International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
DOI: https://doi.org/10.17762/ijritcc.v11i9s.7429
***Article Received**: 10 May 2023 **Revised:** 29 June 2023 **Accepted:** 26 July 2023*

Hybrid Dynamic Source Routing Technique and Security Implementation in Adhoc Network Topology

Eswar Patnala[1*], Srinivasa Rao Giduturi[2]
[1*]Research Scholar ,GST,GITAM University, A.P, India
[2]Associate Professor ,GST, GITAM University, A.P, India
[1*]Corresponding Author : eswar.patnala@gmail.com

Abstract-- Routing protocols that are developed with the error-prone environment and resource constraints of mobile nodes in mind perform better in wireless Ad Hoc environments. A good and dependable routing method is required to meet the packet transition aim. When the network is small, most existing routing algorithms operate fine, but when the network is large, there is a problem with link breakage in multipath routing algorithms, especially on demand routing algorithms. As a result, we investigated many forms of routing protocols in order to identify all of the existing algorithms' flaws. In this study, we examine existing protocols in terms of network factors such as delay, throughput, energy consumption, control overhead, and so on.

Keywords: AODV, DSDV, Zone based DSR.

I. INTRODUCTION

The popularity of a wireless connection has increased and is currently at an all-time high[1,2]. Users can communicate with each other and send data using wireless networks without using a cable connection. The development of wireless devices has helped wireless networks gain popularity. Components and mobile devices are mostly focused on local area networks (WLAN). In generally, they have two operating modes: the first one is the infrastructure (BS), which is when control modules are present, as well as the second is when control modules are not present. An ad hoc network's operations are not reliant on infrastructure. The systems may display similar fundamental radio communication problems, also including low battery life, bandwidth limitations, poor lesser quality, and insufficient coverage. Just like in conventional wired networks, wireless networks contain hosts and routers as well. In addition to forwarding data or packet over a network, a router can be used as a source or hosts for synchronisation. There is a basic difference in between wired connection and a wired network; apart from of the cable, there is no distinction; the means of communication inside the network are also different. because there is no dependence on the wired link for the wireless network. The signal is weaker while travelling outside the defined area. A radio transmission is referred to as a "range radio signal" when it reaches this location. Most people think that when the receiver gets closer to the radio, the signal gets stronger and the receiver can pick it up. If not, the target recipient is not contacted with the message. Wireless communication is governed by a number of access control mechanisms. A wireless network's elements (nodes) are mobile and modify the network's topology at random [1,2].

II. ROUTING PROTOCOLS IN MANET

Finding a route between both the source and the destination is the first stage in the two-step process of routing in ad hoc wireless networks, after which data packets are transmitted. Routing techniques for typical wired networks not be easily adapted to MANETs due to their limitations and peculiarities, including such dynamic topology, bandwidth limitations, ambiguous link capacities, and energy restrictions[3]. Several routing techniques have recently been developed for detecting and condition will lead in MANETs. The optimum routes connecting nodes at source and destination which may involve several intermediary nodes, are chosen using routing. Depending upon the nature communication type, the routing protocol can be categorised either unicast, multicast, or broadcast. Each of the aforementioned categories has a single sender, but they vary in the number of destination host they have and the methods they use to choose those nodes. In unicast route, there is only single particular destination node, however packets are sent to precisely one destination out of many potential destinations. Creating routes for packets of data to be sent to numerous destinations that are clustered together is the aim of multicast routing. All network nodes are intended to receive data packets using broadcast routing[3].

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
DOI: https://doi.org/10.17762/ijritcc.v11i9s.7429
***Article Received**: 10 May 2023 **Revised:** 29 June 2023 **Accepted:** 26 July 2023*

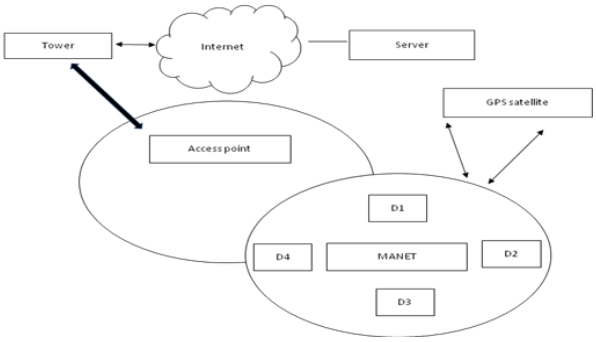


Figure 1 General Architecture of MANET

III. PROPOSED ARCHITECTURE

- Architecture is divided into two phases
  - Network Phase
  - Data Transfer Phase

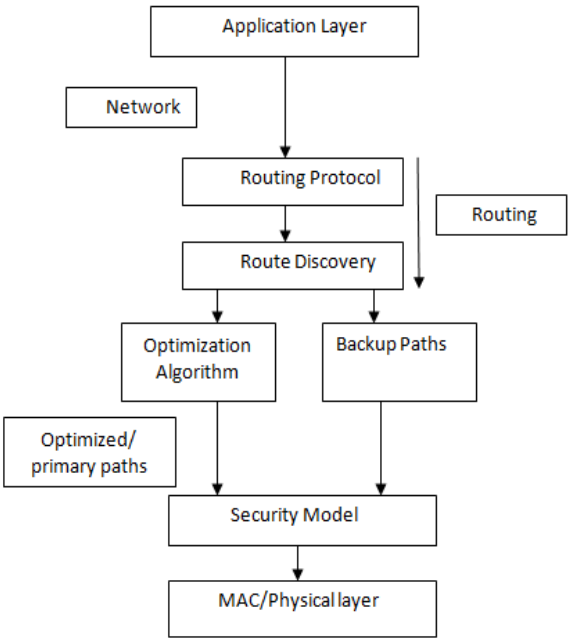


Figure 2 Network Phase

In the above diagram we proposed how the routes will be identified from source to destination. Here first the data will be transmitted from source to destination. The Data will be starts transmitted from application layer and then enters in to the network. Then using some routing protocol , the route discovery will be done and after that we will apply some optimization algorithms get shortest path from source to destination.

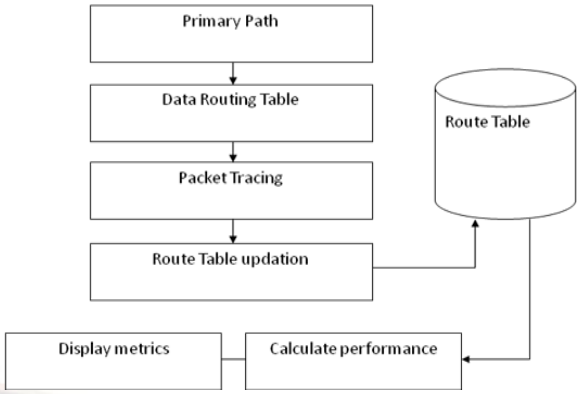


Figure 3 Data Transfer Phase

In the data transfer phase , data will be transmitted from source to destination by identifying the shortest distance. Here first we send the hello packet based on the responses we select one path as primary path and then that will be updated routing table and packet tracing will be done we calculate the performance.

IV. ROUTING PROTOCOL CLASSIFICATION

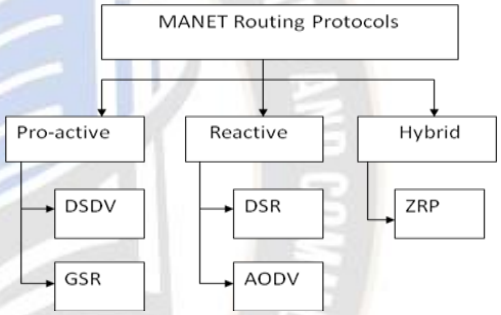


Figure 4 Routing Protocol Classification

Due to the limited wireless connectivity ranges in MANETs, it is frequently necessary to use one or more intermediary nodes to relay packets in between source and the destination mobile nodes. As a result, it is believed each of the network's nodes has routing capabilities. Due to variations within communication networks as well as the mobility of mobile nodes, MANET does have a highly dynamic design. The literature has published a number of strategies for creating and sustaining channels for trustworthy data flow from source to destination, and the categories are important[3].

A. *Reactive Routing protocol:*

Reactive routing methods only choose routes that whenever a sender has data to convey to a destination node. If the path from the source to the intended destination is not accessible, the source node performs a path discovery operation to find the necessary routes[3]. When route discovery, a request packet message (RREQ) is broadcast over the entire network, then rrep packet message (RREP) from a collection of nodes are being sent back to the originating node. The best route out of all those that are available is utilised during

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
DOI: https://doi.org/10.17762/ijritcc.v11i9s.7429
***Article Received**: 10 May 2023 **Revised:** 29 June 2023 **Accepted:** 26 July 2023*

connection setup and data transmission, as well as the chosen path is followed until it is no longer valid, accessible, or functional[7]. Reactive routing's main advantage is its ability to generate a path as soon as one is needed. Reactive routing techniques eliminate the need for static routing table maintenance. On-demand routing are those that find routes only after being asked for or desired. Reactive routing techniques do not use bandwidth while a node is not sending data packets; rather, they only use bandwidth when a node have information to send to the a destination. The reactive routing technique decreases bandwidth of the network consumption and battery consumption since no route update messages are usually delivered in the network[9].

1) Dynamic Source Routing:

A simple and effective routing protocol called Dynamic Source Routing (DSR) was created to multi-hop ad hoc networks containing mobile nodes. Without the requirement for any pre-existing network architecture or management, DSR allows the network can self-organize and configure itself. It's a reactive protocol, which means that all of its parts operate according to demand. Source routing is the foundation of this concept. Source routing is a type of routing method where the sender of the a packet chooses the entire list of nodes that the packet will go through[9].

Source routing has the advantage of removing the requirement for intermediary nodes to maintain current route data in order to appropriately route the packets that forward. The protocol's two core techniques are "Route Discovery" & "Route Maintenance." The DSR mandates that every node maintain its route cache of the all the known self-to-destination pairs. A node will attempt to use this cache to deliver any packets it has to send. The path discovery phase is started by submitting the route discovery process to find a path to the target if the destination is not already cached. This request contains the source address, the destination address, and a special identifying number[9].

If a route is still accessible via the route - cache but is no longer valid, a route maintenance operation can be started. A node processes a route request packet if it hasn't been processed before and the address isn't stored in the route cache. A route reply is generated by destinations or any one of the adjacent nodes when they are aware of how to get there.

2) AODV(Adhoc On-Demand Distance Routing protocol)

The RFC 3561 proposed AODV for standardisation in July 2003. The same group that made the DSDV also made this one. The distance vector routing method AODV bases routing choices on the quantity of hops needed to reach the target. This network's capacity to support multicast & unicast routing is indeed a special feature[8].

Characteristics of AODV[8]:

- Communication is divided into three types: Unicast, Broadcast, and Multicast.
- Route creation on demand with little latency.
- Due to the usage of sequence numbers, all routes are loop-free.
- To keep track of the accuracy of the data, sequence numbers are utilised.
- Instead of keeping track of the complete route, it *only keeps track of the next hop.*

Advantages &Disadvantages[8]:

- The main advantage of this protocol is the ability to establish routes on demand and identify the most recent route to a destination using destination sequence numbers. It takes less time to establish a connection.
- Inconsistencies in routes may emerge from intermediate nodes if a source sequence number seems to be very old and they have an higher but not the most current destination sequence number, leading to stale entries. This is one of the protocol's downsides. A large level of control overhead can also emerge from sending multiple Route Reply packet in response to a particular Route Request packet.
- The excessive bandwidth usage of AODV's recurrent beaconing is another drawback[8].

B. *Proactive Routing protocols*

Proactive routing protocols ensure that there is always a path between any pair of network nodes. For the purpose of creating and maintaining routes, the network periodically sends out route update messages [3]. Periodic updates are transmitted between nodes at predetermined intervals regardless of the volume of traffic or the mobility of the nodes. On the other hand, event-triggered updates only take place when a certain event, like a connection breaking, takes place. Node mobility directly influences connection modifications, increasing the number of event-triggered updates. In this class of routing protocols, the number several routing tables are used to store routing information. The "table-driven routing protocols" refers to the fact that all these tables are updated often. The main advantage for proactive routing protocols is the constant availability of reliable and current routes among all nodes in the network in routing tables. However, a notable drawback is the considerable cost involved in creating, maintaining, and updating this routing table. Routing table modifications may become quite frequent when there is high node mobility. Mobile ad - hoc protocols involve Destination-Sequenced Distance Vector (DSDV) as well as Optimized Link State Routing (OLSR).

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
DOI: https://doi.org/10.17762/ijritcc.v11i9s.7429
***Article Received**: 10 May 2023 **Revised:** 29 June 2023 **Accepted:** 26 July 2023*

Destination-Sequenced Distance Vector (DSDV):

The Bellman Ford Algorithm has been updated to create the Destination Sequenced Distance Vector Routing protocol, which is based on the ideas of distance vector routing[10].

Each node broadcasts a table describing its distance between directly linked nodes with distance vector routing (DVR), and other nodes propagate the updated routing based on that data. The nodes that cannot be reached right away are designated as "infinite"[10].

However, ongoing routing table updates result in an endless cycle that is frequently referred to it as Count-To-Infinity problem[10].

Every time this routing table is modified, an sequence number is issued there in routing table to avoid the issue of counting to infinity. A sequence number variable has been added to DSDV's process, which is comparable to Distance Vector Routing's.

For each node, the DSDV protocol simply requires and maintains one single table. [10].

Routing Table: It includes the sequence number and the distance between each node and each of its neighbours

To ensure that every node broadcasts and receives correct info about all nodes, including their distance & sequence number, this is updated for each step[10].

Advantages:

- Commercial or large-scale implementation is not possible.
- When used to small networks, efficient results will be obtained.

Disadvantages

- The time it takes to process a protocol is longer.
- There is less bandwidth available.
- Not ideal for big networks with a high degree of dynamicity.

2. ***Global State Routing:***

The essential notions of link state routing underpin global state routing.

A single routing table is sent from one node to its neighbours with Link State Routing (LSR), who then send it to various nodes. This process will go on until every node in the network has received the routing table[11].

Regarding Global State Routing, however, a node's routing table is only broadcast to its immediate neighbours. Then the surrounding nodes' initial tables are updated. These updated tables are broadcast one by one, and this process continues until all nodes in the network have broadcast their tables to each other[11].

For each node, the GSR protocol employs and maintains three tables. These are the tables:

- Distance Table
- Topology Table
- Next Hop Table

Distance Table: This table shows a node's distance from all other nodes in the network.

Topology Table: This table contains Link state data information as well as a sequence number that may be used to determine when the data was last updated.

Next Hop Table: The information about a node's immediate neighbour will be stored in the next hop table[11].

Advantages:

- In comparison to LSR, GSR has a higher accuracy in creating optimal paths.
- When compared to flooding, which is employed in LSR, broadcasting reduces mistake rates.

Disadvantages:

- Large amounts of bandwidth are consumed.
- Operational costs are higher.
- Larger message sizes require more time to process[11].

C. ***Hybrid routing protocols***

Due to the high overheads involved with routing tables, a completely proactive routing method is not suited for MANET environments. A pure reactive protocol, on the other hand, cannot be totally successful in MANETs due to its inherent drawbacks. As a result, significant components of the both systems can be integrated to form the Hybrid protocols, a new class among mobile ad hoc routing protocols [3]. These techniques sometimes show reactive behaviour, while other times they show proactive behaviour. In the MANET context, hybrid routing approaches offer flexibility and scalability by assuming that the entire network is divided into zones [8]. The hybrid classes include the ZRP and ZHLS.

Zone Based DSR:

Essentially, it combines the advantages of proactive and reactive routing strategies into a single package. These protocols are adaptable by nature, taking into account the zone and location of the sending and receiving mobile nodes. One of the most used hybrid routing systems is Zone Routing Protocol (ZRP).

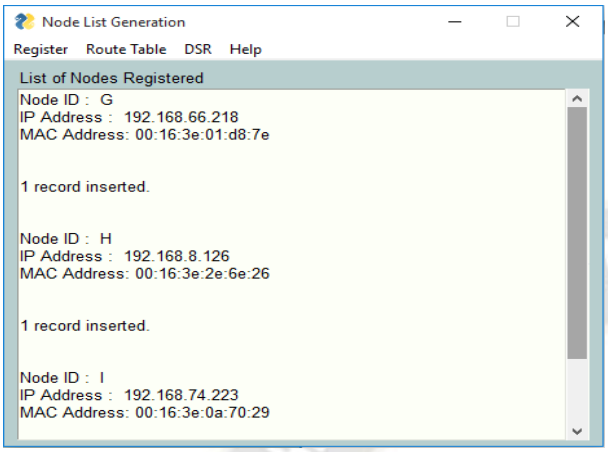
Zones are created for the entire network, and the locations of the sources and destinations mobile nodes are therefore monitored. Proactive routing is used to send data packets between mobile nodes that are in the same zone as the source and destination. Reactive routing is used to send data

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
DOI: https://doi.org/10.17762/ijritcc.v11i9s.7429
***Article Received**: 10 May 2023 **Revised:** 29 June 2023 **Accepted:** 26 July 2023*

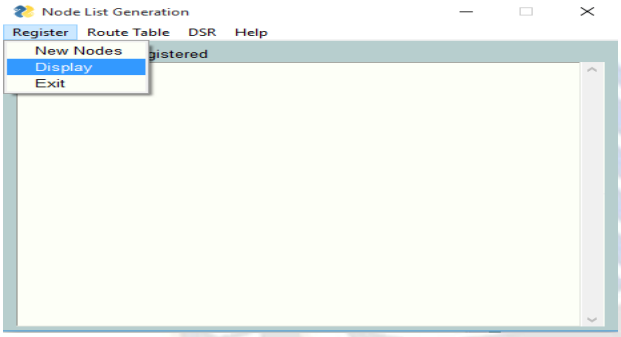
packets between mobile nodes that are in distinct zones as the source and destination.

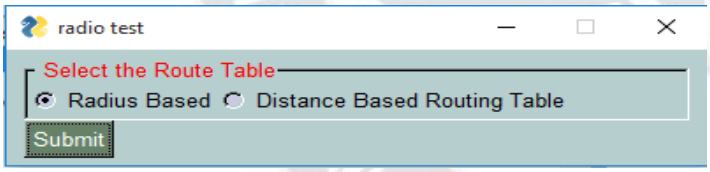
V. DSR IMPLEMENTATION

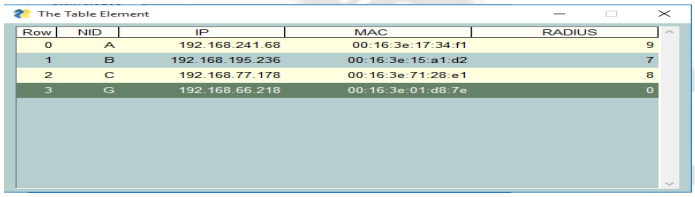
D. *List of Nodes Registered*



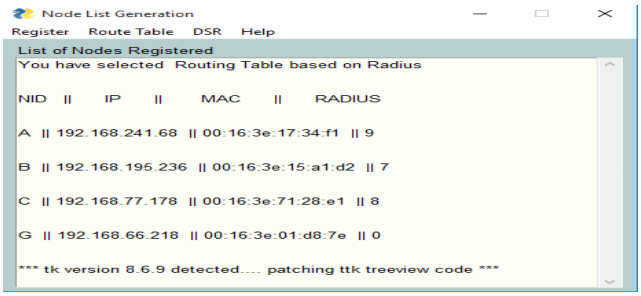
E. *Display route tables basing on Radius and Distance*

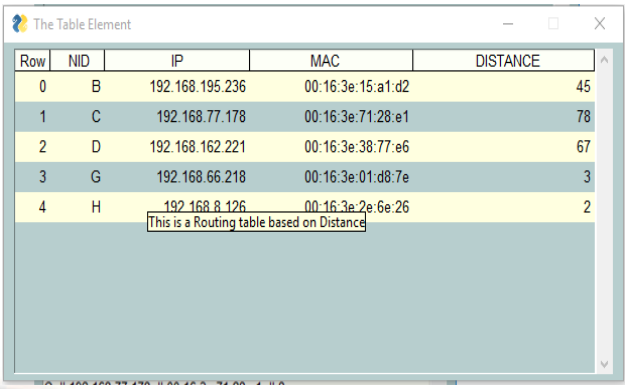


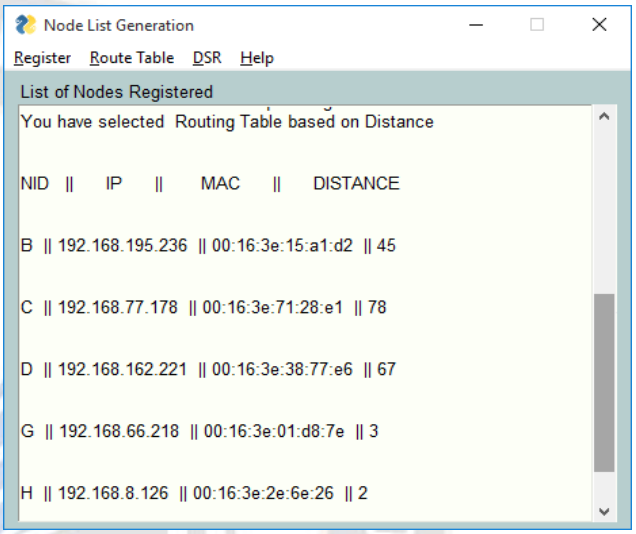




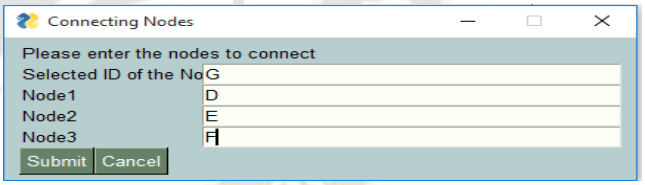
F. *Node List Generation:*



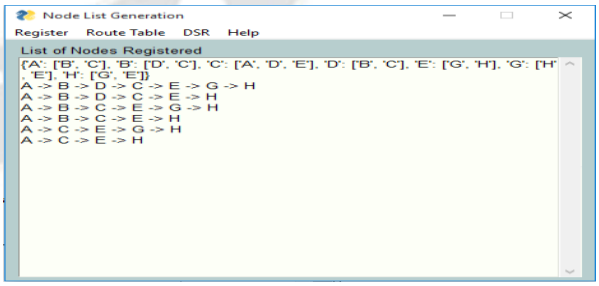




G. *Route Construction:*



H. *Route Request*



Route Reply:

The details of the shortest route is generated

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
DOI: https://doi.org/10.17762/ijritcc.v11i9s.7429
***Article Received**: 10 May 2023 **Revised:** 29 June 2023 **Accepted:** 26 July 2023*

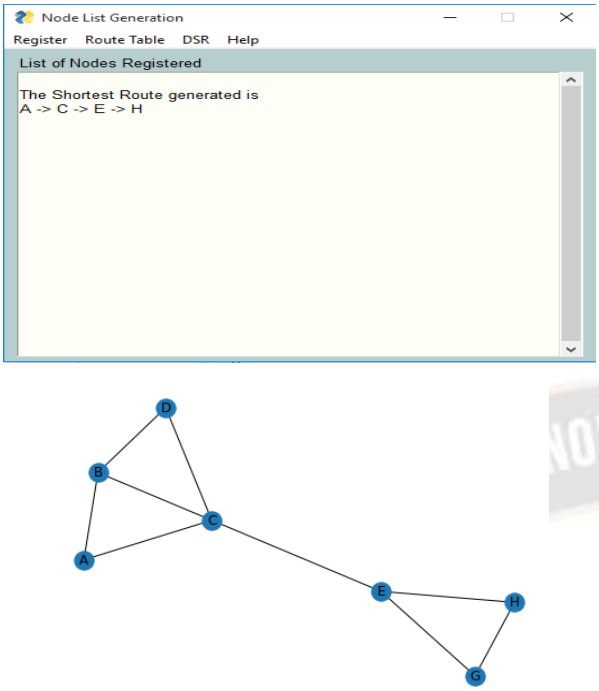
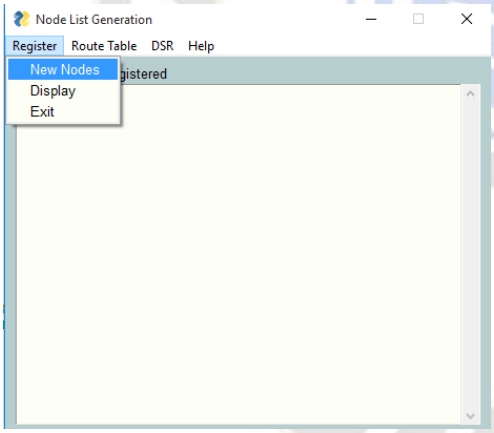
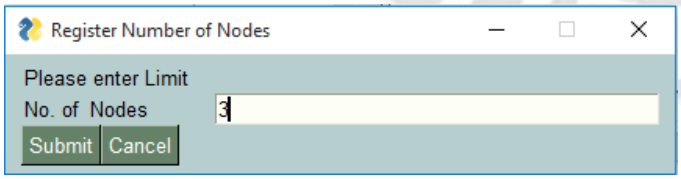


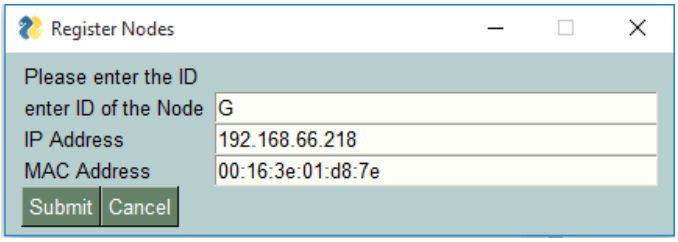
Figure 5 Shortest path generated

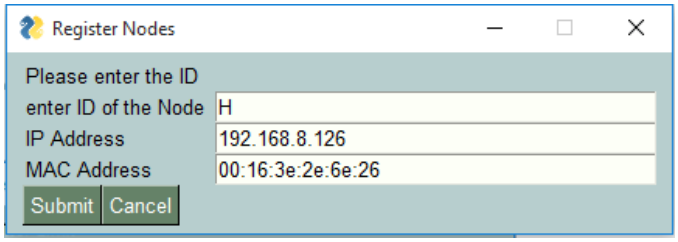
VI. HYBRID DSR IMPLEMENTATION

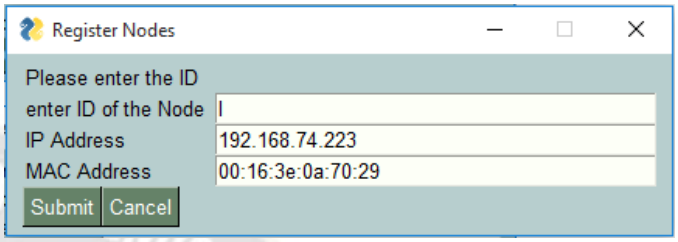
Registering new nodes:

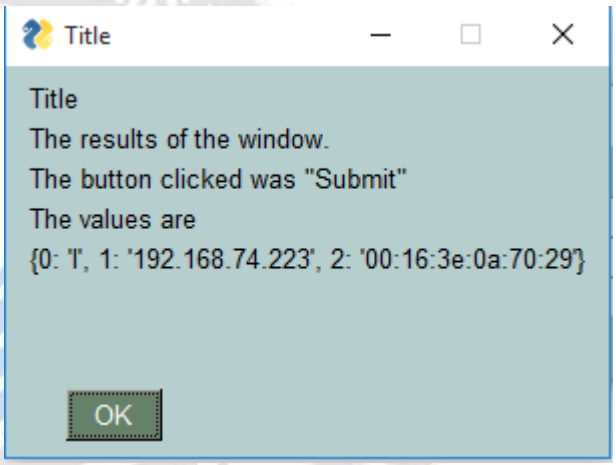




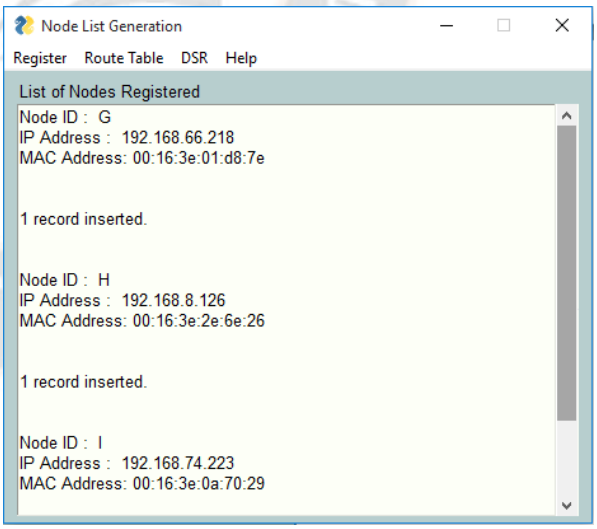




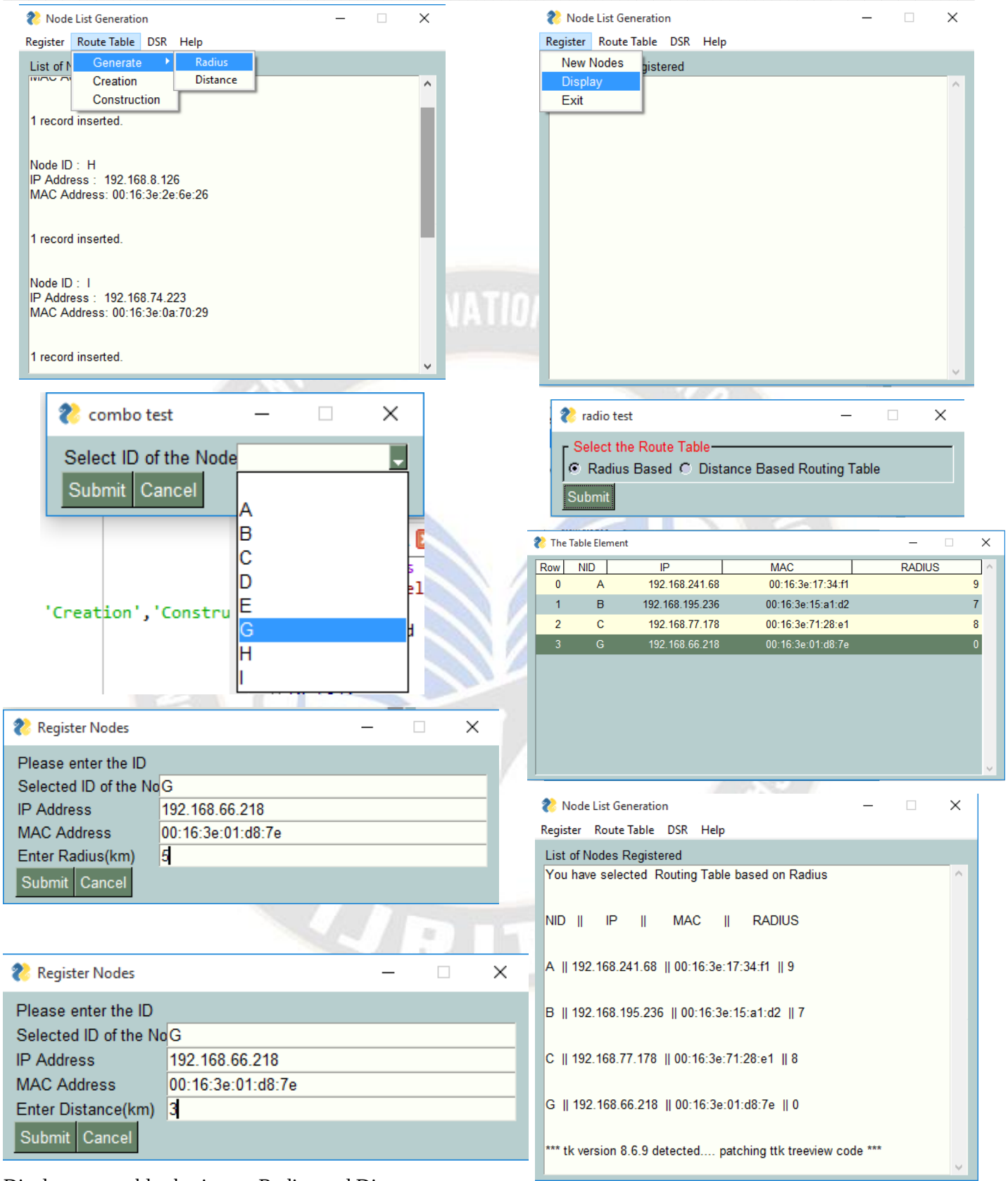




List of Nodes Registered.

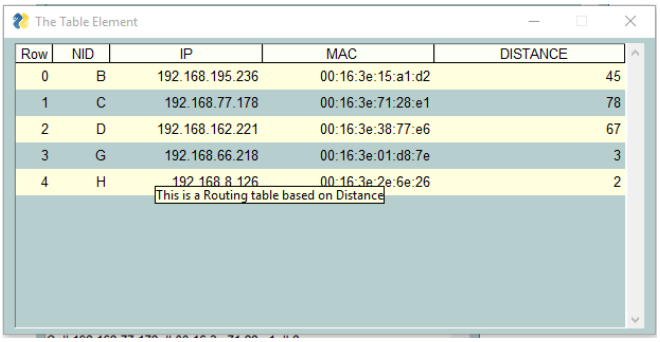


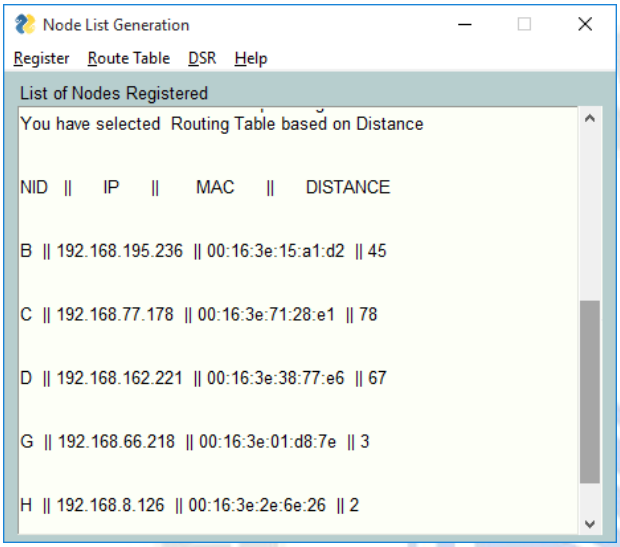
International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
DOI: https://doi.org/10.17762/ijritcc.v11i9s.7429
***Article Received**: 10 May 2023 **Revised:** 29 June 2023 **Accepted:** 26 July 2023*



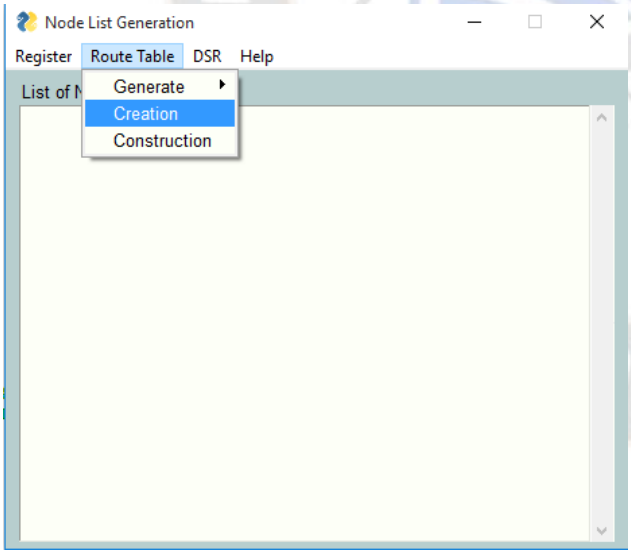
Display route tables basing on Radius and Distance

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
DOI: https://doi.org/10.17762/ijritcc.v11i9s.7429
***Article Received**: 10 May 2023 **Revised:** 29 June 2023 **Accepted:** 26 July 2023*

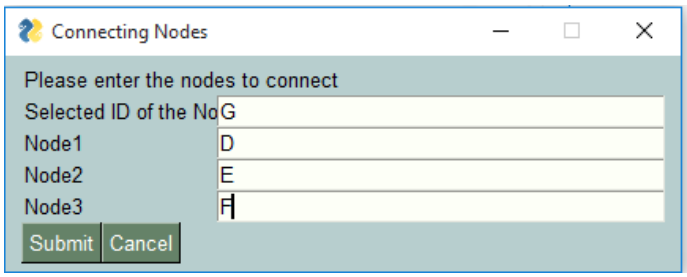




Creation of Route table

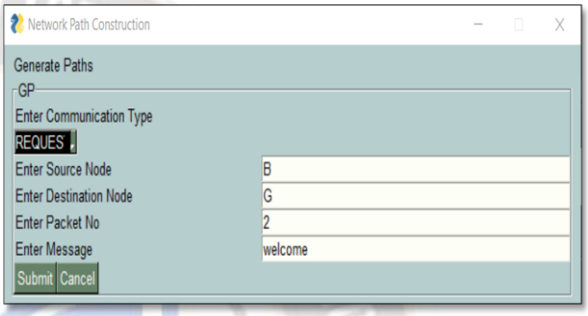


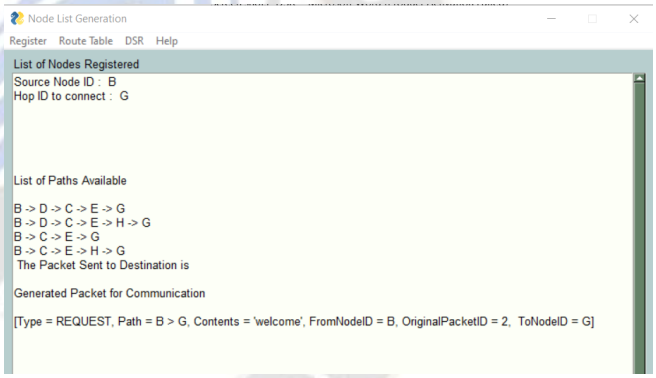
Route Construction:



DSR

Route Request:





VII. PARAMETER COMPARISON BETWEEN DSR AND HYBRID DSR

Parameter	Hybrid DSR	DSR
No. of Node visited	4	6
Execution Time	0.9364275932312012 seconds	21.488828897476196
Latency	21.3347616s	24.734215s

Table 1 parameter comparison

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
DOI: https://doi.org/10.17762/ijritcc.v11i9s.7429
***Article Received**: 10 May 2023 **Revised:** 29 June 2023 **Accepted:** 26 July 2023*

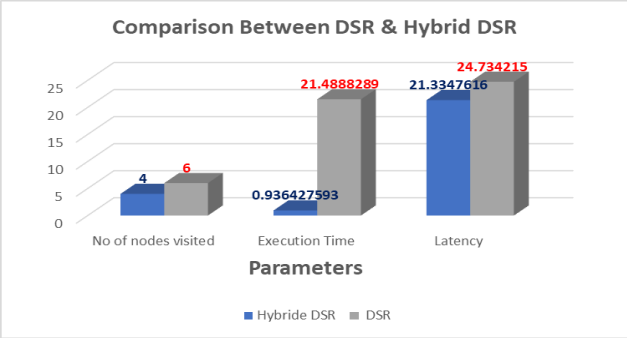


Figure 6 Comparison between DSR & Hybrid DSR

Route Reply:

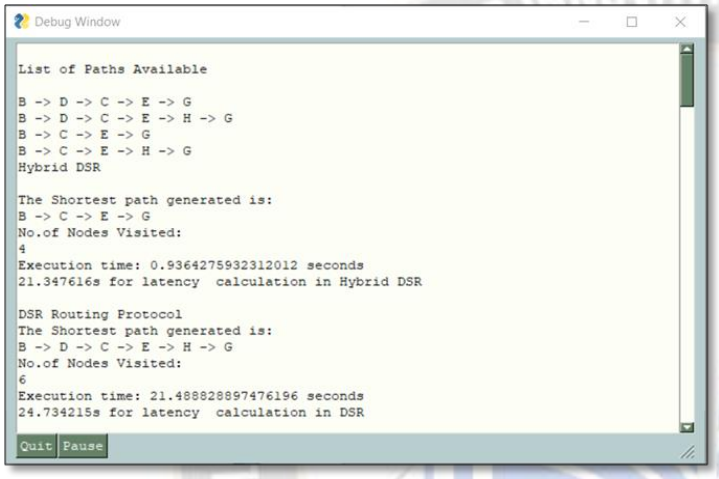


Figure 7 Shortest Paths and latency calculation using DSR and Hybrid DSR

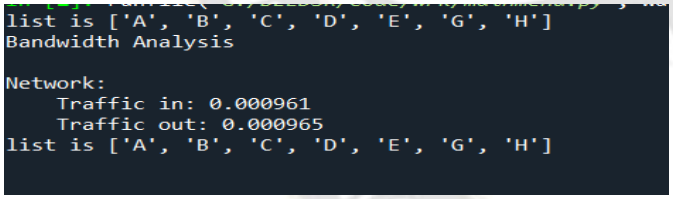


Figure 8 Bandwidth Analysis with input and output traffic

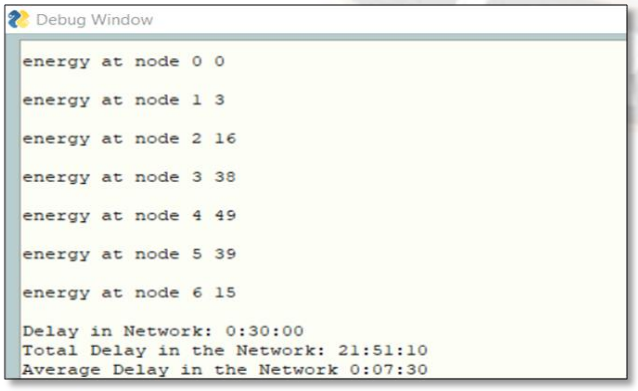


Figure 9 Energy calculation at each node and Delay Calculation in the network

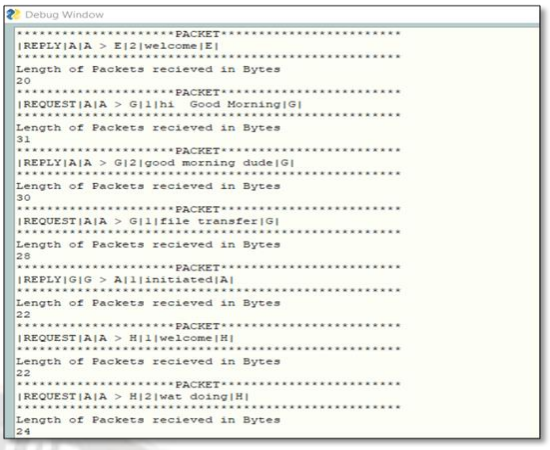


Figure 10 Packet Format received at each node received with length of the packets received.

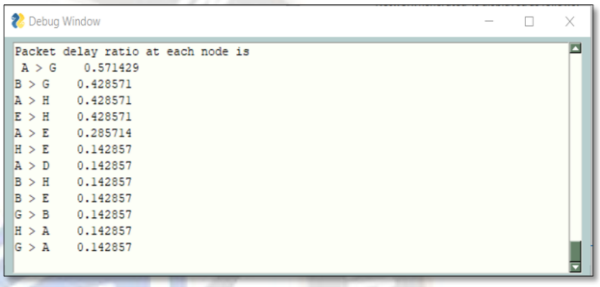


Figure 11 Calculation of Packet Delay Ratio at each node

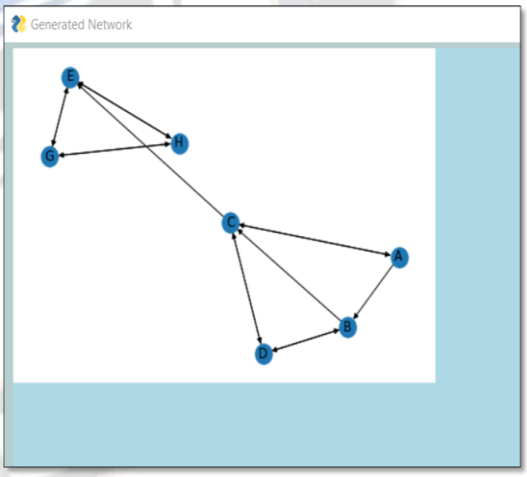


Figure 12 Generated Network

VIII. SECURITY IN MANETS

The MANET network is more vulnerable to attacks than other networks because the nodes, which are movable and are in charge of routing the packets, are mobile. There are a few fundamental security issues with MANET, as noted below.

- Due to a shortage of resources, cryptographic techniques that operate in wired networks cannot be implemented in ad-hoc networks.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
DOI: https://doi.org/10.17762/ijritcc.v11i9s.7429
***Article Received**: 10 May 2023 **Revised:** 29 June 2023 **Accepted:** 26 July 2023*

Because of this, innovative solutions in this field are required.

- Interoperability in wireless devices results in a lack of privacy. They make it simple to eavesdrop on messages.
- As routers in ad-hoc networks participate in the message relaying process, any attacker node can exploit this to abuse the network traffic by intercepting it or altering it.
- Security concerns also arise from network node location. Ad-hoc network nodes may be installed in an unsafe setting. This could lead to a lot of actual physical attacks on the deployed nodes.
- Ad-hoc networks' changeable network topologies give hostile nodes more options for attack[12].

Name of the Attack	Cause	Prevention
Sleep Deprivation Attack	False requests are switched to assure resource consumption on the target node.	To forward a packet to any node in a cluster, the cluster head utilises a threshold value. No packet of data will be entertained after the threshold .
Black Hole Attack	fake responses with higher - level sequence numbers from a malicious node	by looking for routes that share nodes. based on the use of several routes to transmit packets .
Impersonation Attack	logical or physical address spoofing.	by identifying routes with shared nodes. depending on the choice of several routes for transmission of packets .
Rushing Attack	increased transmission rate and packet forwarding speed	Many general defence strategies against rushing attacks.
Poisoning of Routing Table Attack	higher packet forwarding and transmission rates	Using a hash chain can stop the creation of erroneous higher order sequence numbers[12].

ENHANCED DATA ENCRYPTION:

The majority of the time, storage, and battery power are all resources that encryption techniques need heavily. Due to the fact that all mobile nodes in MANET are portable devices like laptops, PDAs, and mobile phones, battery life is a concern due to the energy consumption of encryption methods.

Compared to other technologies, battery technology is gradually advancing. Thus, it is essential to offer an appropriate method with low computational and energy requirements and enhanced security. One of the most popular encryption algorithms for networks, DES, is not appropriate for MANET since the encryption process demands more processing time and energy.

Improvements to DES (EDES) that take into account the CPU, memory, and battery usage restrictions on mobile nodes.The DH (Diffie Hellman key exchange algorithm) key protocol is used to transfer the symmetric key in a more secure manner[13].

Goals of Cryptography:

Confidentiality: Encryption is used to achieve confidentiality, which simply serves to make sure that the information is secure and secret.

Data Integrity: This protects against either intentional or unintentional data change.

Authentication: To verify that the source is genuine and known to the recipient, authentication is required.

Non-Repudiation: Non-Repudiation ensures that neither the sender nor the recipient may deny that the message was sent[14].

Asymmetric Key Algorithm

Asymmetric key algorithms employ two distinct keys: a public key and a private key. Since only the recipient will be able to decrypt the message, the public key is typically used for encryption and the private key for decryption. Hence, the sender encrypts the message using the recipient's public key and sends it; the recipient can then decrypt it using his own private key[14].

Symmetric key Algorithm

We will only utilize one key in the symmetric key technique for both decryption and encryption. The sender will encrypt the communication with a private key that is shared between both the sender and the receiver confidentially. The receiver will use this key to decipher the sender's encrypted text. Thus, this algorithm uses a single secret key.

Cryptographic hash functions:

The functions that accept an input and return a fixed-length alphanumeric string are known as cryptographic hash functions. The string is also known as a checksum, message digest, digital fingerprint, or hash value.

Three key characteristics define the optimum hash function: (A) The process of calculating a hash for any given data is

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
DOI: https://doi.org/10.17762/ijritcc.v11i9s.7429
***Article Received**: 10 May 2023 **Revised:** 29 June 2023 **Accepted:** 26 July 2023*

incredibly simple. The computation of an alphanumeric string with a given hash is exceedingly challenging. (c) It is incredibly rare that two messages that are just a little bit different will use the same hash[14].

While still being effectively computable, a hash function in cryptography should look as much feasible like a random function. From a cryptographic perspective, a cryptographic algorithm is deemed "insecure" if it is computationally possible to uncover collisions—where two distinct messages share the same hash value—or to locate a previously unknown text that match a given hash value.

PROPOSED SYSTEM:

The suggested system incorporates many layers of security into MANETS, encrypting and decrypting data before sending it to the final location, where the SHA algorithm is used to verify the integrity of the data.

Using the SHA-256 method, the sender determines the digest of the information that has to be communicated; the data is then encrypted and sent to the destination along with the message digest. The hash code value of the inbound information is compared to the one that is appended to the input text when the message is decrypted and received at the destination. In this manner, the message's authenticity is confirmed.

SHA-256:

The SHA-2 family of hash algorithms, which also includes SHA-256 and SHA-512 that differ in terms of word block sizes, includes SHA-256. The SHA-256 adheres to the FIPS PUB 180-2 specification. The National Institutes of Standards and Technology (NIST) and other public and commercial organizations produced this[14].

A mathematical operation known as a hash function transforms an input value into some other compressed information of a predetermined length. The hash function accepts input of any length, but the output has a defined length.

SHA-256 functions similarly to MD4, MD5, and SHA-1. The message is divided into 512-bit message blocks called M1, M2,..., Mn after being initially padded with its length such that the output is a multiple of 512-bit long word. The blocks are now processed one at a time, progressively calculating from the initial buffer H (0).

$$H(i) = H(i\text{-}1) + C_{Mi} \cdot (H(i\text{-}1))$$

Where + denotes addition in word-wise mode 232 and C is the SHA-256 compression algorithm. The message's hash or message signal is represented by H(n)[14].

Conclusion:

In the above paper i have discussed, various routing protocols in MANET ,like reactive ,proactive and hybrid protocols and classifications, also specified the general architecture of MANET. which was further divided into network phase and data transfer phase ,this architecture will show ,how the data will be transferred from originating to ending ,and how the network is established. Implemented DSR and Hybrid DSR algorithms and also taken values for some metrics like no. of nodes visited, Execution time ,latency, where hybrid DSR shows better results when compared to DSR in all parameters.

REFERENCES

[1] S.Misra, N. Saha, “Detour: Dynamic Task Offloading in … S. Misra, I. Woungang and S.Misra (Eds.), Guide to Wireless Ad Hoc … and Networks Series, Springer-Verlag, London, U.K., February 2009, 632 pages
[2] K.Toh ,Ad Hoc Mobile Wireless Networks: Protocols and Systems,Prentice Hall PTR,NJ,2002
[3] Misra and B. J. Oommen, “Adaptive Algorithms for Network Routing and Traffic Engineering”, Proceedings of the 19th National Conference on Artificial Intelligence (AAAI’04) , San Jose, California, USA, July 25-29, 2004.
[4] Q. Y. Liu, Multipath based QoS routing in MANET,, Journal of Networks 4 (8) (2004) 771–778.
[5] J. Haas, Pearlman MR: The zone routing protocol: a hybrid framework for routing, Vol. 2001, Addison-Wesley, Reading, MA.
[6] Nasipuri, R. Castaneda, Das SR: Performance of multipath routing for on-demand protocols in mobile ad hoc networks, Mob. Netw. Appl 4 (339-349) 10–1023.
[7] Ducatelle, Di, Caro GA, Gambardella LM: Using ant agents to combine reactive and proactive strategies for routing in mobile ad hoc networks, Int. J. Comput. Intell. Appl. (Special Issue on NatureInspired Approaches to Networks and Telecommunications) 2005 5–2.
[8] https://www.brainkart.com/article/Ad-Hoc-On-Demand-Distance-Vector-(AODV)--Algorithm,-Illustration,-Advantages,-Disadvantages_9942/
[9] https://www.brainkart.com/article/Dynamic-Source-Routing-protocol-(DSR)--Algorithm,-Example,-Advantages,-Disadvantages_9941/
[10] https://minigranth.in/mobile-adhoc-networks-tutorial/dsdv-routing-protocol-manet
[11] https://minigranth.in/mobile-adhoc-networks-tutorial/global-state-routing-gsr-manet.
[12] Vaishali, Priyank Pandey, Prashant GoelA Review on Security in MANET, International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181 Published by, www.ijert.org ICCCS - 2017 Conference Proceedings
[13] S.Sudha, V.Madhu Viswanatham, K.Brindha, L. Agilandeeswari , School of Information Technology and Engineering, School of Computing Science and Engineering VIT University, Vellore-632 014, TamilNadu, IndiaImplementation of Enhanced Data Encryption

Standard on MANET with less energy consumption through limited computation, International Journal of Engineering Research and Development eISSN : 2278-067X, pISSN : 2278-800X, www.ijerd.com Volume 2, Issue 4 (July 2012), PP. 46-52.

[14] Neelima, Lekharaju Sai Siddhartha, Chavali Meghana, Shaik Sameer4,Shaik Ashika,Vemulamada Naga Chandramouli,SECURITY IN MANETS USING CRYPTOGRAPHY ALGORITHMS, International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056,Volume: 04 Issue: 03 | Mar -2017 www.irjet.net p-ISSN: 2395-0072