# MANETS: A Study of Various Routing Algorithms

Geet Kiran Kaur
Assistant Professor,
CSE Department
Chandigarh University,Gharuan
Punjab India

Charanpreet Kaur
Assistant Professor,
CSE Department
Chandigarh University,Gharuan
Punjab India

Abhishek Sharma
Assistant Professor,
CSE Department
Chandigarh University,Gharuan
Punjab India

***Abstract*— Our everyday lives have become more and more dependent on computers in the last several years as their importance has grown. Thus, new networking needs have emerged from consumers. Wired solutions could no longer meet the rising demand for Internet access, e-mail reading and sending, and access to a wide range of data from almost any location. Ad-hoc networks are the solutions to this goal. This study examines the many elements of routing and privacy protection in mobile area networks**

***Keywords— Manets, Ad-hoc network, Routing, Privacy preservation Introduction***

## I. INTRODUCTION

Selecting a MANET is made up of a network of wireless devices that may communicate freely and cooperate to send shipments on behalf of one another. MANET does not need centralized management or a permanent infrastructure [1]. Due to their limited broadcast range, remote mobile nodes interact through multichannel pathways. MANETs are an interesting alternative for various applications, including combat communications, island or ship communication, disaster recovery operations, conference calls the need for a variety of applications, including combat communications, island or ship communication, disaster recovery operations, conference calls without the need for cable infrastructure, and correlated information exchange. Each mobile node participates in data forwarding within MANET; each mobile node participates in data forwarding on the other's behalf. Self-organizing protocols are used, and routing discloses node identities, neighbors, and communication destinations. Additionally, many modes of action need nodes to reveal their actual position openly. Additionally, nodes need to promote their online presence profiles in order to contribute to the network, which is very disagreeable. Military and civilian MANETs may regard information exposure as undesirable; a node must be able to maintain its uniqueness, position, and private correspondence in order to remain anonymous [2]. Fig 1. illustrates the MANET architecture.

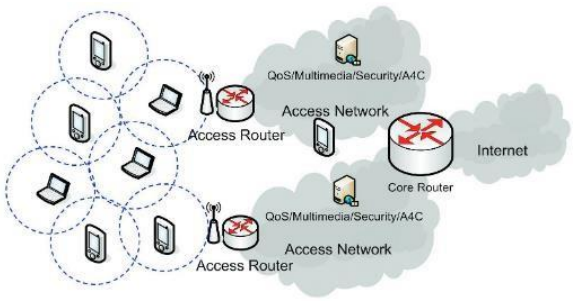


Fig. 1. Manet Architecture

In contrast to wired networks, any anonymous solution has to overcome the inherent limitations of wireless broadcasting which makes it vulnerable to eavesdropping and makes do with fewer resources. Because broadcast media trafficking is so easily analyzed, simple measures like encrypting packets are worthless [3]. It is thus very difficult to keep private information secure on MANETs.

## II. ROUTING

MANET is self-distributing and decentralized. Network topology is constantly changing and decisions are made in a dispersed manner by the nodes in MANET. The dynamic nature of the network has made MANET routing a difficult undertaking, and wireless communication has become error-prone [4]. MANET aspires to provide security, accessibility, dependability, QoS (Quality of Service), and scalability. When packets of information are sent from one node to another, the process is known as routing. An Ad-hoc network's topology is subject to rapid change, which makes packet routing a challenge. Network traffic is controlled by a routing protocol, which also selects the most efficient route to the destination. There are three types of routing protocols.

### *A. Table Driving Protocol:*

It's a proactive routing protocol. In which, each node preserves complete network topology information by continually assessing the route to each node, and these protocols attempt to uphold reliable, up-to-date route information from each node on the network.

### B. *On-Demand Routing Protocol*

On-demand routing protocol, a source node initiates and responds to the development of routes. In order to go to a certain location, each node on the network initiates a route-finding process. After finding a route, this process is finished. This route will be sustained by part of the route maintenance until the destination can no longer be reached at any time from the source of the route become obsolete. Adhoc on-demand routing vector protocol is an improvement over the DSR protocol. It was developed to overcome the disadvantages. of an existing protocol. In the existing protocol, data packets were transmitted from one mobile node to the other node after the route is discovered. The data packet includes the information of the complete path in its header. As a result, the size of the data packet increase, as the length of the total route increase when the size of the network grows. resulting in the slowdown of the entire network. Ad-Hoc On-Demand Vector Routing protocol was developed as a solution. The primary difference is in how the route is stored; AODV keeps it in the routing table in contrast to the data packet's header in DSR.

### C. *Hybrid Routing Protocols*

Table-driven and On-demand protocols both have some advantages. To take benefit from both the approaches the third kind of protocol was proposed. The hybrid protocol combines both approaches. Proactive operations are confined to a narrow domain in this case, whereas reactive protocols are used to identify nodes outside of these domains. A zone routing protocol is based on the principle of hybrid routing. In a zone routing protocol, the complete network is segregated into zones. For routing the exact position of the source and the destination node is determined. When both nodes are found in the same zone, table-driven routing is employed to route data packets between them. And if the mobile nodes are found in separate zones, on-demand routing is employed to connect them.

A comparison of table routing protocol, on-demand routing protocol, and hybrid routing algorithm is given in tabular format below

TABLE I. COMPARISON OF ROUTING ALGORITHMS

| Parameters | Routing Protocols | | |
|---|---|---|---|
| | **Table-driven** | **On-Demand** | **Hybrid** |
| Topology distribution | Periodic | On-demand | Both |
| Network infrastructure | Flat and hierarchical | Flat | Flat and hierarchical |
| Route formation delay | Less | More | Average |
| Storage | More | Less than proactive | Average |
| Route accessibility | Forever | When required | Average |
| Communication Overload | More | Less | Average |
| Protocols used | DSDV,WRP, GSR,GPR | DSR, AODV, ABR | WARP, ZRP |

The routing protocol must take security into consideration. MANET routing protocols often lack the necessary security. In general, the wireless environment is very vulnerable to a wide range of threats and assaults. Due to the wireless nature of MANETs, the tactics used to attack them are greater in size than their cables [7]. At the physical layer, denial of service assaults may be avoided using encrypted or frequency-hopping propagation spectrum; however, at the route level, authentication for node communication, non-removal, and encryption for private networks to prevent hostile organizations are necessary. A hybrid protocol combines the benefits of many routing methods, which are often favored [8]. To prevent loading the protocol, it should be far more reactive (responding on-demand) than proactive (using a periodic refresh of the information). The routing protocol must be aware of the QoS associated with the destination pair's latency and bandwidth and be able to validate its endurance in real-time so that the application can depend on it

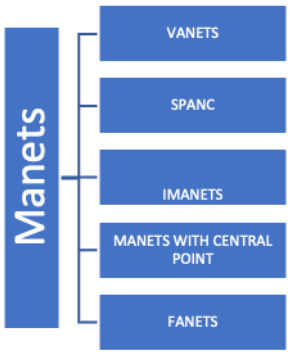

Fig. 2. Types of Manets

## III. TYPES OF MANETS

MANET is an acronym for Mobile ad-hoc Network, often known as an ad-hoc wireless network or wireless ad-hoc network. They are made up of a collection of wirelessly linked mobile nodes that form a self-configuring, self-healing network without the need for permanent infrastructure. MANET nodes are allowed to migrate freely due to the frequent changes in the network structure.

- VANETs – it is a variant of manet in which vehicles communicate with each other as well as other equipment through a secure channel to construct a network[20].
- SPANC – It is a variant of an ad-hoc area network that uses the underlying hardware of smart handheld devices. Wi-fi and Bluetooth technology is leveraged to create a network with the need to depend on the cellular area network[1].
- iMANETS- This is a variant on manet which is compatible with internet protocols.it combines

internet technology and mobile nodes to create a manet network.[1]

- MANETS WITH A CENTRAL POINT. In this arrangement, multiple Manets are connected together using a Hub
- Manets for military or tactical use: this is used for defense purposes high confidentiality mobility rapid routing are the requirements for these Manets.
- FANETS also known as Flying Ad hoc Networks)– includes unmanned aerial vehicles (commonly known as drones). Connects rural places and enables,

## IV. Privacy Preservation in Routing Algorithms

Maintaining privacy is critical for an ad hoc network that requires enhanced privacy protection. The MANET's dynamic and movable character is critical for protecting the network against complex security assaults [9]. Privacy in communication has become a vital security need for protecting mission-critical communications with communication infrastructure. It is particularly accurate for MANETs due to the dynamic nature of communication nodes and the nature of wireless communication.
Some fundamental terminologies include the following:

- Privacy is sometimes referred to as Anonymity. It is referred to as the state that is undecided within the collection of topics and is abbreviated as SoA. (Set of Ambiguity). Generally, anonymity is classified into three categories: sender, recipient, and connection. Sender anonymity implies that a message is not associated with any specific sender and that no message is associated with any particular sender. Similarly, receiver anonymity implies that the communication cannot be traced
  back to a few recipients and that the recipient cannot contact any message. The term "relationship anonymity" refers to the fact that the sender and receiver are unrelated. One may argue that the sender and receiver are not conversing, despite the fact that they are clearly engaging in certain exchanges [11]. Relationship anonymity is less secure than any sender's anonymity combined with the recipient's anonymity. The aforementioned anonymities are sometimes referred to as complete anonymity since they assure that the receiver, sender, or communication connection cannot be determined from a sent message.

- Trust is often drawn from social science and quantified as the subjective belief degree on the behavior of a given entity. The two types of trust are Reliability trust and Decision trust [12]. The term "reliability trust" refers to the subjective likelihood that a user A predicts that another user B will do a given action based on the user's welfare. Decision trust is the calculation by which a user is excited to rely on someone in a certain situation by the use of security, even when the consequence is likely to be unpleasant. Due to the unique properties of MANETs and the inherent unreliability of wireless media, confidence in MANETs should be exercised with caution.

- There are three sorts of attacks: reconnaissance, access, and denial of service. Reconnaissance is both an attack-type and an attack phase. Before trying to gain access to or impair network resources, intruders often conduct reconnaissance on the target network. Reconnaissance on a target network is seen as an assault. Reconnaissance is the acquisition of data about system resources, vulnerabilities, or services by an unauthorized party. Typically, reconnaissance assaults precede access and denial-of-service attacks. Hackers must, of course, be aware of what is accessible for attack prior to initiating any breach. The term "access" encompasses a broad range of attacks requiring an

- intruder to get access to a protected system without authorization in order to manipulate data, elevate privileges, or just gain access to the system in the first place. Attempts to gain system access, modify data, or increase privileges are all examples of "access attacks.". The goal of a denial-of-service attack (DoS) is to disable, damage, or crash network resources in order to prevent their intended users from using them. E-businesses confront one of the most devastating sorts of attacks: cyber-terrorists trying to block clients from accessing the company's online shop. As a result of this form of assault, the target corporation will be unable to execute its operations.

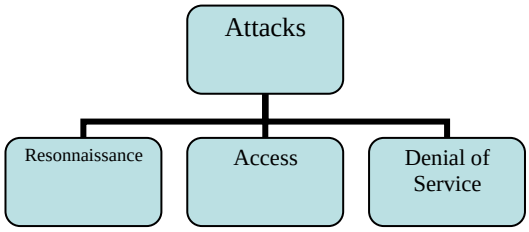


Fig. 3. Classification of attacks

## V. Anonymity in Routing Algorithms

Anonymity may not be required in civilian applications or in vital military applications. Consider MANET, which was brought to a halt on the battlefield. Anonymous routing methods provide secure communication through a concealed node identity, and traffic analysis attacks in the external viewer are banned. In MANETs, anonymity encompasses the uniqueness and anonymity of data sources, destinations, and the route itself. Due to the similarity and site anonymity of the sources and destinations, it is difficult to apply for different nodes to have their original identities and accurate locations as sources and destinations [14]. MANET's

anonymous routing technologies ensure the secrecy of network nodes and identities. Due to the network's dynamic nature, MANET routing is seen as a dangerous undertaking, and wireless connection has evolved into a highly error-prone MANET [4]. MANET desires security, accessibility, dependability, QoS (Quality of Service), and scalability. Routing is the process of transporting packets or data from a source node to a destination node. Because the ad hoc network's topology changes rapidly, routing packets becomes challenging. However, there is anonymous middleware that works between the application and the network layer. Because topology routing does not need node location information, location anonymity is not required [15].

TABLE II. ANONYMOUS DATA

| S.no | Anonymity dataset | | |
|---|---|---|---|
| | ***Sex*** | **Pin code** | **Salary** |
| 1 | Male | 110110 | >50k |
| 2 | Female | 110111 | >150k |
| 3 | Male | 110101 | >100k |
| 4 | Female | 110001 | >50k |
| 5 | Male | 110101 | >100k |
| 6 | Female | 110112 | >150k |

## VI. ADVANTAGES AND DISADVANTAGES

A mobile ad-hoc network is very useful in situations in which permanent infrastructure is relatively expensive or not possible. Manets do not require much human intervention as heavy installations are not required. It has a building capability of 4G architecture. Manets are compatible with the internet. Manets are flexible and can extend coverage and connectivity. Although it has many positives, there are some challenges like no centralized authority, limited transmission ranges, and updating information in the nodes of the mobile network. Battery constraint among others[22].

## VII. CONCLUSION

Wired solutions could no longer meet the rising demand for Internet access, e-mail reading and sending, and access to a wide range of data from almost any location. Ad-hoc networks are the solutions to this goal. This study examines the many elements of routing and privacy protection in mobile area networks This paper summarizes the concept of MANET with its key points. It will help the researchers to understand the various routing algorithms and provide a direction ti their research.

## REFERENCES

[1] Rashid, S., & Wadhwa, S. (2016). EAACK-A Secure Intrusion Detection System for MANET: SURVEY.

[2] Muthusenthil, B., &Murugavalli, S. (2017). Privacy preservation and protection for cluster based geographic routing protocol in MANET. Wireless Networks, 23(1), 79- 87.

[3] Amiruddin, A., Ratna, A. A. P., & Sari, R. F. (2017). New Key Generation and Encryption Algorithms for Privacy Preservation in Mobile Ad Hoc Networks. International Journal of Communication Networks and Information Security (IJCNIS), 9(3).

[4] Bahri, L., Carminati, B., Ferrari, E., & Tran, N. H. (2015, June). Privacy preserving decentralized identity validation for geo-social networks over MANET. In Proceedings of the 7th International Workshop on Hot Topics in Planet-scale mObile computing and online Social neTworking (pp. 7-12). ACM.

[5] Reddy, M. K., &Ponnapalli, V. L. N. (2017). Performance Analysis on Routing Protocol in Mobile Ad-hoc Networks (MANETS). IJRCCT, 6(11), 312-318.\

[6] Li, T., Ma, J., & Sun, C. (2017). SRDPV: secure route discovery and privacy- preserving verification in MANETs. Wireless Networks, 1-17.

[7] Joshi, S., & Mishra, D. K. (2016, November). A roadmap towards trust management & privacy preservation in mobile ad hoc networks. In ICT in Business Industry & Government (ICTBIG), International Conference on (pp. 1-6). IEEE.

[8] Prasad, A. S. V., &Venkanna, V. (2017). Minimizing Query Delay And Prediction of File Availability Of Nodes In MANET. IJRCCT, 6(01), 011-013.

[9] Guo, M., Jin, X., Pissinou, N., Zanlongo, S., Carbunar, B., &Iyengar, S. S. (2015). In- network trajectory privacy preservation. ACM Computing Surveys (CSUR), 48(2), 23.

[10] Ratna, A. A. P., & Sari, R. F. (2017). New Key Generation and Encryption Algorithms for Privacy Preservation in Mobile Ad Hoc Networks. International Journal of Communication Networks and Information Security, 9(3), 376-385.

[11] Murugavalli, S. (2016). Privacy preserving with location verification hybrid routing in hierarchical Manet.

[12] Madhavan, P., Malathi, P., &Abinaya, R. (2015). Effective Path Discovery Among Clusters for Secure Transmission of Data in MANET. In Artificial Intelligence and Evolutionary Algorithms in Engineering Systems (pp. 499-509). Springer, New Delhi.

[13] Gao, C., Ma, J., & Zhang, S. (2015). A collaborative self-governing privacy- preserving wireless sensor network architecture based on location optimization for dynamic service discovery in MANET environment. International Journal of Distributed Sensor Networks, 11(8), 456146.

[14] Borekar, P. P., &Muhkerjee, N. (2015). Enhancing Privacy Preservation using S-ALERT Protocol to Diminish Routing Attacks in MANETs. International Journal of Computer Applications, 117(19).

[15] Santhi Raju, G., Soma Sekhar, B. V., & Naidu, U. G. (2018). The Novel Security Framework for MANETs Using Secure Routing and Communication Security Protocols. IJRCCT, 7(2), 064-074.

[16] Ahmad, M., Salam, A., & Wahid, I. (2018). A survey on Trust and Reputation-Based Clustering Algorithms in Mobile Ad-hoc Networks. Journal of Information Communication Technologies and Robotic Applications, 59-72.

[17] Rao, R. Lakshmana, B. Satyanarayana, and B. Kondaiah, "Performance of CBIDS on AODV Routing Protocol against Black hole attacks in MANET,"2018

[18] Sen, B., Meitei, M. G., Sharma, K., Ghose, M. K., & Sinha, S. (2018). A Trust-Based Intrusion Detection System for Mitigating Blackhole Attacks in MANET. In Advanced Computational and Communication Paradigms (pp. 765-775). Springer, Singapore.

[19] Verma, Roshani, Roopesh Sharma, and Upendra Singh, "New approach through detection and prevention of wormhole attack in MANET," Electronics,

[20] Chaturvedi, Kamal Nayan, Ankur Kohli, Akshat Kamboj, Shobhit Mendiratta, and Nitin Rakesh, "NS2 Based Structured Network Attack Scrutiny in MANET," Networking Communication and Data Knowledge Engineering, pp. 99- 111, 2018.

[21] Sandeep N. Kugali , Sneha Kadadevar, 2020, Vehicular ADHOC Network (VANET):-A Brief Knowledge, INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT) Volume 09, Issue 06 (June 2020),

[22] Alo, R. U., Stanly, N. I., & Onwe, N. F. (2018). Mobile Ad Hoc Network (MANET): Applications, Benefits and Performance Issues in a Global Positioning System. International Research Journal of Engineering and Technology (IRJET), 5(11).