ISSN: 2348 - 2117

International Journal of Engineering Technology and Computer Research (IJETCR)

Available Online at www.ijetcr.org

Volume 9; Issue 6; November-December; 2021; Page No. 01-10

Mobile Adhoc Network(MANETS) : Power Aware and Security Related Issues

Garima Chaudhary[1], Roshan Jain[2]

[1]Research Scholar Rajasthan College of Engineering for Women

[2]Assistant professor Rajasthan College of Engineering for Women

Abstract

Because of the mobility of the nodes, as well as the use of unstable wireless channels for data transmission, it is well-known that frequent connection failures occur in mobile ad-hoc networks. In order to achieve improved transmission in ad-hoc networks, the majority of the research is focused on multipath routing protocols, which are becoming more popular. There is a study here that discusses the provision of a Multicasting routing technique in MANET such that the whole transmission is energy efficient. The primary purpose of the suggested approach was to establish which multicasting routing mechanism was the most energy efficient in order to ensure that the whole transmission in MANET was as energy efficient as possible. After all of the research and tests are carried out in a novel manner, it is discovered that, first, a path that leads to the target is identified, and then data is sent from the source in an extremely efficient manner. It has also been observed that practically all of the mobile nodes have extremely limited battery capacity, making it evident and essential to utilise energy effectively in a MANET. The focus of this work is on introducing a power-aware multicast routing protocol (PMRP) in order to achieve improved mobility prediction for MANETs, which is the subject of the study. In addition, a specific subset of pathways has been identified that will contribute to the improvement of the stability and dependability of routes. In the event that a node has a significant amount of data packets remaining to broadcast, the global positioning system (GPS) is used to determine the location of the node. Detailed information regarding the position, velocity, and direction of the mobile nodes is provided in this section. It is therefore necessary to use this same information in order to calculate the link expiry time (LET) that exists between the two mobile nodes that have been linked. As observed, every destination node makes a point of selecting the routing path that has a short LET and utilises the same as the route expiry time when route discovery is carried out on the network (RET). It can be observed that the destination nodes check to see if they have certain possible routes and then choose the one with the longest RET to use as their main routing path. The same path is then utilised for the source node as it is for the routes that have been chosen. The suggested system in this paper makes use of OMCRM, and the results of testing have shown that the proposed systems are effective in reducing delay time and are efficient in packet transfers. Another essential feature that has been accomplished is that route rescuer has been implemented, which has eliminated the delay and enhanced both the time and the efficiency with which the packets are being transmitted.

Keywords:- MANET (Mobile Adhoc Network), Multipath Routing Mechanism, routing protocols

1. INTRODUCTION

When it comes to the interaction with the router, an ad-hoc network is also characterised as a packet switching network that is dependant on wireless connections. This may be classified as dynamic because of the mobility of the routers and the changes in characteristics of the radio channels used to transmit the information. There is an extra obstacle to doing multicasting in ad hoc networks

as opposed to the internet, since there is a demand to make best use of several resources at the same time, which is more difficult to do than on the internet. [7]

When we speak about classic multicast protocols, it is important to remember that they were originally suggested for wired infrastructure. However, these systems are incapable of dealing with topologies that change on the fly as data is being sent via the network. As a result, it becomes abundantly evident that they cannot be employed in ad hoc networks at some point. In wireless ad hoc networks, there are two kinds of multicast protocols to choose from: tree-based and mesh-based protocols. Because of its simplicity, tree-based multicast routing is widely used and attractive to programmers and network administrators. The purpose of this study is to discover the most energy-efficient multicasting routing technique for MANET transmission, with the ultimate objective of making the whole transmission as energy-efficient as possible.

It has also been discovered that all of the mobile hubs have less battery management, making it obvious and very required to use energy in a MANET in an effective manner. Further research is around the development of a power-aware multicast routing protocol in order to meet the high level of adaptability that is expected of MANETs in the future. There has also been a special subset of methods that have been developed to improve the consistency and unwavering quality of courses. If there is a hub that has a significant amount of capacity remaining to send information bundles, the hub may also make use of the global positioning system to get location data. This contains detailed information regarding the location, speed, and bearing of the interchangeable hubs in real time. Using comparable information, the calculation of the link expiration time that is in the centre of the two related portable hubs is carried out after the conclusion of the previous step. [8] [10] The fact that each objective hub makes it a point to choose the most direct route that has a short LET and utilises the same as the RET has been observed during course disclosure, among other things.

MANET research has made significant advances in the realm of catastrophe avoidance. In terms of application, there are several MANET versions, such as VANET (Vehicle Ad-hoc network) and UWMANET (Under Water Mobile Ad-hoc Network). For disaster prevention and rescue activities in the modern world, underwater wireless mobile ad hoc networks (MANETs) are becoming more important. In the case of a calamity, MENT communication may be quite beneficial. MANET has numerous drawbacks, including high power consumption, slow response times and limited scalability [1]. The classic MANET, on the other hand, has a lower level of security because of its thick medium and the presence of more attackers.

These intruders may take a long time to penetrate the network and interact with its resources, causing network latency [2]. As a result, gathered data is sent to the surface station through underwater sensors. When referring to the MAN, four distinct terms come to mind: A network may be deployed under water, which is dense, mobile, ad-hoc, and a few hubs [3]. [4] The term "network" refers to a pool of hubs, not to a network of hubs. MANET [4, 5] is the name given to this network because to its characteristics as an underwater mobile ad hoc network. Many gadgets can communicate with the MANET network.

2. LITERATURE REVIEW AND KNOWLEDGE GAP

Protocols and algorithms are discussed in this part, as well as communication concerns, obstacles, and solutions. According to the previous research, these efforts may be used to communicate constrained environments (in simulation), flood-based catastrophes, and undersea abrupt movements in MANET disaster response applications. SO-AODV was the term given by Singh and Gupta in [2020] [3] to a solution for DRA-based problems. Ad-hoc on-demand distance vector routing over AODV with Quality of Service (QoS) for Disaster Response Applications is the recommended solution (DRA). Pigeons Swarm Optimization uncovers the quickest route (PiSO). In addition, PiSO decreases the number of hops in the shortest possible path. This approach uses "Hello" packets to verify user

identity. To ensure the confidentiality of event communications, we use the Ciphertext Stealing Technique (CST) in conjunction with a public key based on QuVanstone Elliptic Curve Cryptography (qV-ECC). The public key is generated by the qV-ECC. To assess and compare NS2 experimental with AODV for many metrics, such as PDR and throughput and end-to-end latency, etc. An "Energy-Efficient Multipronged Reliable Strategy guaranteeing Secure and Scalable QoS across Disaster Response Apps," as described by Singh and Gupta in [2020] [4], studied an AODV protocol for DRA-based applications that was cognizant of power use. MANET energy efficiency and security was addressed by the writers. Enhancements such as security and energy efficiency have been added to the conventional AODV approach shown here (through residual energy concept). The proposed method uses a key generation approach, i.e. qu-Vanstone ECC-based public-key cryptography, to authenticate a "hello" message using LDW and to encrypt event messages using CST (Ciphertext Stealing Technique).

UWMANET, a three-dimensional ad hoc network, was built using the E2 - SCRP protocol, which Yadav and Kush proposed and developed in [2019] [5]. UWMANET is a 3D underwater acoustic MANET, a unique network environment into the water (UWMANET). In order to keep track of underwater activities, sensors and recording devices are positioned in three dimensions at various depths. When it comes to energy efficiency, type two fuzzy-based multilayered approaches are used, while CST is utilised to meet security requirements. PDR, power consumption, security, end-to-end delay, and throughput, for example, are all investigated in a simulated environment to verify the proposed protocol's authenticity. Using a tiered approach for occasion inclusion.

Yu et al. [2016] [6] developed a method for organising unbalanced clusters of data. Various depths of the submerged organization's power consumption during data transmission are being investigated. It is structured in a variety of ways, with multiple levels and a variety of distinct groups. The system develops deferral from beginning to end and increases energy usage under this structure. Using portable hubs for data collection.

Ghoreyshi et al. in [2016] [7] advocated a hop-constrained clustering approach in underwater sensor organisations. This technique is used in the case of thick underwater sensors. There is a primary focus on speeding up data collecting and reducing power consumption. The clustering measure is used to collect data. Moving underwater utility vehicles will use sensors to collect data even farther ahead of land-based ones. In order to gather information from sensor nodes, moving utility vehicles choose the best possible route to be close to the sensor nodes. Sensor data collection and planning for the future are critical. However, there is no evidence to support the use of large-scale networks to address these issues. Flexible edge components were proposed in

Cai and colleagues [2019] [8] by, which allow for a true portable replica. In this case, the utility vehicle's speed and adaptability are two of the most important factors for obtaining information about ocean depth. Factual data is communicated through a combination of auditory and magnetic links. It restricts the amount of time available for data collection. Other execution metrics, such as network lifespan, PDR, and throughput, are also changed throughout the whole business. Since long-range communication necessitates large amounts of data to be gathered, the suggested approach isn't appropriate for use in emergency circumstances or in environments where scalability is an issue. When the network is overburdened with data, the transmission time of that data is significantly increased.

A power-aware routing system was used by Zhu and Wei in [2018] [9] to enable inconsistent groups for networks depending on sensing devices. An asymmetrical group, communication routing and modification and maintenance of the cluster are all covered in this article. As a result of examining the information dissemination and compilation processes, this paper identifies hotspot issues. a new multi-pronged optimization technique is proposed to deal with the costs and incentives for cluster leaders (multi incoming link point). The forward ratio and the residual power of

the sensor nodes were assessed using this approach. A good solution to hotspots is inconsistent clustering, although this doesn't solve all of the problems associated with grouping. There is a method called ADAN-BC.

Khan and Dwivedi discovered in [2018] [10], where the nodes may create big gaps in the operating region. Sensor placement in the suggested strategy may be helped by network mobility measures. For better integration in the organisation, portable sensor hubs are organised haphazardly. Groups are formed based on the amount of available space and power among mobile sensor nodes (residual).

According to Wang and Bang [2017] [11], an underwater sensing company may benefit from a node tumbling approach. It addresses the problem of network connection and coverage, as well as how an organisation is set up. Anchored hubs make up the structure. The sensor hubs are strewn around the ocean floor in an erratic fashion. Using an advanced three-dimensional circle pressing method, the primary sink hub cluster may be easily identified. Secondly, sink hub availability is evaluated, and thirdly, sink hubs are used to fill in any gaps in the network. Large-scale 3D underwater networks do not benefit from the sinking calculation of the hubs.

In [2018] [12], Khosravi and Rostami introduced the SDV fusion technology. Using this communication mechanism, two challenges related to water depth-based sensor networks are highlighted (UWSN). Listed below are the details: The safety of a route or connection, as well as the volume of communication. This article aims to improve undersea system efficiency, power usage, dependability, and data transmission ratio. The vector-forwarding approach improves the routing process significantly. Scalability is a major issue with this method.

3. Routing in Ad-Hoc Networks

Mobile Ad-Hoc Networks (MANETS) are defined as peer-to-peer, multi-hop networks that do not rely on any pre-existing infrastructure and operate in the field. The usage of intermediate hosts to route communications is required when a network host desires to connect with another network host that is outside of the network host's radio range. Because of this, routing capability must be included into the mobile hosts themselves.

In wired networks, routing algorithms are classified as either link state based protocols (for example, OSPF Open Short Path First) or distance vector based protocols (for example, RIP) (e.g. RIP Routing Information Protocol). The Dijkstra algorithm is used by the link state protocols. All network routers get link state advertising, which are transmitted to them all. In order to compute the shortest path to each node, the routers collect link-state information, which is then utilised in conjunction with the Dijkstra algorithm. It is the Bellman-Ford algorithm that is used in distance vector-based protocols.

Routing tables must be distributed solely to neighbouring routers in order for this to be accomplished. This approach may be used to retain and update routing information in a wireless network when there is a low degree of mobility, as shown by the Bellman-Ford example. With the introduction of high levels of mobility, Bellman-Ford protocols are unable to keep up with the frequent connection changes, which results in poor network convergence and limited communication throughput. When developing routing protocols for mobile ad-hoc networks, it is important to consider the following considerations: -

(1) Dispersed operation: Because there is no central hierarchy of routers, routing must be distributed across the nodes that are participating in the network.

(2) Loop-freedom: Attempt to prevent route discovery or maintenance procedures from revolving from node to node endlessly Route discovery and maintenance:

(3) Demand-based operation vs. proactive operation: - Should routes be determined when a source requests them, or should a pre-defined current database of routes be provided across nodes? Both techniques are used in adhoc networks, and protocols may be classified as belonging to either of these two groups.

(4) Operation during the "sleep" period: As part of the effort to save energy, it is preferable that when

a network node is not actively engaging, it has the ability to enter a "sleep" state. The routing protocol should be able to tolerate such intervals without having a significant influence on the overall performance of the system.

Manets security problem and proposed solution

Because we are aware that MANETs do not have a centralised administration or previous structure, the security risks that exist in MANETs are distinct from those that occur in traditional networks. MANETs are more vulnerable to assaults because of the use of wireless connectivity. Hackers will find it easy to eavesdrop on conversations and acquire access to sensitive information. As a result, they find it less difficult to join to or disconnect from a wireless network since no physical connection is necessary. Furthermore, they may actively target a network in order to remove messages, insert bogus packets, or impersonate a node.. The availability, integrity, authentication, and nonrepudiation goals of the network are jeopardised as a result of this. Nodes that have been compromised may potentially launch attacks from inside a network. The majority of routing algorithms being suggested now do not include strategies to guard against such assaults. In this section, we discuss techniques that are relevant for authentication, key distribution, intrusion detection, and rerouting in the event of Byzantine failures in MANETs, among other things.

4. RESULT EXPLANATION

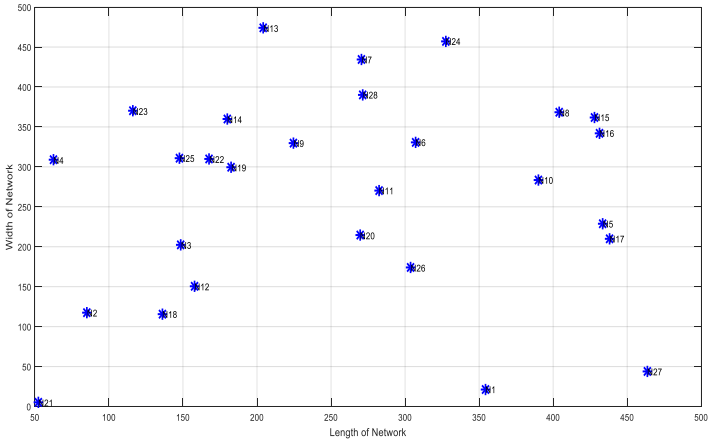

Fig 1: Network Creation

Figure 1 depicts the establishment of a network in which the nodes are deployed in a network with a length of 700 metres in length and breadth of 700 metres, and a total area of 1000 metres in length and width. The simulation is accomplished via the use of MATLAB programming.

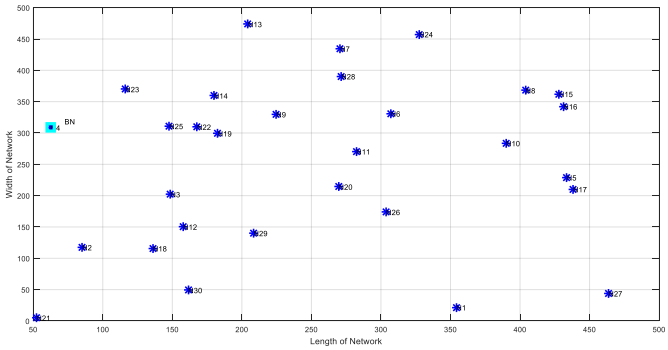

Fig 2: Identification of black hole node

The fig 2 shows the black hole node in the cyan color and also it acts as a malicious node which will generate the fake route path

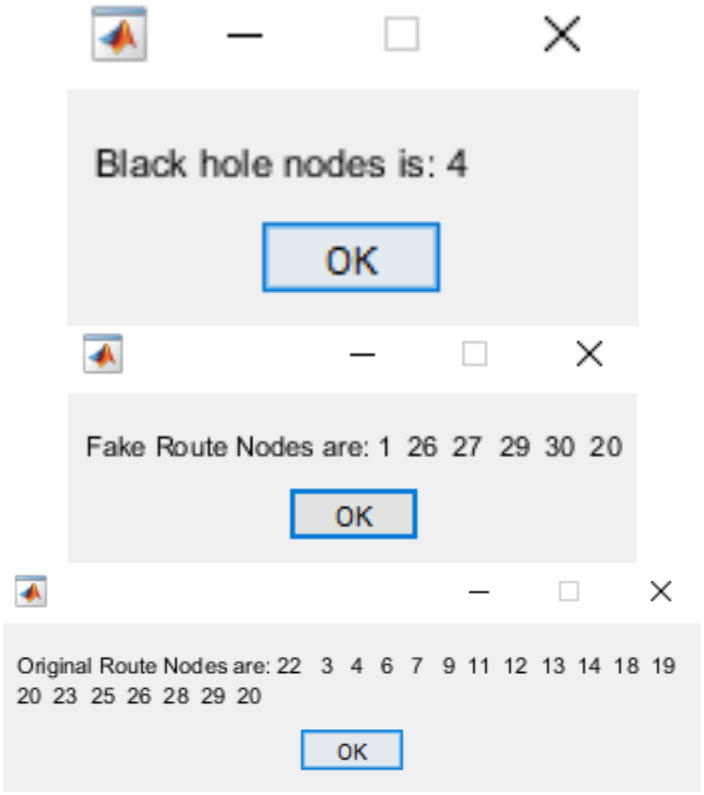

Fig 3: Node ids (Black Hole node, Fake Rout, Original Route after Mitigating)

The node ids for the black hole node, as well as the false route node ids generated by the malicious node in the presence of the attack, are shown in Fig 3. The original node ids, which are obtained after mitigating the effects of the attack in the sensor network, are also shown in Fig 3.

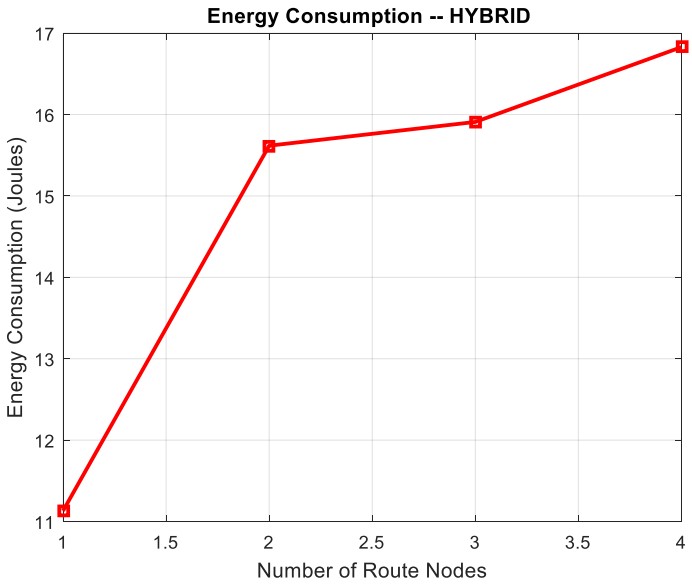

Fig 4: Energy consumption

Figure 4 depicts the energy consumption in relation to the total number of nodes executing or participating in the route, and it demonstrates that the hybrid strategy is capable of achieving lower energy consumption, which will result in longer node lifespans.

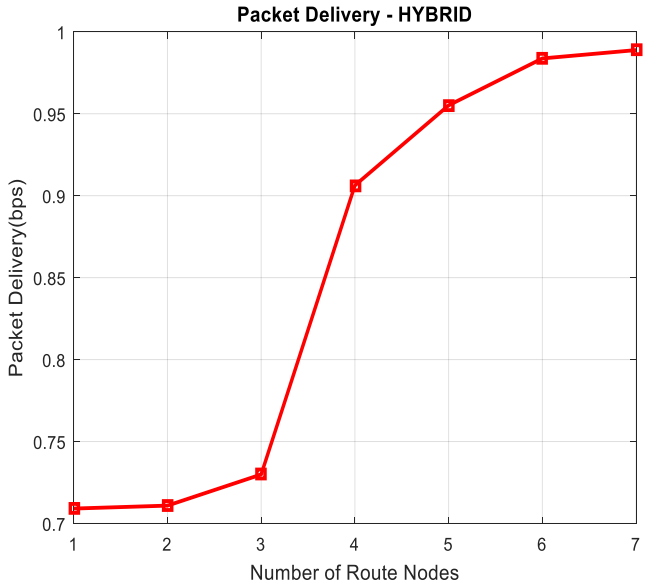

Fig 5: Packet Delivery

As shown in Fig 5, the network's packet delivery is measured in terms of probability, demonstrating that the proposed approach can achieve high packet delivery rates in terms of successful packet deliveries. Furthermore, the graph is closest to one, demonstrating that the proposed system can achieve high packet delivery rates in terms of successful packet deliveries.

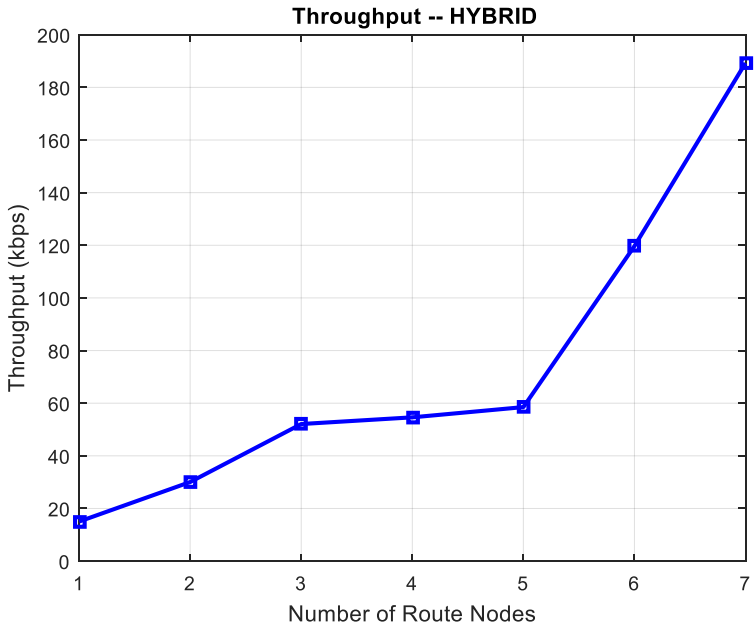

Fig 6: Throughput

In Fig. 6, we can see the network throughput measured in kilobits per second, demonstrating that the proposed approach is capable of achieving high network throughput. This indicates that the network is delivering packets from source to destination in an attack-free environment, which is accomplished in an efficient manner by our proposed approach.

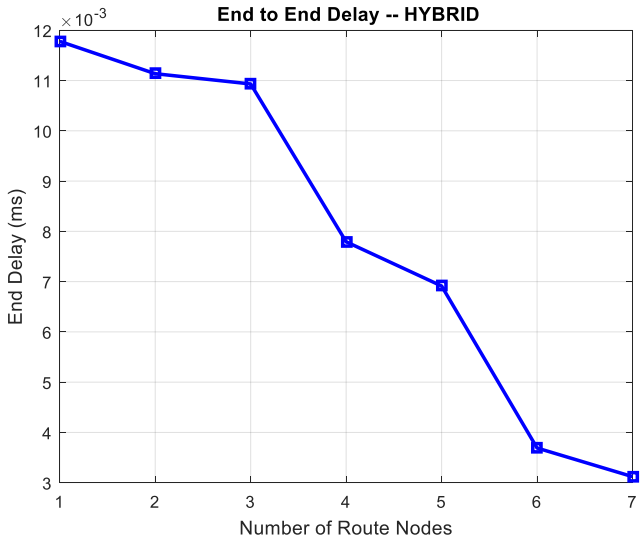

Fig 7: End Delay

The end delay of the network, which must be low in order to achieve high packet deliveries and low packet losses, is shown in Fig. 7, demonstrating that the proposed system is capable of achieving a lower end delay from the source to the destination.

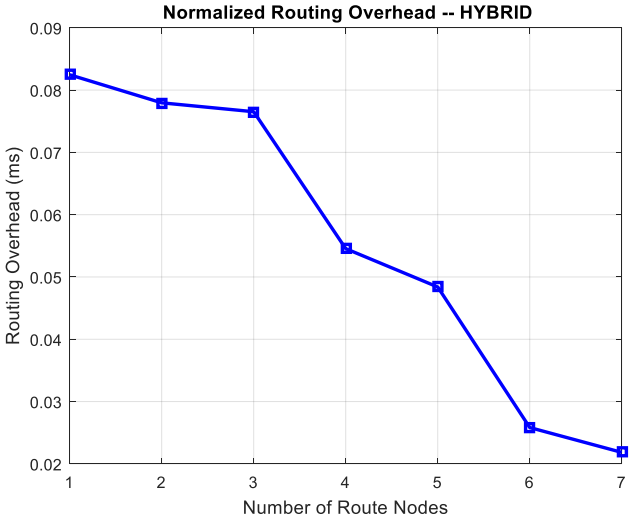

Fig 8: Routing Overhead

The fig 8 displays the routing overhead of the network which is one of the essential parameter in the sensor network which must be less for the low efficient overhead for the fewer collisions of the packets between the nodes in the sensor networks. This parameters must be fewer as the number of routing nodes grows.

Conclusion

MANETs are made up of mobile nodes that are linked via multihop communications channels or radio connections to form a network. Nodes, which are movable platforms that may move at any speed in any direction and assemble themselves randomly, make up a MANET. Nodes can communicate with one another and with the rest of the network. The nodes in the network perform a variety of tasks, including serving as routers, clients, and servers.

This group of nodes is restricted in terms of its power consumption, bandwidth, and computing capability. Traditional techniques to security in MANETs are ineffective due to the specific features and limits of the network. It is frequently

too inefficient to employ traditional authentication, key distribution, and intrusion detection techniques on devices with limited resources in MANETs since they are too resource-intensive. In this research, we propose to integrate efficient cryptographic algorithms with a distributed intrusion-detection system to create a more effective intrusion detection system. Additionally, we recommend that distributed Certifying Authorities (CAs) be used in conjunction with per-packet and per-hop authentication to solve the relevant security challenges.

References

1. K. Singh, and A. K. Yadav. A Qualitative and Quantitative Analysis of Routing Protocols in MANET, International Journal of Advanced Research in Computer and Communication Engineering, 5(7), 2016.
2. K. Singh, and R. Gupta. Comparative Assessment and Performance Analysis of Numerous Mobile Ad-Hoc Network Routing Protocols, Journal of Computational and Theoretical Nanoscience, Vol. 16, pp. 3906–3911, 2019.
3. K. Singh, and R. Gupta. SO-AODV: A Secure and Optimized Ad-Hoc On-Demand Distance Vector Routing Protocol over AODV with Quality Metrics for Disaster Response Applications, To be Published in Journal of Information and Technology Reserch (JITR), 14(3), by IGI global publications, US, 2020.
4. K. Singh, and R. Gupta. E 2S-AODV: An Energy Efficient Multipronged Reliable Strategy ensuring Secure and Scalable QoS over Disaster Response Applications, International Journal of Advanced Trends in Computer Science and Engineering, Volume 9, No.4, July – August 2020.
5. A. K. Yadav, and A. Kush. E 2 -SCRP: An Energy Efficient Secure Cluster based Routing Protocol for 3D Underwater Acoustic MANET (UWMANET), International Journal of Innovative Technology and Exploring Engineering, ISSN: 2278-3075, 8(11), 2019.
6. Shanen Yu, Shuai Liu, Peng Jiang, "A High-Efficiency Uneven Cluster Deployment based on Network Layered for Event Coverage in UWSNs", Sensors Basel, MDPI, Vol. 16, Issue.2, PP. 2016.
7. Seyed Mohammed Ghoreyshi, AlirezaShahrabi, TuleenBoutaleb, Mohsen Khalily, "Mobile Data Gathering with Hop-Constrained Clustering in Underwater Sensor Networks", IEEE Access, vol.7, pp. 21118-21132.
8. S. Cai, Y. Zhu, T. Wang, G. Xu, A. Liu and X. Liu, "Data Collection in Underwater Sensor Networks based on Mobile Edge Computing," in IEEE Access, vol. 7, pp. 65357-65367, 2019, doi: 10.1109/ACCESS.2019.2918213.
9. Fang Zhu, Junfang Wei, "An Energy Efficient Routing Protocol Based on Layers and Unequal Clusters in Underwater Wireless Sensor Networks". Journal of Sensors. 2018. 1-10.
10. Guilista Khan, Rakesh Kumar Dwivedi, "Autonomous Deployment and Adjustment of Nodes in UWSN to Achieve Blanket Coverage (ADANBC)", International Journal of Information Technology, PP. 1-10, 2018.
11. Zhongsi Wang, Bang Wang, "A Novel Node Sinking Algorithm for 3D Coverage and Connectivity in Underwater Sensor Networks", Ad Hoc Networks, Vol. 56, PP. 43-35, 2017.
12. Mohammed Reza Khosravi, HmaidHabibRostami, "Efficient Routing for Dense UWSNs with High-Speed Mobile Nodes using Spherical Divisions", The Journal of Supercomputing, Vol. 74, Issue 2, PP. 696-716, 2018.
13. Gomathi R.M, J Martin Leo Manickam, "Energy Efficient Shortest Path Routing Protocol for Underwater Acoustic Wireless Sensor Network", Wireless Personal Communications, Vol.98, Issue.4, PP. 1-14, 2017
14. R.M. Gomathi, J. Martin Leo Manickam, "Energy Efficient Static Node Selection in Underwater Acoustic Wireless Sensor Network", Wireless Personal Communications, pp. 1-19.
15. ChhaganLal, Roberto Petroccia, KonstantinosPelekanakis, Mauro Conti, Joao Alves, "Toward the Development of Secure Underwater Acoustic networks", IEEE Journal

of Oceanic Engineering, IEEE Journal of Oceanic Engineering, Vol.12, issue.4, PP. 1075-1087, 2017.
16. Yue Zhao, Bo Tian, Zhouguo Chen, Yiming Liu, Jianwei Ding, "An Energy-Efficient Key Agreement Mechanism for Underwater Sensor Networks", Lecture Notes in Electrical Engineering, Vol. 450, PP.1-13, 2017.
17. Jing Yan, Xian Yang, XiaoyuanLuo, Calian Chen, "Energy Efficient Data Collection over AUV-assisted Underwater Acoustic Sensor Network", IEEE Systems Journal, PP. 1-12, 2018.
18. Bisen, Dhananjay & Sharma, Sanjeev. (2017). An enhanced performance through agent-based secure approach for mobile ad hoc networks. International Journal of Electronics. 105. 1-21. 10.1080/00207217.2017.1355019.
19. T. S. Vamsi, P. Kumar, and T. Sruthi. Performance Analysis of AODV Routing Protocol in MANET under Blackhole Attack, Journal of Engineering Research and Application, ISSN: 2248-9622, 9(5), pp. 58-63, 2019