ISSN: 2348 - 2117

International Journal of Engineering Technology and Computer Research (IJETCR)

Available Online at www.ijetcr.org

Volume 10; Issue 5; September-October; 2022; Page No. 01-11

Applications of Mobile Ad-Hoc Networks and the Challenges They Present

Priya Poonia, Pawan Raj

[1]**Research scholar, Yagyavalkya Institute of Technology**

[2]**Assistant Professor, Yagyavalkya Institute of Technology**

Conflicts of interest: Nil

Corresponding author: Priya Poonia

Abstract

In contrast to traditional wireless networks, Mobile Ad-Hoc Networks (MANETs) are ad hoc groups of mobile nodes that operate independently of one another (Smart phones, Laptops, iPads, PDAs etc.). As nodes join and leave the network, the network automatically adjusts its topology and routing table to facilitate the seamless transfer of data packets. The article focuses on the uses and difficulties of MANETs. Researchers will be able to understand MANET in its entirety, from its purposes and potential pitfalls to its many practical uses. By relying only on wireless connections, mobile nodes in a Mobile Ad Hoc Network (MANET) may send and receive data packets with one another without requiring a centralised network administrator. Offering a power-aware, secure routing protocol in such a network is challenging due to the dynamic nature of the topologies and the scarcity of available resources. In this research, we present a secure routing system that is both power-aware and reputation-based. A Krill Herd based Grasshopper Optimization Algorithm (KH-GOA) is developed, along with the reputation model and power, to construct a secure path from the starting node to the final destination. The reputation model takes into account a wide range of reputation parameters, including node mobility, actual capabilities, prior records, and reputation among neighbours. Reputation requirements for each node are analysed, and the KH-GOA approach, a combination of the Krill Herd (KH) and the Grasshopper Optimization Algorithm (GOA), is proposed for constructing a secure path from the source to the destination (GOA). The proposed KH-GOA-based routing protocol makes use of multi-objective factors such as reputation, power, distance, and latency.

Keywords:- MANET, MANET Challenges and Applications

Introduction

Due to advancements in wireless network technology, the internet field has spawned many new applications. One of the most promising areas for wireless network research and development is the Mobile AdHoc Network (MANET). Increased interest in mobile devices and wireless networks has made wireless ad hoc networks one of the most lively and active areas of communication and networking. Various mobile devices, such as laptops, smart phones, sensors, etc., are linked

together wirelessly to establish a mobile ad-hoc network. These units operate together to provide the crucial network capabilities in a decentralised fashion, giving the impression of a stationary administration. By acting as a standalone network or providing many points of access to cellular networks or the Internet, this architecture paves the door for a wide range of novel and exciting uses [1].

In a MANET, all of the nodes work together to determine the best path for a packet to take on its way to its final destination Each node in a network can only talk to other nodes within its broadcast radius R, even if the distance between them is significantly less than the transmission radius R. Without centralised support from an access point or base station, a multihop wireless ad hoc network cannot function. In a MANET, mobile devices must advance data-packets for one another in order to allow transmission between devices outside the transmission range. Mobile nodes in a network are untethered and may go anywhere they like. It is possible for the nodes to disconnect and reconnect to the network at will. Thus, a node often encounters changes in the connection states of the node with other nodes. The mobility of nodes in an ad hoc network, as well as other features of wireless transmission including attenuation, multipath propagation, interference, etc., pose increasing difficulties for MANET routing algorithms. The difficulties are exacerbated by the fact that many different types of nodes, each with limited resources, may be added to the network [2].

The overarching purpose of this study was to conduct an in-depth analysis of MANET routing protocols; specifically, 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; to evaluate and analyse these routing protocols under the various environments by using some parameters like WLAN delay, WLAN throughput, WLAN network load, FTP traffic sent and received by the nodes and ser; and to draw conclusions about the relative

Mobile Ad-Hoc Network

The term "mobile ad hoc network" (MANET) refers to a network of wirelessly connected, mobile devices that may form new groups on the fly. These networks consist of a collection of mobile nodes that are not tethered to a central hub but instead communicate with one another through wireless connections and may freely roam the landscape, causing the network's topology to shift and evolve in real time. Due to the short range of communication between nodes in a MANET, packets are relayed over numerous hops from the originating node to the destination node.

Mobile and Wireless Networks

Wireless networks not only allow users to connect from anywhere, but also help extend the network into new buildings and other areas that may not have a hardwired connection. As can be seen in Figure 1, there are two distinct kinds of these links: substructure networks and ad hoc networks. In wireless networks with an infrastructure, an access point (AP) is a device controller. Any device with an access point may join the network. The access point coordinates the interconnection of the BSSs to ensure that the path is always available (BSSs). Another drawback of utilising a network structure is the significant extra labour involved in maintaining routing tables [4]. Data-packet transport and reception are more difficult in Ad-Hoc or structure-less networks since there is no clear topology or centralised controlling point. There are many ways to categorise wireless networks, including single-hop, multi-hop, infrastructure-based, and ad hoc. Single-hop wireless networks relied on electromagnetic waves for communication between the base station (BS) and wireless devices. When using a multi hop wireless network, wireless nodes relay data from one node to another, and so on, until it reaches the base station.

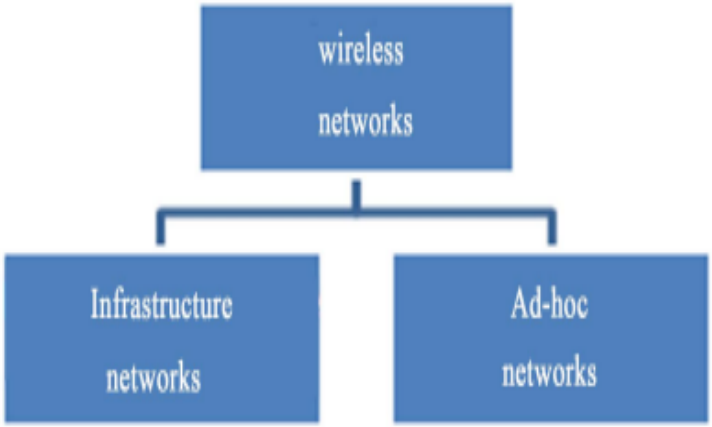

Figure 1. Classifications of wireless networks.

How MANETs Are Unique Independent of any external support system: MANET operates autonomously, without need for hierarchical organisation or supervision. Since everything operates in a decentralised P2P fashion, each node acts as a router on its own and creates its own data. When administrators of a network have to split their time across several nodes, fault detection and management become more challenging With multi-hop routing, every node acts as a router, forwarding data packets across mobile hosts. There isn't any kind of built-in router. Evolutionary topologies: As nodes randomly relocate throughout the network, the topology (often a multi-hop structure) is constantly evolving. Because of this, there will be shifts in traffic patterns, subdivisions within networks, and maybe dropped packets. Atypical capacities of links and nodes: Every gadget might have a different set of radio interfaces with unique transmitting and receiving capabilities.

These may also serve throughout a wide range of frequencies. These disparate radio capabilities of the nodes may lead to unstable connections. Because mobile nodes might have a wide variety of software and hardware configurations, the computing power they provide may also change. It may be difficult to plan network protocols and algorithms for such a heterogeneous system, since variables (such as power and channel availability, traffic load/distribution fluctuations, congestion, and so on) are constantly changing and must be taken into account. Action determined by energy input. Processor efficiency suffers on any portable device due to its limited battery life. This means that the features and functionality of any individual gadget are restricted. Each node's dual roles as a system and a router result in a net energy drain. Packer forwarding to other nodes consumes extra resources. Therefore, this becomes an even bigger issue in mobile ad hoc networks. The ability to expand the capacity of the network is a key challenge to the widespread adoption of such systems. The most well-known algorithms for managing networks today are incapable of functioning with dynamic or even moderately large wireless networks. High networks with a large number of nodes are common in many mobile ad hoc network applications, such as sensor networks and tactical networks. There are a number of challenges that must be overcome before such a network can be put into place. Problems with addressing, routing, location management, configuration, interoperability, security, large capacity wireless technologies, etc

Benefits of MANET

Extremely useful when a reliable, cost-effective, and widely available fixed-line network is unavailable or impractical to build. Fast setup requiring little user input, please. There is no need for extensive preparation or careful placement of base stations. Connecting an ad hoc network to the Internet or the World Wide Web allows for the

incorporation of a wide variety of devices and the access of more users to the network's services. Their capacity, range, and energy efficiency all argue for their usage in conjunction with preexisting cellular networks to increase coverage and connection. It is the goal of MANET, which is designed to take use of the upcoming 4G architecture and its services, to provide ubiquitous computing environments that help people get their work done, get the information they need, and stay in touch no matter where they are or what device they're using [5].

Changes in the MANET Environment Programming for MANETs takes into account the network's dynamic topology and all of its permutations. Because each node in a MANET performs the same functions, this configuration is known as a symmetric environment. In a MANET, wireless mobile nodes link with one another without centralised command or established hierarchy. In contrast to expanse nodes, which rely on their neighbours to relay packets, those that are in close proximity to one another may communicate with one another wirelessly. This node may function as either a router or a host in a MANET. Nodes in a MANET may quit or join the system at any moment, creating a dynamic environment similar to that of a fully maintained network.

The Oddball Skills in MANETs include transmission sequences and radio sequences that may evolve over time. Nodes will vary in their mobility, battery life, and computational power. As part of their irregular responsibilities, certain network nodes may act as cluster heads while others may act as packet trackers. Unicast, multicast, geocast, content-based addressing, host-based addressing, and capability-based addressing are just a few examples of how traffic characteristics might vary across various ad hoc networks. It is possible for MANETs to cooperate with and even coexist in a conventional network arrangement. People in the airport lounge, cabs, the military, and secure networks all have various mobility arrangements. Data traffic patterns, network layout, and radio interference all have a role in how effectively a mobile ad hoc network functions. Characteristics of mobility, such as velocity, directional bias, predictability, movement plan, and feature consistency among nodes, are all listed in [6].

MANET Problems:

The following problems highlight MANET's deficiencies and constraints that must be overcome: Wireless networks have a limited transmission range since the radio group is constrained, hence the quantity of data they can send is significantly less than that of a hardwired network. This means that wireless network routing protocols must make efficient use of available bandwidth. Keeping the overhead to a minimal is one way to accomplish this goal. Constraints on routing algorithms for maintaining the topographical information are imposed by the limited transmission range. Keeping track of topological information on each node in a MANET requires extra controller overhead, which reduces available bandwidth even more, due to the frequent changes in topology. Variables of the wireless connection over time: Path damage, degrading signal strength, intervening transmitters, and physical obstacles are only some of the broadcast diseases that might affect a wireless channel.

These parts are impervious to the sequential nature, high data rate, and constant nature of these wireless communications. The extent to which these factors impede transmission is dependent on environmental factors and the adaptability of the receiver and the emitter. Nyquist's and Shannon's theorems are two important limits that may be measured, since they govern the capacity to transfer information at different data levels. As a broadcast medium, wireless communications: All devices in its direct transmission coverage area establish the broadcast character of the radio channel, such as broadcasts produced by a device. No other device in the immediate area, including the sender, is required to transport data while a device is receiving data. When a device's communications aren't going to disrupt any ongoing session, it may get access to the shared media. Data-packet

collisions are common in wireless networks due to the high number of devices that might be active at once.

The network itself may develop a hidden terminal problem or transmit a storm. The phrase "concealed terminal problem" refers to the destruction of data-packets at a reception device as a result of direct transmission from nodes that are outside the straight communication series of the transmitter but inside the communication series of the receiver. Errors in transmission that cause packet loss: Extraordinary BER in the wireless channel, larger crashes due to the existence of unseen terminals, intervention, position-dependent controversy, unidirectional associations, regular pathway breakages due to device movements, and the integral declining characteristics of the wireless passage all contribute to the advanced packet damage practised by ad hoc wireless networks.

The system topography in an ad hoc wireless network is very dynamic as a consequence of node motion; as a result, a continuously occurring meeting experiences multiple pathway breakages as a result of this dynamic topography. Changes to the planned course are commonplace when in such a predicament. Flexibility management is therefore a major area of study for ad hoc networks. Mobility-induced packet losses: Because ad hoc network communication links are unsecure, MANETs with a high damage frequency will function poorly while using successively cautious practises. Nonetheless, supplying a data-packet to its destination is challenging due to the high frequency of error. Battery life is a major issue in ad hoc networks because of the limited resources available to mobile devices. In order to maintain the node's movability, size, and capacity, nodes in such a network have limitations imposed on its dominance foundation. The nodes are bulky and immobile because of their accumulated power and processing capabilities. Therefore, only MANET devices are permitted to make use of this asset. Network partitions may occur often in an ad hoc network because nodes may be easily moved, creating partitions. The effects of such a split on intermediate nodes may be profound in certain situations.

The security concerns associated with the ease of eavesdropping on wireless transmissions: Using wireless transmission for ad hoc networks in the wild. It is something that all connected gadgets have access to simultaneously. Any gadget in a direct line of connection with another device will recognise the data that has been sent via it. As a result, any data or information transferred inside the network is at risk of being stolen by an intruder. If the opponent can deduce information via spying, the concealment will be broken [6]. In contrast to single-hop wireless networks, the increased need for unicasting, multicasting, and geocasting across MANET nodes presents a significant routing difficulty. This is due to fluctuations in network architecture and variations in user mobility. The varying requirements for service quality across the network nodes poses a significant difficulty for MANETs.

These networks need top-notch QoS management, in particular for multimedia, since it is more challenging to meet the many degrees or priority demands associated with quality of service [7]. As a result of its wireless nature, MANET's security is a major concern. Users' information passing from one node to another must do so securely and without loss. Organizational MANETs may also benefit from the security enhancements offered by the least privilege concept. In addition, there exist hybrid versions that combine the best features of two different access control systems [8].

Methods and Uses of MANET Differentiating uses for MANETs include: When it comes to the military, Ad-Hoc networking may help the army take use of established network technology to reliably maintain any data connection between moving vehicles, troops, and command centres. Cooperative work: The need for collaborative computing is especially important outside of the typical office setting and environment in order to assist commercial settings. People like to gather in a public place in order to discuss and collaborate on any given project. Confined area: Ad-Hoc networks

may easily associate with immediate, also temporary hypermedia network through laptop computers for sharing the information with all the participants, for example in a classroom or conference setting.

The home network setting, where various gadgets may connect directly to exchange data, may also be a viable and limited-level use. Similar to a PAN, a Bluetooth network has a limited range of devices that typically belong to a single user. Communicating between several mobile devices, such a laptop and a cell phone, may be simplified using a short-range MANET, like Bluetooth. Ad hoc networks have the potential to be employed in the business world for rescue and emergency procedures during times of natural disasters like floods, fires, and earthquakes. Where transmissions infrastructure is broken or nonexistent, and where rapid creation of a transmission network is necessary, emergency saving methods should be used [10]. Sensor Networks:

Using Mobile Ad Hoc Networks (MANETs) to Control Household Appliances, Locally and Long-Range. Keeping tabs on things like animals. Tasks associated with weather monitoring equipment. Services in case of emergency: disaster clean-up, liberation operations, hospital patient diagnostic and record transfer, and fixed-site infrastructure repair. Communications infrastructure for computer-based meeting rooms, classrooms, and labs [10] in the educational sector.

Results & Discussion

Statistical evidence suggests that the assumption that existing tactics use more energy is false. The proposed approach surpasses existing solutions and has shown itself capable of efficiently deploying the specified services. In the context of a flooding attack, the research shows latency, detection rate, throughput, and power consumption. Time lag analysis of the KH-GOA vs the status quo. At 30 seconds, the measured delays for AOMDV-SAPTV, Secure reputation-based routing, FR-DSR, and the proposed KH-GOA are 0.112 milliseconds (ms), 0.103 milliseconds (ms), 0.113 milliseconds (ms), and 0.098 milliseconds (ms), respectively. The proposed method has the lowest latency compared to other possible solutions. Depicted in Figure 5b are the results of a research that compared the detection rates of the AOMDV-SAPTV, Secure reputation-based routing, FR-DSR, and proposed KH-GOA across time intervals of 0 to 50s.

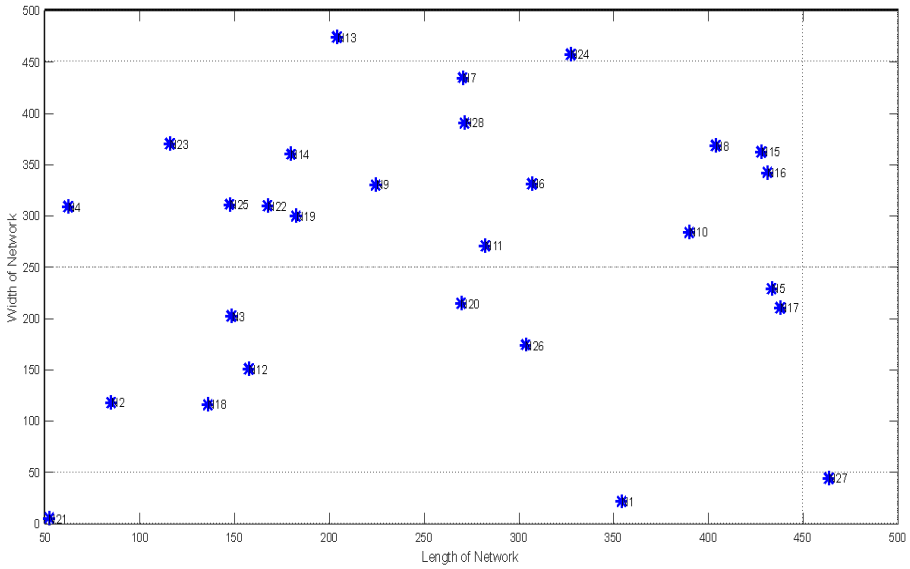

Fig 2: Network Creation

Nodes are spread out throughout a 100-meter-long and 100-meter-wide network, as shown in Figure 2. The simulation is built using MATLAB code. In Figure 2, the cyan node represents the black hole that is both malevolent and creates a false route. We tried running the simulation with stricter penalties in place, and saw frequent changes from prohibited to allowed nodes. There were three possible outcomes for calculating the longevity factor: node in neighbourhood, valid lifespan; node in neighbourhood, invalid lifetime; and node not in neighbourhood, invalid lifetime. Either state for Node is equally possible. For this reason, we have lowered the lifespan factor to 0.33. Since we wanted wp and wss to be very influential, we kept them at 0.9 and 0.8, respectively, but wjs is only 0.5, therefore this view cannot override the views with weights wp and wss. We kept wp and wss at 0.8 and 0.7 and 0.6, respectively, but found that the weights were diluted when they were combined. The following cases were taken into consideration

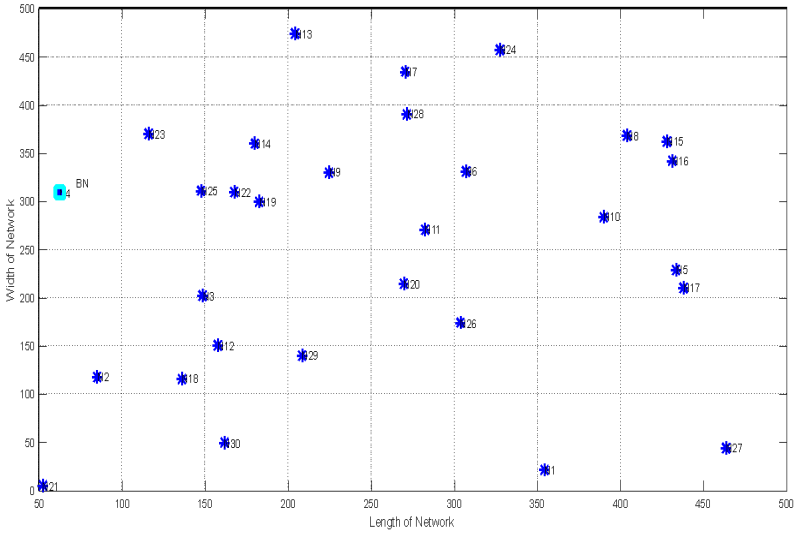

Fig 3: Identification of black hole node

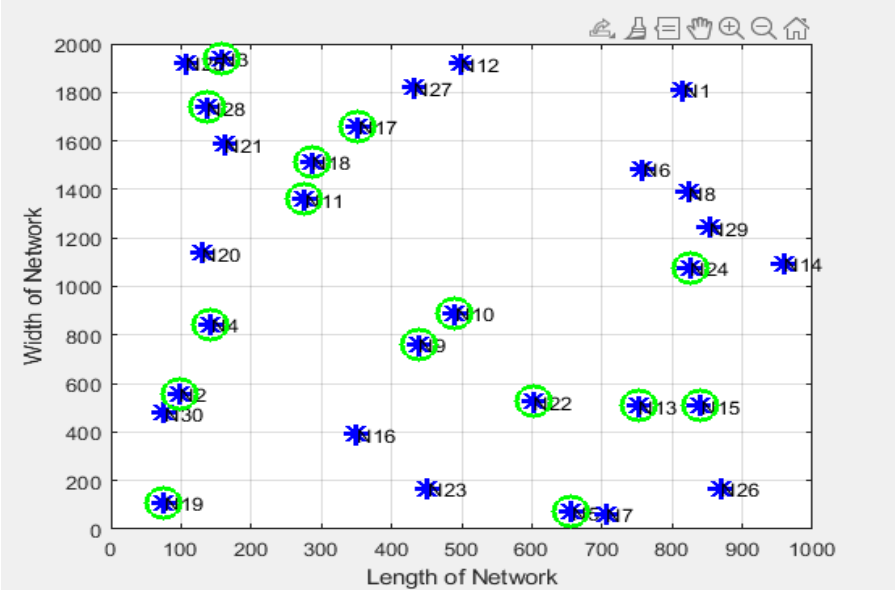

Fig. 4- Identification of the node of a black hole

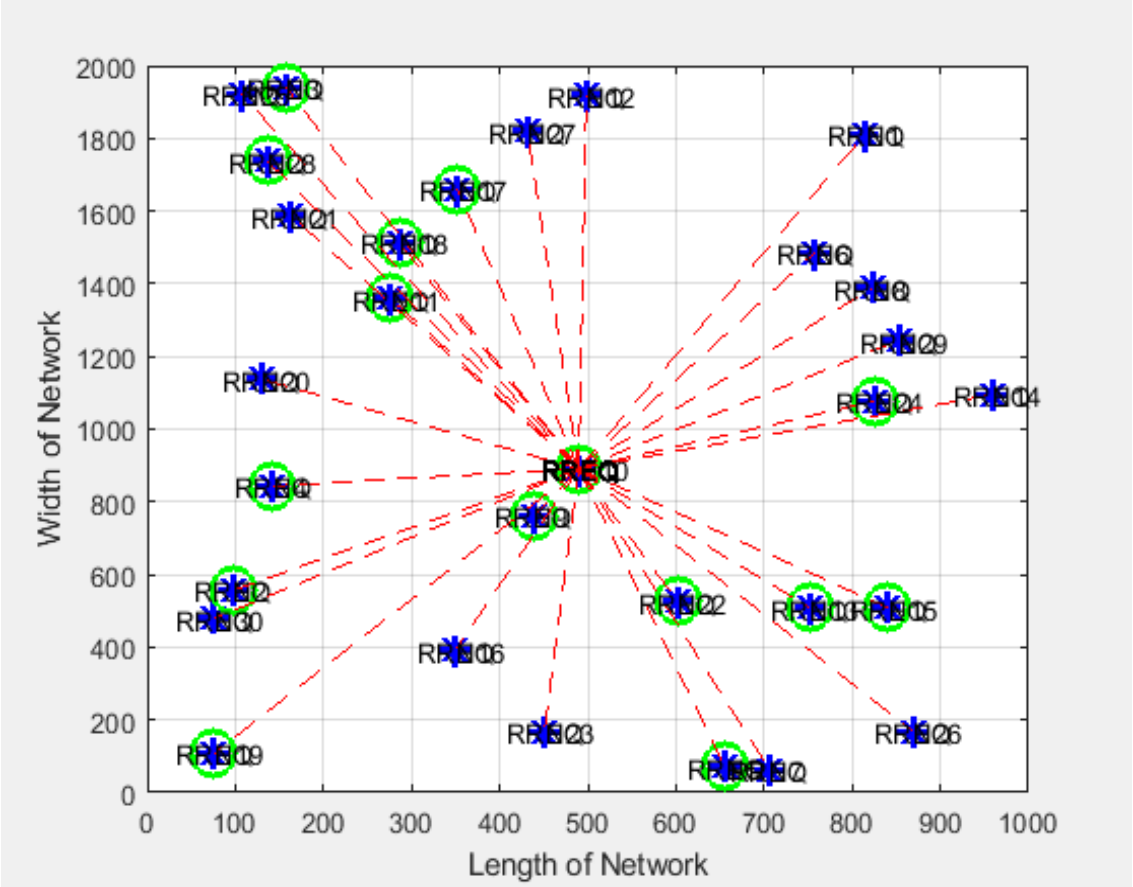

Fig 5- Each of the node of a connected

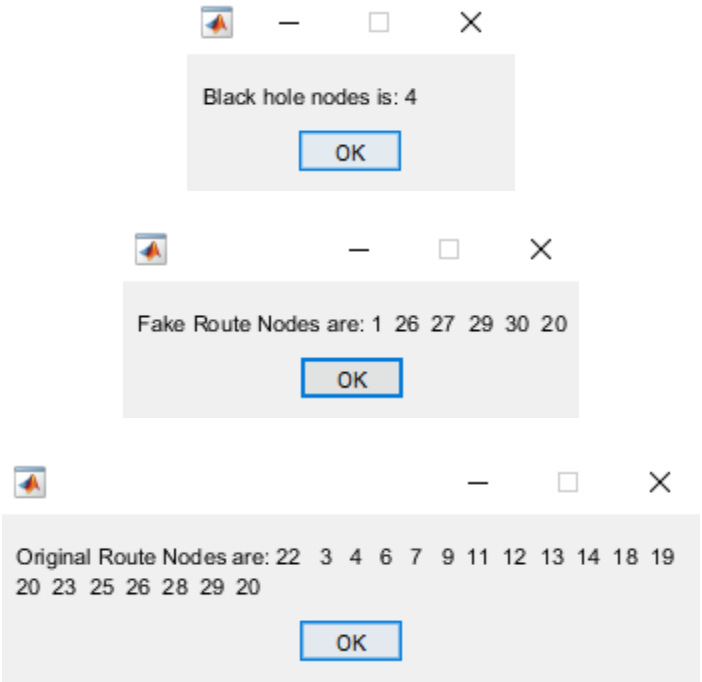

Fig 6: Ids of nodes (Black Hole node, Fake Rout, Original Route after Mitigating)

Fig. 6 displays the black hole node id, the fake route node ids generated by the malicious node during an attack, and the true node ids retrieved after the attack's effects were mitigated in the sensor network.

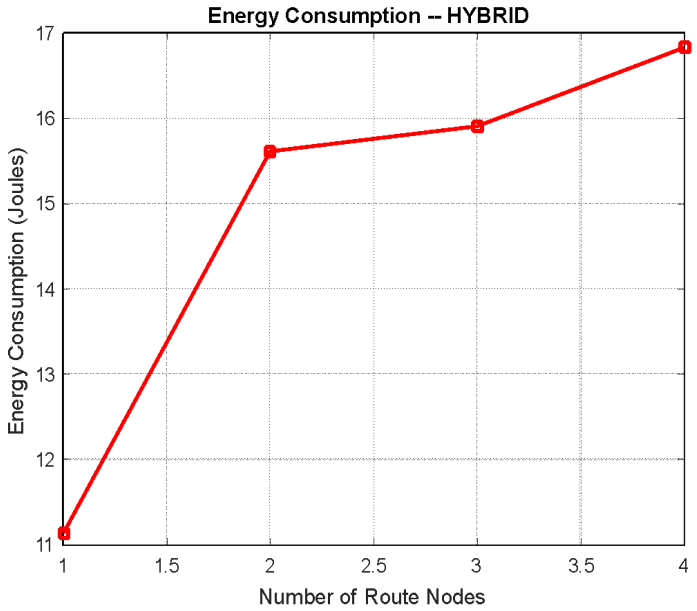

Fig 7: MANNET Energy consumption

Figure 7 shows the energy usage relative to the number of nodes executing or participating in the route, showing that the hybrid approach may achieve reduced energy consumption and prolong the node's lifespan.

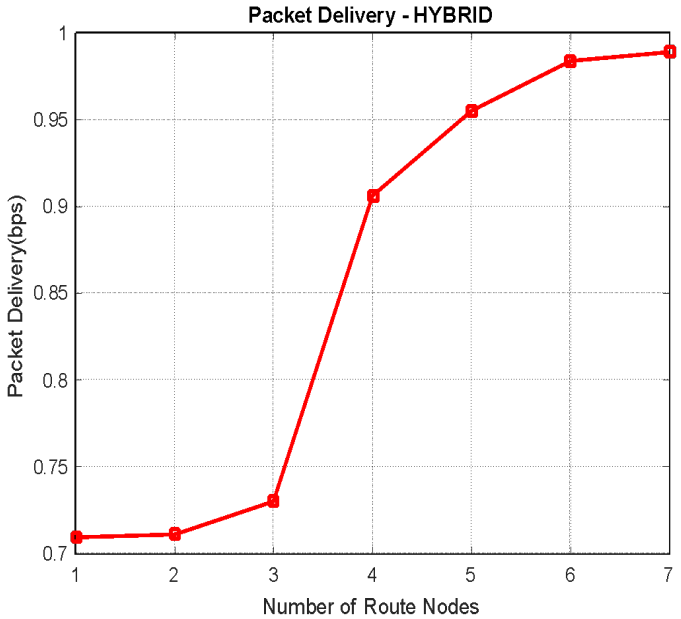

Fig 8: MANET Delivery Packet

Figure 8 shows the network's packet delivery in relation to the maximum possible, proving that the suggested method can achieve high packet delivery in terms of successful packet deliveries, as the line is closest to 1.

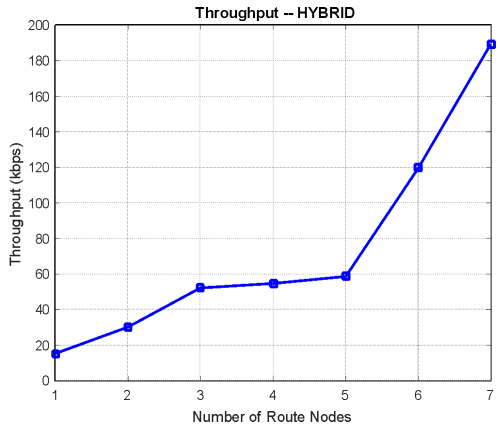

Fig 9: Throughput

The network throughput is shown in (KBPS). The high throughput seen in Fig. 9 is evidence that our suggested technique is effective at effectively transporting data over an unattacked network.

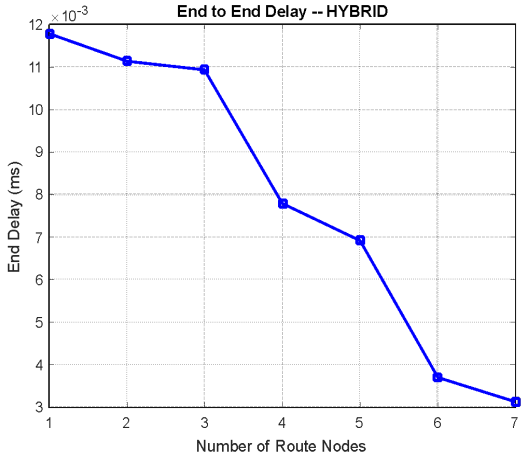

Fig 10: End Delay

With a decreased end latency from the source to the destination, as shown in Figure 10, the proposed method ensures high packet delivery and minimal packet losses.

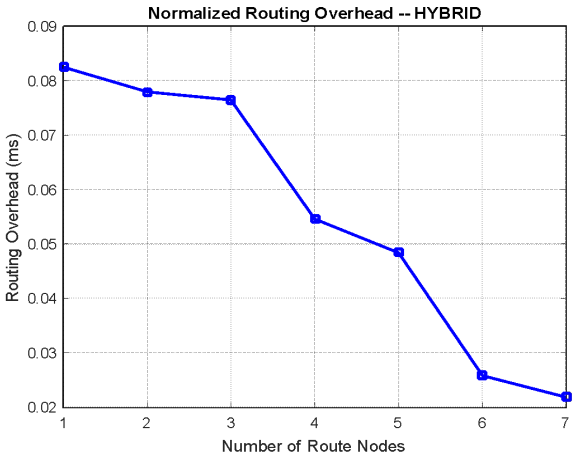

Fig 11: Routing Ove

rhead

A sensor network's routing overhead (shown in Figure 11) is a crucial feature that must be small to ensure minimal overhead and few packet collisions between nodes. These settings need to be tightened up as the number of routing nodes increases.

Conclusion

Emerging though it may be, MANET nevertheless presents significant obstacles that must be addressed in order to get optimal performance. Network security is a major issue across the board, but it is particularly problematic for wireless systems like MANET. Using MANET's capabilities, we can improve our output. A few security measures may greatly improve the situation's safety.

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
10. Chitkara, M. and Ahmad, M.W. (2014) Review on MANET: Characteristics, Challenges, Imperatives and Routing Protocols. International Journal of Computer Science and Mobile Computing, 3, 432-437.