Libyan Open University Journal of Applied Sciences (LOUJAS)
Volume 2 - Issue 1 - 2026 - Pages 427-436

A Comprehensive Study of Ad Hoc Networks: Routing, Challenges, and Security

Aziza Mohamed Abudina *[1],Reem Saad Mosbah Abdallah [2], Aisha Ahsein Douma[3], Sarah Sasi Alzarqani khaleefah [4].
[1] Department of Information Technology, College of Engineering Technology , Janzour-Libya
[2] Computer Department, Higher Institute of Science and Technology , Tamzawa Al-Shatea,Libya
[3] Department of Computer Engineering, Atilim University, Ankara, Turkey.
[4] Higher Institute of science and Technology ,Tarhuna, Libya
*** Email (for reference researcher):** abudinaaziza6@gmail.com

دراسة شاملة لشبكات Ad Hoc: التوجيه، والتحديات، والأمن

عزيزة محمد سعيد أبودينة[1]* ، ريم سعد مصباح عبدالله[2] ، عيشه احسين دومه [3]، ساره ساسي الزرقاني خليفه[4]
[1] قسم تقنية المعلومات، كلية التقنية الهندسية – جنزور، ليبيا
[2] قسم الحاسوب، المعهد العالي للعلوم والتقنية – تمزاوة الشاطئ، ليبيا
[3] قسم هندسة الكمبيوتر،جامعة أتليم، أنقرة، تركيا
[4] المعهد العالي للعلوم والتقنية ترهونة، ليبيا

Received: 12-02-2026; Accepted: 25-04-2026; Published: 15-05-2026

Abstract:
Wireless Ad Hoc Networks are highly dynamic, self-organizing networks that do not rely on any fixed infrastructure, allowing mobile nodes to communicate directly with one another. These networks are particularly useful in scenarios where conventional communication systems are unavailable, such as in disaster recovery, emergency response, military operations, temporary events, and social or collaborative applications. Each node in an Ad Hoc Network can function both as a host and a router, forwarding data packets for other nodes and thus extending network coverage in a flexible and decentralized manner.
The architecture of these networks supports various routing strategies to efficiently manage data transmission. Flat routing approaches treat all nodes equally, while hierarchical or clustering-based methods organize nodes into groups to reduce overhead and improve scalability. Proactive protocols maintain up-to-date routing information at all times, ensuring low-latency communication, whereas reactive protocols discover routes only when necessary, reducing unnecessary traffic but sometimes introducing initial delays. Hybrid protocols combine elements of both proactive and reactive strategies to balance efficiency, latency, and network overhead.
Security in Wireless Ad Hoc Networks is a major concern due to the open nature of wireless communication and the constant movement of nodes. Networks are susceptible to threats such as data interception, tampering, privacy breaches, and denial-of-service attacks. Effective security mechanisms, including encryption, authentication, trust management, and intrusion detection, are essential to ensure reliable communication and protect sensitive information.
Overall, Wireless Ad Hoc Networks provide a versatile and robust communication framework. Proper selection of routing protocols and implementation of security measures enhance network reliability, maintain connectivity despite frequent topology changes, and support the expanding applications of mobile networks across civilian, commercial, and military domains. With their flexibility, scalability, and resilience, these networks continue to play a crucial role in modern mobile communication systems.

Keywords: Wireless Ad Hoc Networks, Dynamic Routing, Hybrid Protocols, Security and Data Protection, Scalability, and Decentralized Communication.

Libyan Open University Journal of Applied Sciences (LOUJAS)
Volume 2 - Issue 1 - 2026 - Pages 427-436

الملخص:
شبكات Wireless Ad Hoc Networks هي شبكات ديناميكية ذات تنظيم ذاتي لا تعتمد على أي بنية تحتية ثابتة، مما يتيح للعقد المتنقلة الاتصال المباشر فيما بينها. تُستخدم هذه الشبكات بشكل خاص في السيناريوهات التي تكون فيها أنظمة الاتصال التقليدية غير متاحة، مثل حالات الطوارئ والكوارث، والاستجابة السريعة، والعمليات العسكرية، والفعاليات المؤقتة، وكذلك التطبيقات الاجتماعية والتعاونية. كل عقدة في شبكة Ad Hoc يمكن أن تعمل كـ host وأيضًا كـrouter ، حيث تقوم بتمرير حزم البيانات للعقد الأخرى وبالتالي توسيع تغطية الشبكة بطريقة مرنة ولامركزية.
يدعم هيكل هذه الشبكات استراتيجيات توجيه متنوعة لإدارة نقل البيانات بكفاءة. تعتمد طرق التوجيه flat routing على معاملة جميع العقد على قدم المساواة، بينما تقوم الأساليب الهرمية أو القائمة على التجمعات clustering بتنظيم العقد في مجموعات لتقليل الحمل وتحسين القابلية للتوسع. تقوم البروتوكولات proactive بالحفاظ على معلومات التوجيه محدثة باستمرار لضمان تأخير منخفض في الاتصال، بينما تكتشف البروتوكولات reactive الطرق عند الحاجة فقط، مما يقلل من حركة المرور غير الضرورية ولكنه قد يسبب بعض التأخير الأولي. تجمع البروتوكولات hybrid بين عناصر كلا النوعين لتحقيق توازن بين الكفاءة، التأخير، وحجم حركة الشبكة.
الأمن في شبكات Ad Hoc يمثل تحديًا كبيرًا نظرًا للطبيعة المفتوحة للاتصال اللاسلكي وحركة العقد المستمرة. الشبكات معرضة للتهديدات مثل اعتراض البيانات، التلاعب بها، انتهاك الخصوصية، وهجمات الحرمان من الخدمة (DoS). تعتبر آليات الأمان الفعالة، مثل التشفير، التوثيق، إدارة الثقة، ونظم كشف التسلل، أساسية لضمان اتصال موثوق وحماية المعلومات الحساسة.
بشكل عام، توفر شبكات Wireless Ad Hoc Networks إطارًا مرنًا وقويًا للاتصال. يؤدي اختيار بروتوكولات التوجيه المناسبة وتطبيق تدابير الأمان إلى تعزيز موثوقية الشبكة، والحفاظ على الاتصال رغم التغيرات المستمرة في الهيكل الشبكي، ودعم توسع التطبيقات في المجالات المدنية والتجارية والعسكرية. بفضل مرونتها وقابليتها للتوسع ومتانتها، تستمر هذه الشبكات في لعب دور حيوي في نظم الاتصال المتنقلة الحديثة.

الكلمات المفتاحية: شبكات الاستجابة التلقائية اللاسلكية، التوجيه الديناميكي، البروتوكولات الهجينة، الأمان وحماية البيانات، قابلية التوسع، والاتصال اللامركزي

Introduction

Wireless Ad Hoc Networks have become a crucial technology in many fields, including social applications, military operations, and environments without established infrastructure. These networks provide temporary, dynamic connections between devices, allowing nodes to communicate directly without relying on centralized access points or fixed infrastructure. The self-organizing nature of Ad Hoc Networks makes them highly flexible and adaptable to environmental changes. (Perkins & Royer, 2000)

In an Ad Hoc Network, communication between two nodes does not require a router or other central device. Instead, nodes can directly establish connections, forming multi-hop paths when necessary. This characteristic allows the network to maintain connectivity even in rapidly changing environments. Cellular networks, mobile networks in remote areas, and temporary disaster recovery networks are practical examples of Ad Hoc Network applications. (Perkins & Bhagwat, 2001)

The primary goal of an Ad Hoc Network is to enable seamless communication between endpoints, while addressing challenges such as node mobility, routing efficiency, bandwidth limitations, and power constraints. The dynamic structure requires the implementation of routing algorithms and security mechanisms to ensure reliable and secure data transmission.

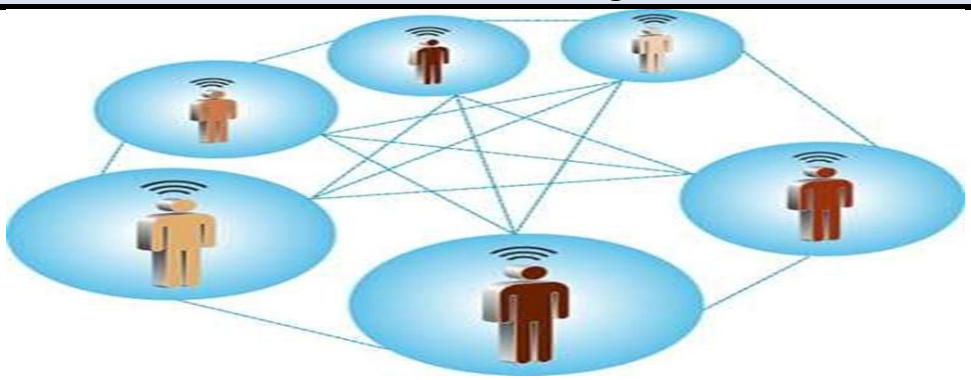

Figure 1: Structure of an Ad Hoc Network

This figure illustrates the basic structure of an Ad Hoc network, where multiple wireless nodes communicate directly with each other without relying on a fixed infrastructure. Each node acts as both a transmitter and a router, allowing data to be forwarded through intermediate nodes until it reaches the destination. (Marina & Das, 2006)

Ad Hoc Networks can vary in size and complexity. Small networks are relatively easy to manage, whereas larger networks require division into smaller subnetworks or clusters for efficient control and communication management. Temporary Ad Hoc Networks can evolve into more stable structures, resembling Local Area Networks (LANs) when the connection is long-term. (Wu & Tay, 2001)

Mobile devices commonly rely on wireless communication to maintain constant connectivity. In situations where traditional infrastructure is absent or insufficient, Ad Hoc Networks provide a flexible alternative, using radio or wireless links to facilitate communication. The self-configuring capabilities of these networks allow nodes to move freely while maintaining network functionality, making them suitable for dynamic environments. (Marti et al., 2000)

Key Features of Ad Hoc Networks:

- Lack of central administration for network management.
- High mobility of network nodes.
- Wireless-only communication, without cables.
- Significant power management considerations due to wireless operation.
- All nodes function in diverse roles and positions as needed.

Network Types

Networking technologies can generally be classified into wired networks and wireless networks. Wired networks use physical cables to connect devices and are known for their stability and high data transmission speeds. However, they limit device mobility and require physical infrastructure.

Wireless networks, on the other hand, allow devices to communicate without cables using radio frequency signals. These networks provide greater flexibility and mobility, making them suitable for modern communication environments. (Sanzgiri et al., 2002)

Wireless Networks

Wireless networks utilize radio frequencies, infrared, or microwaves to connect devices without cables. Common devices such as laptops, smartphones, and PDAs typically include wireless adapters to facilitate network connectivity. (Zhou & Haas, 2003)

Advantages of Wireless Networks:

- Mobility: Users can move freely within the coverage area.
- Cost: In some large-scale networks, wireless connections can reduce infrastructure costs.
- Flexibility: Easier to expand and connect devices without physical cables.
- Time Efficiency: Rapid deployment is possible compared to wired setups.

Disadvantages of Wireless Networks:

- Speed: Generally slower than wired connections (1–54 Mbps for Wi-Fi vs. Up to 100 Mbps for wired).
- Security: Wireless transmissions are more vulnerable to unauthorized access.
- Configuration Complexity: Setting up wireless networks can be more challenging.
- Interference: Physical obstacles and environmental conditions can affect performance.

Infrastructure Wireless Networks

Infrastructure wireless networks rely on access points to manage communication between devices. These networks are commonly used in homes, offices, universities, and public spaces.

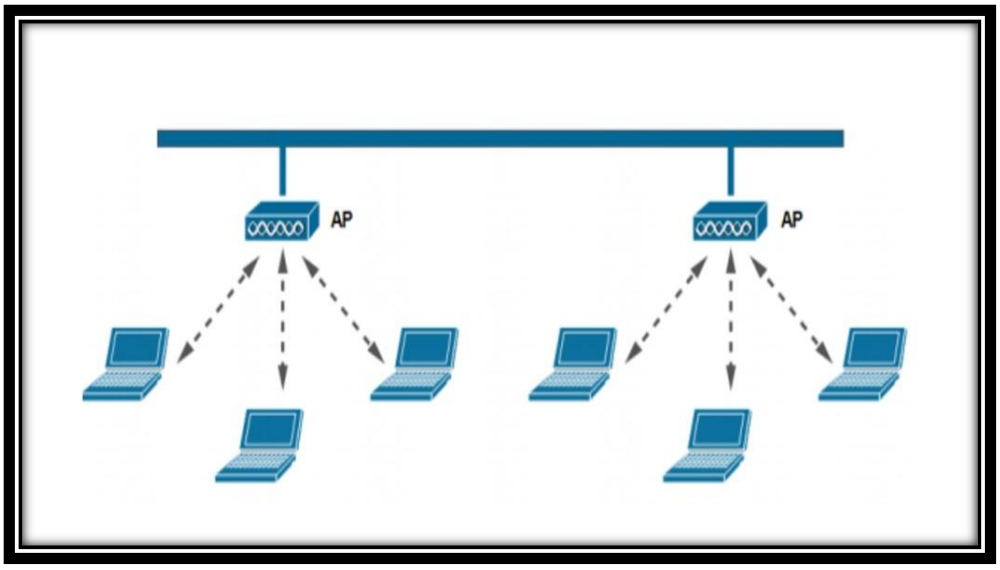

Figure 2: Infrastructure Wireless Network

Ad Hoc Networks

Ad Hoc Networks differ from infrastructure networks because they do not rely on centralized access points or fixed infrastructure. Instead, nodes communicate directly with one another and can dynamically organize themselves according to network conditions. (Ramasubramanian & Haas, 2003)

In such networks, nodes may function as both communication endpoints and routers, forwarding data to other nodes when necessary. Due to their wireless nature, efficient power management and bandwidth utilization are essential.

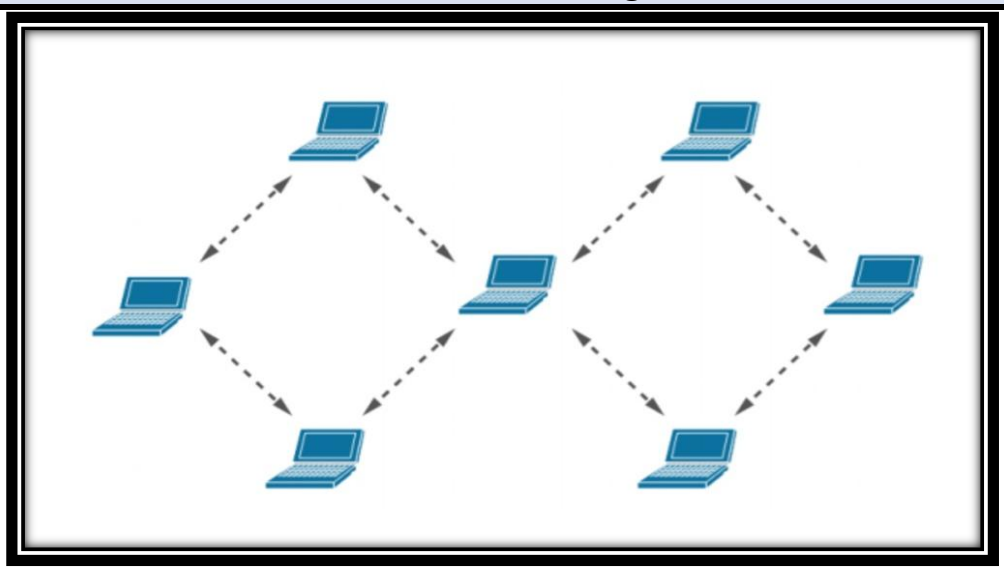

Figure 3: Ad Hoc Network

Ad Hoc Network Architecture

The architecture of Wireless Ad Hoc Networks follows a layered structure similar to traditional network models, but it is adapted to support node mobility and dynamic topology changes.
The main layers involved in Ad Hoc network communication include:
Physical Layer: Responsible for wireless signal transmission, transmission range, and energy consumption. (Sharma, et al, 2016)
MAC Layer: Manages access to the shared wireless communication channel and helps prevent transmission conflicts between nodes.
Network Layer: Handles routing decisions, maintains communication paths, and adapts to topology changes caused by node mobility.
In Ad Hoc Networks, nodes can perform multiple roles simultaneously. A node may function as a communication endpoint or act as a router that forwards packets to other nodes. This cooperative behavior enables multi-hop communication, allowing data to reach distant nodes through intermediate devices.
To improve efficiency in large networks, nodes may also be organized into clusters, which helps simplify routing and network management.

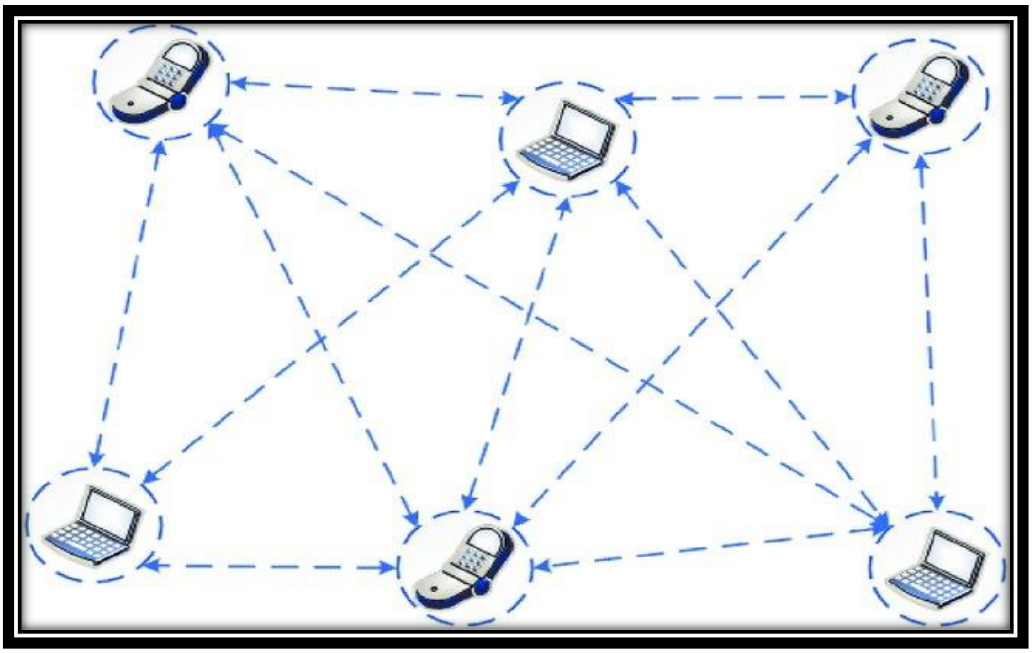

Figure 4: Wireless Sensor Network Architecture

Problems in Ad Hoc Networks

Ad Hoc Networks are dynamic systems in which nodes can join or leave the network at any time. Due to node mobility and the absence of centralized infrastructure, several technical challenges may affect network performance. These challenges appear mainly in the physical layer, MAC layer, and routing mechanisms. (Boukerche et al., 2007)

4.1 Physical Layer

The physical layer in Ad Hoc Networks is responsible for wireless signal transmission between nodes. One of the main challenges is signal attenuation, where signals weaken due to distance or obstacles in the environment.

Another important issue is energy consumption, since most nodes rely on battery power. Efficient power management is necessary to extend the lifetime of the network.

Additionally, node mobility may cause frequent link disconnections, which affects network stability. (Conti & Giordano, 2014).

MAC Layer

The Medium Access Control (MAC) layer manages how nodes share the wireless communication channel. Since bandwidth is limited, efficient channel access mechanisms are required to avoid data collisions. (Mauve et al., 2002)

Common multiple access techniques include FDMA, TDMA, CDMA, and CSMA. If multiple nodes attempt to transmit data simultaneously, collisions may occur, leading to packet loss and reduced network performance.

Routing Challenges

Routing in Ad Hoc Networks is difficult because nodes move frequently and network topology changes continuously. Data packets are often delivered through multi-hop communication, where intermediate nodes forward packets toward the destination. (Younis & Fahmy, 2004)

The main routing challenges include:

- Frequent route breakage due to node mobility
- Network congestion and packet delays
- Limited bandwidth and energy resources
- Efficient routing protocols are therefore essential to maintain reliable communication.

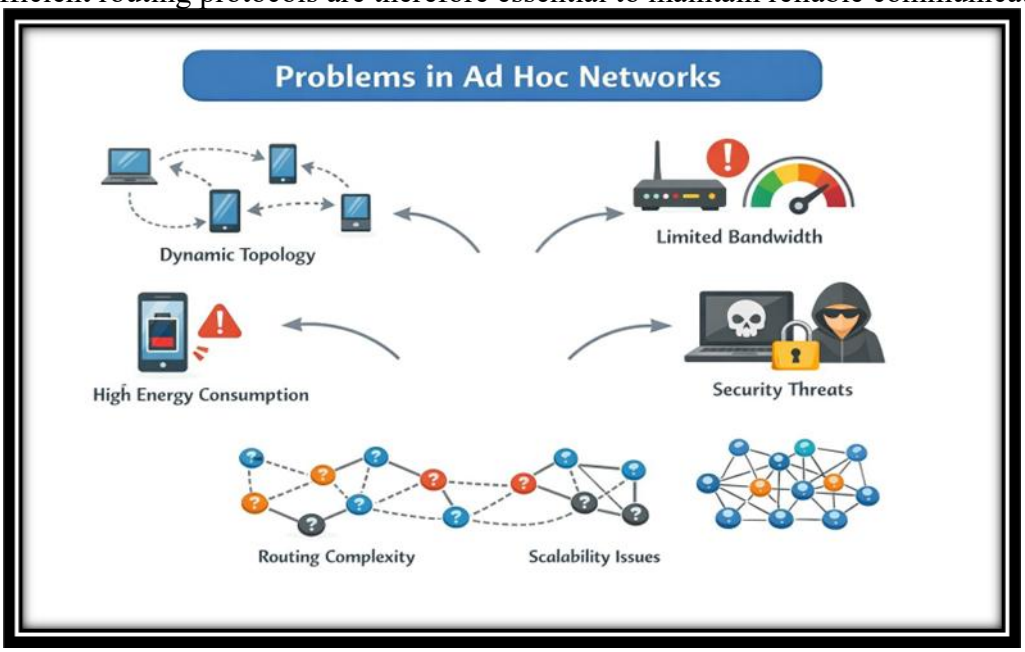

Figure 5: Major problems in Ad Hoc Networks

Routing, Mobility, and Security in Ad Hoc Network

Routing is a fundamental function in Ad Hoc Networks because nodes communicate through multi-hop paths without relying on fixed infrastructure. Due to node mobility and frequent topology changes, efficient routing strategies are required to maintain reliable communication. Routing protocols in Ad Hoc Networks can be classified into three main categories: flat routing, hierarchical routing, and hybrid routing. (Shi & Hou, 2008).

Flat Routing:

In this approach, all nodes have equal roles and participate in the routing process. It is suitable for small networks but may become inefficient as the network size increases.

Hierarchical Routing:

This method organizes nodes into clusters. Each cluster has a cluster head responsible for managing communication and forwarding data to other clusters. This reduces routing overhead in large networks.

Hybrid Routing:

Hybrid routing combines the advantages of proactive and reactive routing strategies. It maintains routing information for nearby nodes while discovering routes for distant nodes when needed.

Mobility and Security in Ad Hoc Networks

Node mobility is one of the main characteristics of Ad Hoc Networks. Since nodes can move freely, the network topology changes frequently, which may lead to route breakage and temporary communication disruptions. As a result, routing protocols must quickly adapt to these changes and establish new communication paths when necessary. (Corson & Macker, 2002)

Security is also a major concern in wireless Ad Hoc environments because communication occurs over open wireless channels. This makes the network vulnerable to several attacks such as eavesdropping, data tampering, flooding attacks, and black hole attacks.

To improve network security, several protection mechanisms can be implemented, including authentication, encryption, and intrusion detection systems (IDS). These mechanisms help ensure secure communication and protect the integrity and confidentiality of transmitted data.

Despite these challenges, effective routing strategies and proper security measures can significantly enhance the reliability and performance of Ad Hoc Networks.

Practical Simulation of Ad Hoc Network

To better understand the operation of Ad Hoc Networks, a practical simulation was conducted using the network simulation tool Cisco Packet Tracer. The purpose of this experiment is to demonstrate how wireless nodes can communicate directly without relying on centralized infrastructure, as well as to observe network behavior under different connectivity conditions.

Simulation Setup

In this simulation, several wireless nodes were created to represent mobile devices within an Ad Hoc network environment. Each node was equipped with a wireless network interface card to allow direct communication with neighboring nodes.

Unlike traditional infrastructure wireless networks, this setup does not use an access point or central router. Instead, nodes communicate directly with each other and may forward packets through intermediate nodes when the destination is outside the direct communication range. (Johnson, Maltz, & Hu, 2001).

The simulated network includes:

- Multiple wireless nodes representing mobile devices
- Direct wireless communication between nodes
- Multi-hop communication when nodes are outside direct transmission range

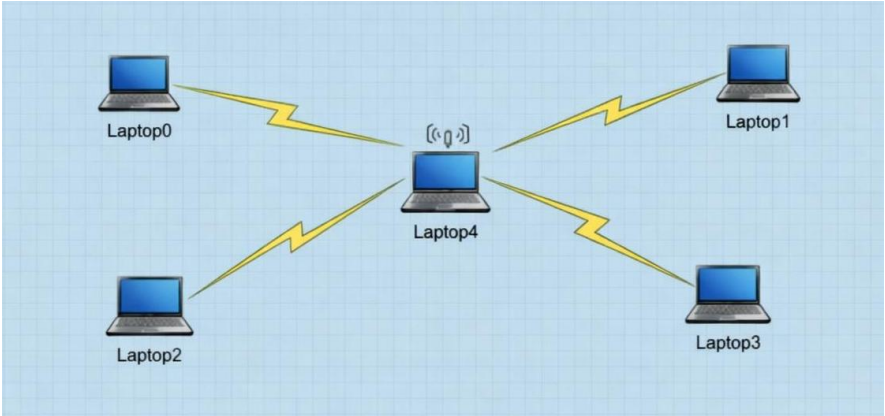

Figure 6: Basic structure of an Ad Hoc Network showing wireless communication between nodes

This figure illustrates a group of wireless nodes communicating directly without centralized infrastructure. Each node can exchange data with nearby nodes and forward packets when necessary.

Packet Transmission

To test network connectivity, a data packet was transmitted from one node to another using the simulation mode in Packet Tracer. When the destination node was not directly reachable, the packet was forwarded through intermediate nodes until it reached the final destination.

This process demonstrates the concept of multi-hop communication, which is one of the fundamental characteristics of Ad Hoc networks. It also highlights how intermediate nodes play a crucial role in maintaining connectivity when direct communication is not possible.

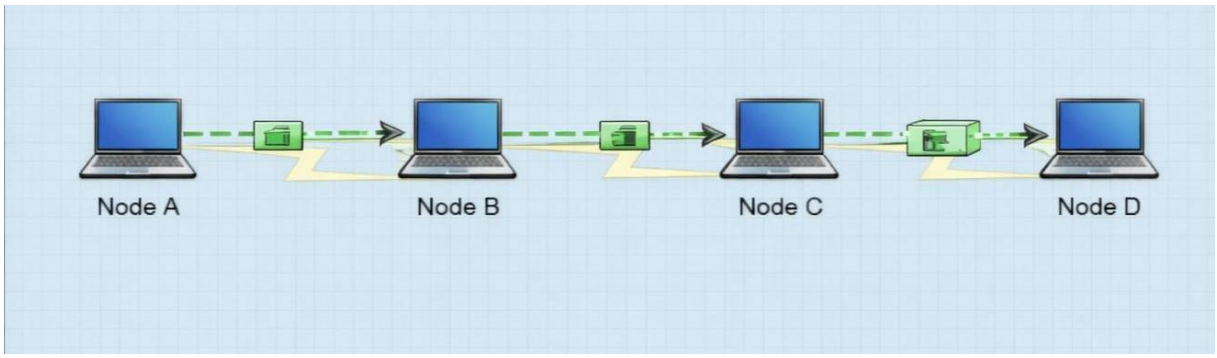

Figure 7: Multi-hop packet transmission in an Ad Hoc Network simulated using Cisco Packet Tracer.

The figure shows how packets travel between nodes through intermediate devices before reaching the destination.

Results and Observations

The simulation demonstrates several important characteristics of Ad Hoc networks:

- Nodes can communicate without centralized infrastructure.
- Each node can act as both a host and a router.

- Multi-hop communication enables connectivity between distant nodes.
- The network can adapt dynamically to communication paths.

In addition, it was observed that network performance depends on node placement and communication range. When nodes are positioned closer together, communication becomes more stable, while increased distance may require more intermediate nodes and can introduce delay.

These results confirm the theoretical concepts discussed earlier and demonstrate how Ad Hoc networks provide flexible and reliable communication in dynamic environments.

Conclusions

Mobile networks exemplify Ad Hoc Networks, using dynamic, infrastructure-less communication and radio frequencies to connect nodes. Their flexible, self-configuring nature maintains connectivity even in changing environments, making them suitable for social networks, disaster recovery, and military use. Routing is complex due to node mobility and dynamic topology, so protocol choice-flat, hierarchical, proactive, reactive, or hybrid-is crucial for efficiency and reliability.

The practical simulation conducted using Cisco Packet Tracer demonstrated the key concepts of Ad Hoc networks, including direct node-to-node communication, multi-hop packet transmission, and dynamic path adaptation. This experiment confirmed that each node can act as both a host and a router, and that connectivity can be maintained even in the absence of centralized infrastructure.

Security remains essential; authentication, encryption, and intrusion detection protect against eavesdropping, data tampering, flooding, blackhole, and wormhole attacks. With proper planning, protocol selection, and awareness of practical constraints, Ad Hoc Networks remain reliable and adaptable. They are expected to grow in civilian, commercial, and military applications, offering flexible and secure wireless communication solutions.

References

1. Broch, J., Maltz, D. A., Johnson, D. B., Hu, Y.-C., & Jetcheva, J. (2002). A performance comparison of multi-hop wireless ad hoc network routing protocols. Proceedings of the 4th Annual International Conference on Mobile Computing and Networking (MobiCom), 85–97.
2. Boukerche, A., Turgut, B., Aydin, N., et al. (2007). Routing protocols in ad hoc networks: A survey. Computer Networks, 55(13), 3032–3080.
3. Conti, M., & Giordano, S. (2014). Mobile ad hoc networking: Milestones, challenges, and new research directions. IEEE Communications Magazine, 52(1), 85–96.
4. Johnson, D. B., Maltz, D. A., & Hu, Y.-C. (2001). The dynamic source routing protocol (DSR) for mobile ad hoc networks. IETF RFC 4728.
5. Marina, M. K., & Das, S. R. (2006). On-demand multipath distance vector routing in ad hoc networks. IEEE International Conference on Network Protocols (ICNP), 14–23.
6. Marti, S., Giuli, T. J., Lai, K., & Baker, M. (2000). Mitigating routing misbehavior in mobile ad hoc networks. Proceedings of the 6th Annual International Conference on Mobile Computing and Networking (MobiCom), 255–265.
7. Mauve, M., Füssler, H., Widmer, J., & Hartenstein, H. (2002). A survey on position-based routing in mobile ad hoc networks. IEEE Network, 15(6), 30–39.
8. Papadimitratos, P., & Haas, Z. J. (2002). Secure routing for mobile ad hoc networks. Proceedings of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference, 27–31.

9. Perkins, C. E., & Bhagwat, P. (2001). Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers. ACM SIGCOMM Computer Communication Review, 24(4), 234–244.
10. Perkins, C. E., & Royer, E. M. (2000). Ad-Hoc On-Demand Distance Vector Routing. Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications (WMCSA), 90–100.
11. Ramasubramanian, V., & Haas, Z. J. (2003). Secure routing for ad hoc networks. Technical Report, School of Electrical and Computer Engineering, Cornell University.
12. Sanzgiri, K., Dahill, B., Levine, B. N., Shields, C., & Belding-Royer, E. M. (2002). Authenticated routing for ad hoc networks. IEEE INFOCOM 2002, 3, 1344–1354.
13. Shi, Y., & Hou, Y. T. (2008). A distributed optimization algorithm for QoS routing in ad hoc networks. IEEE/ACM Transactions on Networking, 16(1), 27–40.
14. Younis, O., & Fahmy, S. (2004). HEED: A hybrid, energy-efficient, distributed clustering approach for ad hoc networks. IEEE Transactions on Mobile Computing, 3(4), 366–379.
15. Zhang, Y., Sengupta, R., & Lee, W. (2002). Intrusion detection techniques for mobile wireless networks. Wireless Networks, 9(5), 545–556.
16. Zhou, L., & Haas, Z. J. (2003). Securing ad hoc networks. IEEE Networks, 13(6), 24–30.
17. Abraham, R., et al. (2002). Secure routing for mobile ad hoc networks. International Conference on Information Systems Security (ICISS), 31–43.
18. Wu, J., & Tay, Y. (2001). AMRoute: Ad hoc multicast routing protocol. IEEE Network, 13(1), 20–25.
19. Corson, S., & Macker, J. (2002). Mobile ad hoc networking (MANET): Routing protocol performance issues and evaluation considerations. IETF RFC 2501.
20. Sharma, N., Sharma, S., & Kumar, D. (2016). A survey on security issues in mobile ad hoc networks. Journal of Network and Computer Applications, 82, 159–187.