

Possible Benefits and Drawbacks of Mobile Ad-Hoc Networks

Neelam Kumari¹, Rajveer Singh²

¹Research Scholar, Rajasthan College of Engineering for Women, Jaipur

²Associate Professor Rajasthan College of Engineering for Women, Jaipur

Conflicts of interest: Nil

Corresponding author: Neelam Kumari

Abstract

Unlike traditional wireless networks, mobile ad hoc networks (MANETs) allow nodes (such as smartphones, tablets, laptops, PDAs, etc.) to communicate and collaborate autonomously. To maintain data packet integrity, the network topology and routing table are constantly updated when nodes join and leave the system. The paper delves into the pros and cons of MANETs. Scientists will have a crystal clear understanding of MANET in every respect, from its aims and challenges to its many uses. Mobile Ad Hoc Networks (MANETs) allow for decentralised data packet sharing between nodes using wireless networks without the need of a central network administrator. In such a network, providing a power-aware, secure routing system is challenging due to the unexpected topologies and limited resources. In this research, we provide a reliable routing algorithm that considers the reputation and power of the network. We use a reputation model, some muscle, and a Krill Herd based Grasshopper Optimisation Algorithm (KH-GOA) to construct a reliable path from the source node to the destination node. Numerous reputational factors are taken into account by the model, including node mobility, actual capabilities, historical records, and reputation among neighbours, among many others. Following a thorough examination of the reputation requirements of every node, we present the KH-GOA approach, which merges the Krill Herd (KH) with the Grasshopper Optimisation Algorithm (GOA) to construct a reliable path from the starting point to the endpoint. A suggested routing protocol based on KH-GOA takes into account latency, distance, power, and reputation as multi-objectives.

Keywords: MANET, MANET Challenges and Applications

Introduction

Thanks to advancements in wireless network infrastructure, the number of applications accessible over the internet has skyrocketed. Wireless networking has just entered a thrilling new era with the advent of the Mobile Ad-Hoc Network (MANET). As the number of people using mobile devices and wireless networks continues to rise, wireless ad hoc networks have emerged as a highly active and dynamic subset of the communication and networking sector. Multiple wirelessly linked mobile devices (e.g., computers,

cellphones, sensors, etc.) form a mobile ad hoc network. All of these parts work together to provide the impression of a centralised administration while really performing the necessary network operations in a decentralised fashion. Since it may either operate alone as a network or provide many connections to cellular networks or the Internet, this architecture opens the door to a wide range of interesting and novel uses [1].

In a MANET, each node works together to get the best possible path for a packet to take. Nodes in a

network are limited to communicating with other nodes within their broadcast radius R , regardless of how close the real distance is. Without the centralised support of an access point or base station, a multihop wireless ad hoc network cannot function. The nodes in a mobile ad hoc network (MANET) must advance data packets for each other before they may permit communication between mobile devices that are not in direct line of sight. Nodes that are mobile in a network may move around freely. Any time the nodes choose, they may disconnect and reconnect with the network. Consequently, the state of a node's connections to other nodes might change frequently. When dealing with the mobility of nodes in an ad hoc network, MANET routing algorithms encounter additional obstacles caused by many features of wireless transmission, such as attenuation, multipath propagation, interference, etc. The network may become much more complex as a result of the addition of several different types of nodes, each with limited resources [2].

This study aimed to simulate DSR, TORA, and OLSR routing protocols using a simulator and compare the results under different scenarios, such as with Nodes Density of 25, 50, and 75 nodes. The parameters used for evaluation and analysis included WLAN delay, WLAN throughput, WLAN network load, and FTP traffic sent and received by nodes.

One way to define a system of linked wireless mobile devices that may form new groups on their own is as a "mobile ad hoc network" (MANET). Because these networks consist of a collection of mobile nodes—devices that aren't permanently installed but instead communicate with one another over wireless connections and are free to roam the environment—their topology is dynamic and ever-changing. Due to the short communication range between nodes in a MANET, data packets must pass through several relays before reaching their ultimate destination.

Local Area Connections and Wireless Networks

Wireless networks allow users to join from anywhere, and they may also extend the network to

areas without wires, such as buildings. Substructure networks and ad hoc networks are two possible classifications for these connections, as shown in Figure 1. In physical-based wireless networks, an access point (AP) controls the devices connected to the network. In theory, anything with an access point may join the network. At all times, the route is accessible (BSSs) since the access point has coordinated their connection. Another drawback of a network design is the amount of extra effort required to keep routing tables current [4]. In Ad-Hoc or structure-less networks, data-packet transit and reception are more problematic due to the lack of a predetermined topology or centralised controlling point. Multiple subtypes of wireless networks exist, including ad hoc, infrastructure-based, single-hop, and multi-hop. In older, single-hop wireless networks, electromagnetic waves were the primary means of communication between the BS and the wireless nodes. Until it reaches the base station, data in a multihop wireless network goes from one wireless node to another.

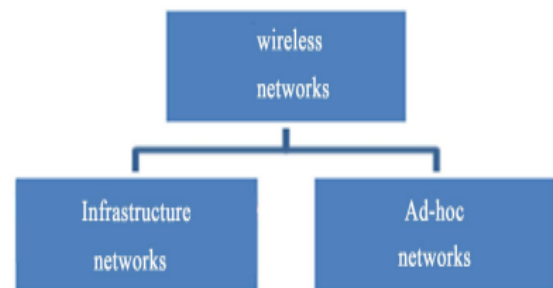


Figure 1. Classifications of wireless networks.

The Unique Features of MANETs In the absence of any external assistance: MANET does its job without interference from higher-ups or formal hierarchies. Being a peer-to-peer (P2P) and decentralised system, each node processes data independently and acts as a router. When administrators have to split their attention across several nodes, it becomes more difficult to identify and handle network problems. Any node in a mobile host network may use multi-hop routing to transmit data packets to other nodes. This does not come with any router capabilities. Structures that change throughout time: As nodes haphazardly

move around the network, its topology (often a multi-hop structure) is continuously evolving. Consequently, we may anticipate changes to traffic patterns, segmentation of networks, and perhaps packet loss. Abilities that are uncommon for nodes and connections: Different devices may have different radio interfaces and transmit/receive capabilities.

Potentially, they might function over a wide range of frequencies as well. Because the nodes' radio capabilities differ, connections could drop. The amount of processing power that mobile nodes can offer is dependent on their software and hardware characteristics. It could be difficult to construct network protocols and algorithms for such a diverse system due to the ever-changing nature of parameters like power and channel availability, traffic load/distribution fluctuations, congestion, and so on. Your level of effort determines the outcome. All portable devices' CPU performance degrades due to the device's limited battery life. This means that the capabilities of any gadget will have their limits. The fact that every node is both a system and a router is what causes the overall energy loss. Transmission of packets to other nodes consumes more resources. Because of this, the issue is of the utmost importance in mobile ad hoc networks. The incapacity to expand network capacity is a barrier to widespread adoption of such systems. Even very little, static wireless networks are too much for today's popular network management approaches. Networks having a high number of nodes are often used in many mobile ad hoc network applications, such as tactical networks and sensor networks. Before such a network can be put into place, a number of hurdles need to be removed. Problems with setup, addressing, security, routing, location management, interoperability, huge-capacity wireless technologies, etc.

Benefits of MANET

When a reliable, inexpensive, and widely available fixed-line network cannot be set up, this becomes very important. Please make the setup procedure as easy and fast as possible. There is no need for

complex planning or strategically placing base stations. With the ability to link to the Internet or the World Wide Web, ad hoc networks may be able to accommodate more users and devices. They provide a compelling argument for increasing coverage and connection when coupled with existing cellular networks because to their capacity, range, and energy economy. With the help of the upcoming 4G architecture and associated services, MANET plans to build ubiquitous computing environments. These environments will enable users to accomplish activities, access information, and stay connected no matter where they are or what device they are using [5].

Changes in the Environment of MANETs The programming of a MANET has to be flexible enough to adapt to the network's dynamic topology. A symmetric environment is best described by a MANET, where each node performs the same function. A MANET is a network architecture in which nodes are mobile and wireless and do not have a central controller or top-down structure. Neighbouring nodes may communicate wirelessly with one another, unlike in a large network where packet relaying is dependent on other nodes. This particular node has the capability to function as both a host and a router inside a MANET. Nodes in a MANET are free to join or go at any moment, making it dynamic like a fully maintained network.

Among the "Oddball Skills" in MANETs that could evolve with time are transmission and broadcasting sequences. Each node will have its own unique combination of computing power, battery life, and mobility. It is possible for certain network nodes to act as cluster leaders and others to be responsible for finding lost packets. The following forms of traffic may occur in ad hoc networks: unicast, multicast, geocast, content-based addressing, host-based addressing, and capability-based addressing, among others. The two types of networks, MANETs and more conventional ones, may function together or even live side by side. Several modes of transportation are available, including the airport lounge, taxis, the military, and private networks. Many things affect how well a mobile ad hoc network works, including the amount of data

being sent, how the network is designed, and whether or not there is radio interference. According to [6], mobility is defined by a number of factors, including quickness, direction bias, predictability, movement strategy, and inter-node feature homogeneity.

Problems with MANET Data Transmission:

Problems with MANET and the obstacles it creates are highlighted by the following: Wireless networks have limited data transmission capabilities compared to wired networks because of the limited size of the radio spectrum. That's why optimising data transmission speeds is a key component of wireless network routing solutions. Cutting costs as much as possible is one way to get there. The topographical data must be carefully preserved by routing algorithms due to the limited transmission range. Additional controller overhead is required to keep track of topological information on each node in a MANET, which reduces available bandwidth, since topology changes often in such a network. Prominence of certain traits in wireless networks: Disruptions to a wireless channel may occur due to route deterioration, signal weakening, interference from transmitters, or physical obstacles, among other possible broadcast disorders.

Even with constant, high-data-rate wireless connections, these parts will not break. There is a context-dependent sensitivity to the extent to which environmental factors and receiver/emitter adaptation limit transmission. The two main quantifiable limitations that regulate the capacity to transfer information at different data speeds are the theorems of Shannon and Nyquist. Wireless networks, as a means of communicating with large audiences: Any and all equipment, including broadcasts, that are directly inside a radio channel's transmission range define the channel's characteristics. No additional device, not even the sender, is required to transmit data to a receiving device. The device is allowed access to the shared media as long as its communications won't disrupt any ongoing sessions. There are a lot of potential

users on a wireless network at once, which makes data-packet collisions common.

Another possibility is a network storm, which might occur as a result of an internal network breakdown. Data packet loss at the receiving end as a result of broadcasts from nodes that are not in the direct communication channel of the transmitter but are in the path of the receiver is called a "concealed terminal problem" in a network. Transmission failures leading to packet loss: Factors such as high bit error rate (BER) in the wireless channel, bigger crashes caused by hidden terminals, interference, position-dependent controversy, unidirectional associations, frequent pathway breaks caused by device movements, and the integral declining characteristics of the wireless passage are common causes of sophisticated packet damage in ad hoc wireless networks.

Route breakages occur often during a continuously occurring meeting in an ad hoc wireless network because the system topology is extremely dynamic due to the mobility of the nodes. It is common practice to deviate from the initial course of action when faced with such a situation. Therefore, approaches to controlling flexibility get a lot of attention from ad hoc network researchers. Because ad hoc network communication links are unsecured, MANETs with a high damage frequency will continue to perform poorly owing to mobility-induced packet losses, regardless of how cautious one is. It is challenging to get a data packet to its destination, however, since mistakes happen so often. Mobile devices confront the problem of short battery life since ad hoc networks are inherently scattered. To maintain the node's movability, size, and capacity, this kind of network places constraints on the node's dominating basis. Because of their combined processing and power, the nodes are bulky and inflexible. This means that no device other than a MANET may access this resource. Network partitions may occur often in an ad hoc network because nodes in the network are mobile. This sort of split might have a significant influence on the intermediate nodes in certain situations.

The ease of interception makes wireless communications vulnerable to security breaches. For unstructured networks, wireless transmission is the way to go. It is accessible from any of the connected devices simultaneously. If two devices are in line of sight, they will both be able to receive data sent via one of them. Consequently, any information or data sent within the network might be stolen by an intruder. Enemy espionage might lead to the disclosure of sensitive information, rendering the concealment useless [6]. In contrast to single-hop wireless networks, MANETs have a significant routing difficulty due to the growing need for unicasting, multicasting, and geocasting between nodes. This is a result of inconsistent network architecture and changes in user mobility. Because different nodes in the network have different expectations for service quality, MANETs face a significant obstacle.

Due to the increased difficulty in meeting the several tiers of priority requirements associated with quality of service [7], modern networks, particularly those supporting multimedia, need first-rate QoS management. Security is a major concern with MANET because of its wireless nature. The transmission of user data must be secure and risk-free. Enterprise MANET security might also be enhanced by using the least privilege principle. Combinations of two or more access control systems often combine their best features [8].

MANET Methods and Their Use The military might reap the benefits of Ad hoc networking by repurposing existing network infrastructure to facilitate the continuous flow of data among mobile vehicles, troops, and command centres; this would be an example of a novel use of MANETs. Companies may benefit greatly from collaborative computing in settings that aren't your typical office. Many groups of individuals who are trying to accomplish something get together in public places. In a confined area, such as a conference room or classroom, a number of individuals may use their computers to construct an ad hoc network and communicate in real time via a makeshift hypermedia network.

A second, more limited, use may be in a home network setting, where various gadgets could link directly to exchange data. Similar to PANs, Bluetooth networks can only support devices belonging to a single user. Bluetooth and other short-range MANETs could make it easier for many mobile devices, such as laptops and phones, to communicate with one another. Businesses may use ad hoc networks for emergency procedures in the case of a natural disaster such as a fire, flood, or earthquake. In the event that a transmission network is required immediately but the necessary infrastructure is not available, immediate action must be taken to save lives [10]. Mobile ad hoc networks (MANETs) are being used to remotely and locally control household appliances using networks of sensors. As an example, tasks related to weather observation instruments include keeping tabs on the health of various animals. Our range of services includes disaster cleanup, liberation operations, hospital diagnostic and record transfer, and on-site infrastructure repair. Academic networks for classrooms, auditoriums, and labs that use computers [10]

Conclusion

Despite its relative youth, MANET poses substantial challenges that must be overcome for maximum efficiency. Wireless systems, such as MANET, have it especially tough when it comes to network security. We can enhance our output by using MANET's capabilities. It may be possible to make the situation more safer with a few precautions.

References

1. Raja, M.L. and Baboo, C.D.S.S. (2014) An Overview of MANET: Applications, Attacks and Challenges.
2. Chitkara, M. and Ahmad, M.W. (2014) Review on MANET: Characteristics, Challenges, Imperatives and Routing N. Raza et al. 136 Protocols. International Journal of Computer Science and Mobile Computing, 3, 432-437.
3. Mohammad, S., Alsanabani, M. and Alahdal, T. (2014) Comparison Study of Routing Protocols

- in MANET. International Journal of Ad Hoc, Vehicular and Sensor Networks, 1, 1-9.
4. Odeh, A., Abdel Fattah, E. and Alshowkan, M. (2012) Performance Evaluation of AODV and DSR Routing Protocols in MANET Networks.
 5. Verma, S. and Singh, P. (2014) Energy Efficient Routing in MANET: A Survey. International Journal of Engineering and Computer Science, 3, 3971-3977.
 6. Mamatha, G. and Sharma, D.S. (2010) Analyzing the MANET Variations, Challenges, Capacity and Protocol Issues. International Journal of Computer Science & Engineering Survey, 1, 14-21. <http://dx.doi.org/10.5121/ijcses.2010.1102>
 7. Goyal, P., Parmar, V. and Rishi, R. (2011) Manet: Vulnerabilities, Challenges, Attacks, Application. International Journal of Computational Engineering & Management, 11, 32-37.
 8. Aftab, M.U., Nisar, A., Asif, D., Ashraf, A. and Gill, B. (2013) RBAC Architecture Design Issues in Institutions Collaborative Environment. International Journal of Computer Science Issues, 10, 216-221.
 9. Aftab, M.U., Habib, M.A., Mehmood, N., Aslam, M. and Irfan, M. (2015) Attributed Role Based Access Control Model. Conference on Information Assurance and Cyber Security (CIACS), Rawalpindi, 18 December 2015, 83-89. <http://dx.doi.org/10.1109/CIACS.2015.7395571>