of the data packet .when the actual path is generated between source and destination we calculated the data loss. The data loss is 0.7943 .The number of nodes effected the transmission of the data.

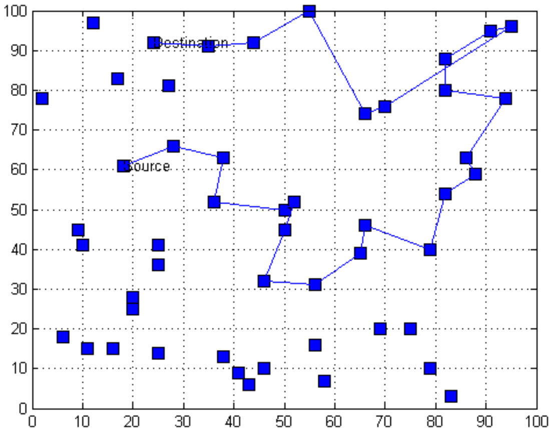

Fig.2

3. In the figure 3we can see that new path is optimized between the source and the destination .the new optimize path the less number of nodes than the actual path establish between the source and destination. After reduction the number of nodes the data loss is 0.3112.This data loss is known as a new data loss .the data loss which is computed when the actual path is establishes is known as a old data loss.

If we compare the new data loss with the old data loss .then we can see that the new data loss is less than the old data loss .we can say that the number of nodes effect on the transmission of the packets.

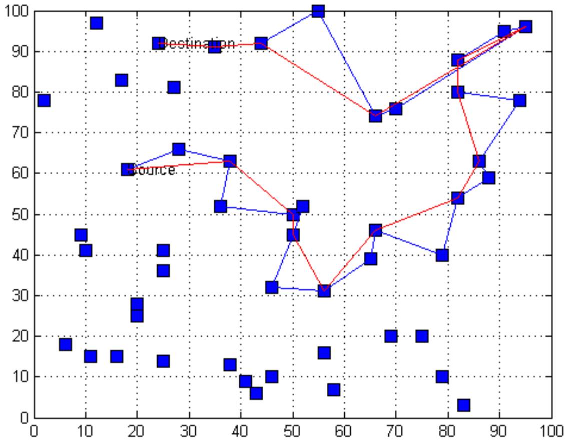

Fig . 3

V. CONCLUSION

In this paper, we discussed the diagnosis a dynamic topology is more complex than the static topology. We can optimize the reliable path between the source and the destination. In our research we can compare the old data loss with the new data loss .The old data loss is come from the actual path is establish source and the node. We can conclude from our research is that the number of nodes affect on the transmission of the packets. We can optimize that type of path in which less number of nodes is used that gives good throuput.

REFERENCES

1. *Clare ,loren p, GregoryJ pottie and jonathan agre (1999)" self organizing distributed sensor networks "proc accessories 99*
2. *E. M. Royer and C.-K. Toh, "A Review of Current Routing Protocols for Ad-Hoc Mobile Wireless Networks", IEEE Personal Communications Magazine, April 1999, pp. 46-55.*
3. *Imrich Chlamtac , Marco Conti , Jennifer J.-N. Liu" Mobile ad hoc networking: imperatives and challenges" Elsevier, Ad Hoc Networks 1 (2003) 13–64.*
4. *] Fujian Qin and Youyuan Liu, "Multipath Based QoS Routing in MANET", Journal of Networks, vol. 4, no. 8, October 2009*
5. *Jinyang Li, Charles Blake, Douglas S. J. De Couto, Hu Imm Lee, and Robert Morris*
6. *Capacity of Ad Hoc Wireless Networks, in the proceedings of the 7th ACM International*
7. *Laura Marie Feeny .Ataxomony for routing protocols in mobile ad hoc networks technical report, institute of computer surden 1999*
8. *M. Elhadef, A. Boukerche, H. Elkadiki, Diagnosing mobile ad hoc networks: two distributed comparison-based self-diagnosis protocols, in: Proceedings of the 4th ACM International Workshop on Mobility Management and Wireless Access Protocols, Terre[3]*
9. *]R. Ahlswede, N. Cai, S. Y. R. Li, and R. W. Yeung. Network information flow. Information Theory, IEEE Transactions on, 46(4):1204–1216, 2000.*
10. *Ramasubramanian, Z. J. Haas, and E. G. Sirer. SHARP: A Hybrid Adaptive Routing Protocol for Mobile Ad Hoc Networks. In ACM MobiHoc*

.