

Chapter: 10
Mobile Ad Hoc Network
Arvind Kumar Shukla
School of Computer Science and Applications,
IFTM University, Moradabad, UP, India
Email: arvindshukla.india@gmail.com

The Internet Engineering Task Force (IETF), the body responsible for guiding the evolution of the Internet, provides the definition as given below. A mobile ad hoc network (MANET) is an autonomous system of mobile routers (and associated hosts) connected by wireless links. The routers are free to move randomly and organize themselves arbitrarily; thus, the network's wireless topology may change rapidly and unpredictably. Such a network may operate in a stand-alone fashion, or may be connected. Or in simple terms we can say that A MANET is an Independent Basic Service Set (IBSS). Ad hoc is a Latin term and literally means "for this purpose only." In other words, it is an autonomous collection of mobile nodes, with networks built on the fly for a specific purpose (i.e., emergency situations, rescue operations, battlefield situations, etc.), that talk to each other over bandwidth constrained wireless links.

1.1. Introduction

The proliferation of wireless portable devices as part of everyday life, such as PDA, mobile phones, and laptops is leading to the possibility for ad hoc wireless communication. With these types of devices there is a fundamental ability to share information. Ad hoc networks are dynamically created and maintained by the individual nodes comprising the network. However, communication over existing infrastructures may be precluded due to deficient facilities, or impractical in terms of time, expense and power. Ad hoc networks do not require a pre-existing architecture for communication purposes and do not rely on any type of wired infrastructure; in an ad hoc network all communication occurs through a wireless median. With current technology and the increasing popularity of notebook computers, interest in ad hoc networks has greatly peaked. Future advances in technology will allow us to form small ad hoc networks on campuses, during conferences, and even in our own homes [1-2].

Ad hoc networks comprise a special subset of wireless networks since they do not require the existence of a centralized message-passing device. Simple wireless networks require the existence of static base stations (BS), which are responsible for routing messages to and from mobile nodes (MNs) within the specified transmission area. Ad hoc networks, on the other hand, do not require the existence of any device other than two or more MNs willing to cooperatively form a network.

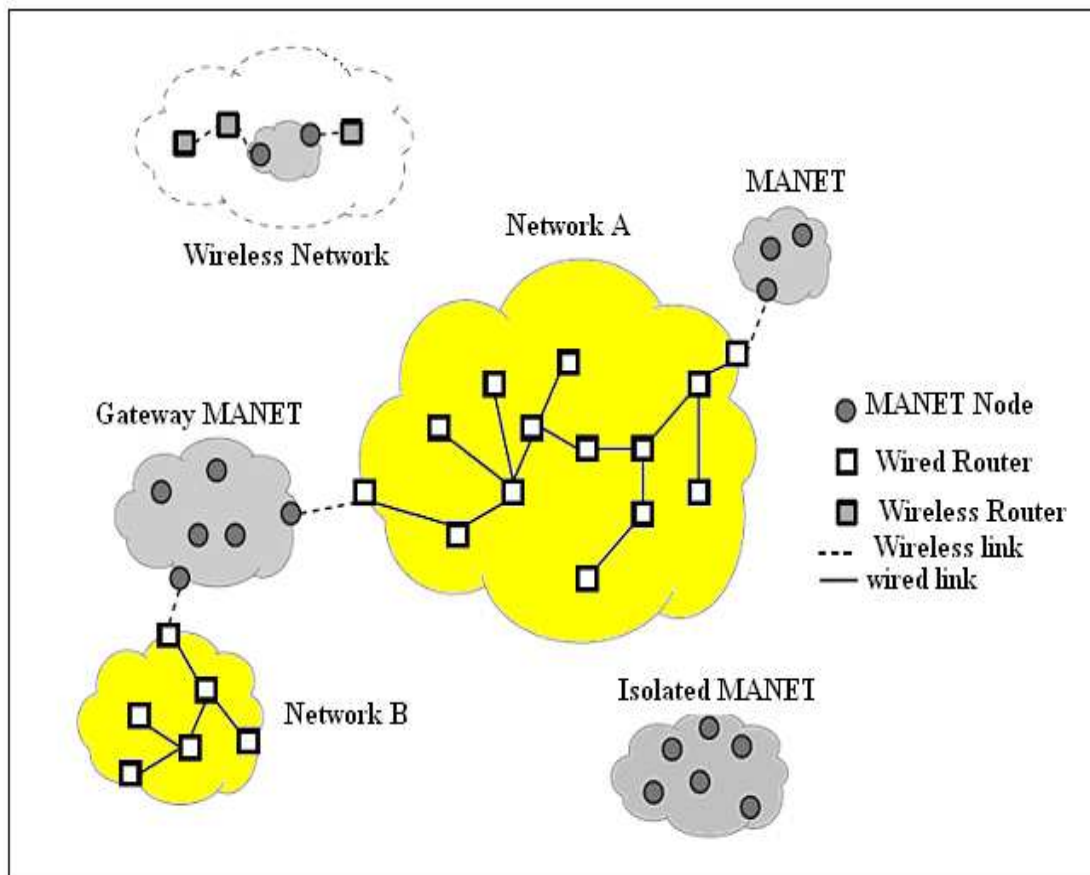


Figure 1.1: MANET

1.2. Mobile Ad-Hoc Networks

Ad hoc networks do not require a pre-existing architecture for communication purposes and do not rely on any type of wired infrastructure. Networks suited to this type of random communication are known as Mobile Ad-hoc Networks (MANETs), where a MANET is a self-organizing collection of wireless mobile nodes that form a temporary network without the aid of a fixed networking infrastructure or centralized administration, as shown in the following figure [3-4].

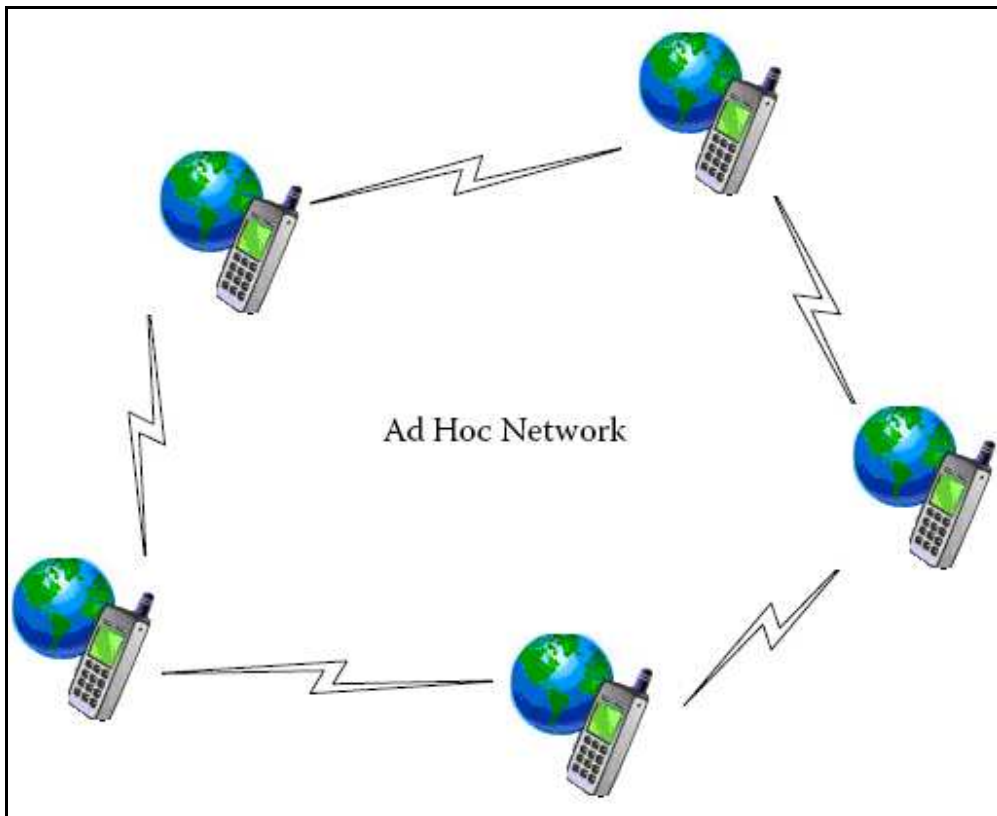


Figure 1.2: Ad Hoc Network

Node mobility causes frequent and unpredictable changes in this arbitrary network topology and as such, MANET routes have to cope with frequent changes and may consist of many hops through other network hosts. As a consequence of this dynamic topology the design of efficient routing protocols is an exigent challenge and crucial problem.

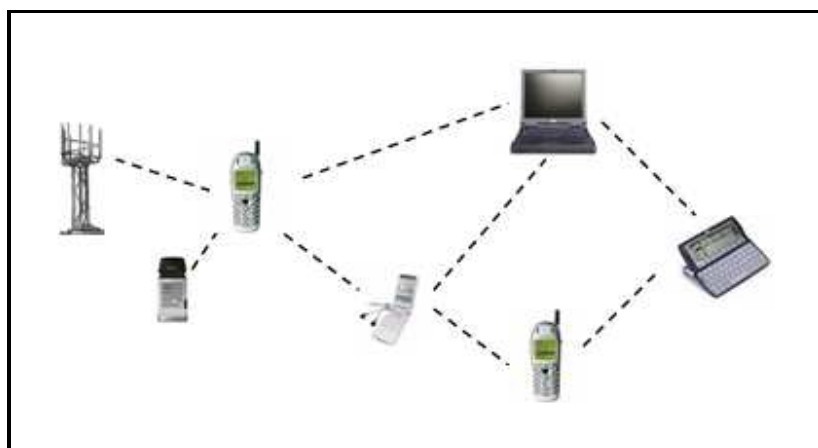


Figure 1.3: Ad Hoc Network Architecture

In ad hoc networks messages sent by a node may be received simultaneously by all nodes within its transmission range, i.e. by its neighbors. Messages requiring a destination outside this local neighborhood zone must be hopped or forwarded by these neighbors, which act as routers, to the appropriate target address. As a consequence of node mobility fixed source or destination paths cannot be maintained for the lifetime of the network. As a result of this, a number of routing protocols have been proposed and developed for wireless ad hoc networks. These protocols have been derived from distance vector and link state techniques and involve determining the shortest path to a destination in terms of distance or link cost. Such protocols are classified as proactive, reactive or hybrid, depending on how route maintenance and discovery is performed.

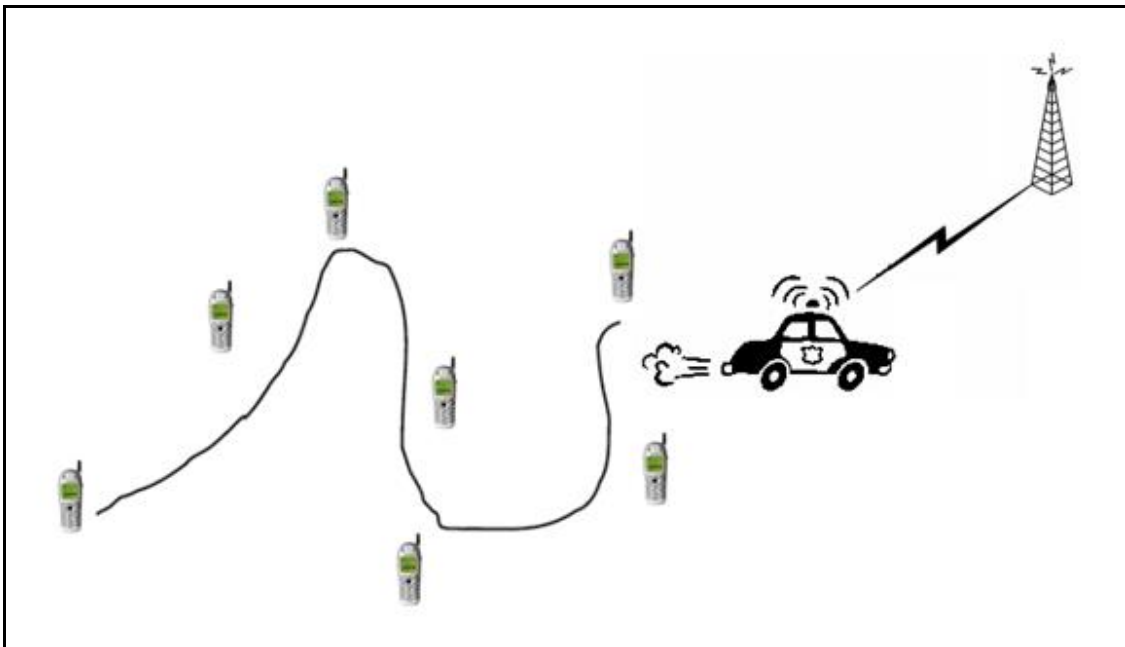


Figure 1.4: Control of Node movement

Wireless ad hoc networks are very attractive since they provide ubiquitous connectivity without the need for fixed infrastructure or centralized control. Mobile Ad hoc Networks (MANETs) is class of wireless ad hoc networks in which mobile nodes exhibit features of free node mobility in addition to ephemeral node association. Node mobility, in particular, can cause frequent and unpredictable topology changes, while ephemeral node associations may limit the link lifetime, hence affecting the route lifetime. Despite these challenges, MANETs are envisioned to have many applications in both civil and military aspects. As such, innovative solutions for the above challenges are highly needed [4-6].

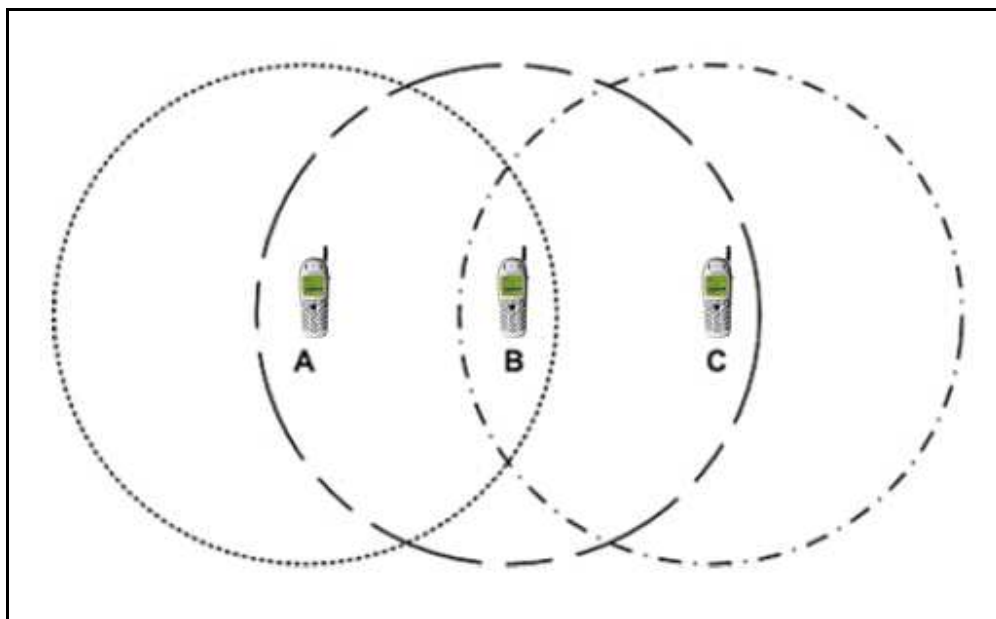


Figure 1.5: MANET with three nodes

1.2.2. Overview of Wireless Network

Wireless networks have become increasingly popular in the computing industry since 1970. It is particularly true within the past decade, which has seen wireless networks being adapted to enable mobility. The area of wireless communication has been and is continuing to develop at a rapid pace over the years. The most wireless network of today consists of cells. Each cell contains (or is represented by) a base station, which is wired to a fixed wire network. The base stations interact with the portable handheld devices and provide these devices the wireless link to the network.

Nodes in mobile ad-hoc network are free to move and organize themselves in an arbitrary fashion. Each user is free to roam about while communication with others. The path between each pair of the users may have multiple links and the radio between them can be heterogeneous. This allows an association of various links to be a part of the same network. Mobile Ad-hoc networks have recently attracted a lot of attention in the research community as well as in industry. The mobility model is one of the most important factors in the performance evaluation of a mobile ad hoc network. Ad hoc networks are dynamically created and maintained by the individual nodes comprising the network. They do not require a pre-existing architecture for communication purposes and do not rely on any type of wired infrastructure; in an ad hoc network all communication occurs through a wireless median. Traditionally, the random

waypoint mobility model has been used to model the node mobility, where the movement of one node is modeled as independent from all others [1-4].

1.2.3. Overview of Mobile Ad Hoc Network

Mobile ad hoc networks originated from the U.S. Government's Defense Advanced Research Projects Agency (DARPA) Packet Radio Network (PRNet) and SURAN project. Being independent on pre-established infrastructure, mobile ad hoc networks have advantages such as rapidity and ease of deployment, improved flexibility, and reduced costs. Mobile ad hoc networks are appropriate for mobile applications in either hostile environments where no infrastructure is available, or temporarily established mobile applications, which are cost crucial. In recent years, application domains of mobile ad hoc networks have gained more and more importance in non-military public organizations and in commercial and industrial areas. The typical application scenarios include rescue missions, law enforcement operations, cooperating industrial robots, traffic management, and educational operations in campus [4-6].

A mobility pattern aware routing algorithm is shown to have several distinct advantages such as

- A. A more precise view of the entire network topology as the nodes move
- B. A more precise view of the location of the individual nodes
- C. Ability to predict with reasonably accuracy the future locations of nodes
- D. Ability to switch over to an alternate route before a link is disrupted due to node movements.

The absence of fixed infrastructure for ad hoc networks means that the nodes communicate directly with one another in a peer-to-peer fashion. The mobility of these nodes imposes limitations on their power capacity, as well as their transmission range. Mobile hosts are no longer just end systems; each node must be able to function as a router, and also must relay packets generated by other nodes. As the nodes move in and out of range with respect to one another, including those that operate as routers, the resulting topology changes must somehow be communicated to all other nodes so the up to-date topology information for routing purposes is maintained. In addition, the communication needs of the user applications, the limited bandwidth of wireless channels and the generally hostile transmission characteristics all impose additional constraints on the type, size and frequency of information to be exchanged. Thus ensuring effective routing is one of the greatest challenges for ad hoc networking.

1.3. SALIENT CHARACTERISTIC OF MANET

1.3.1. Multi-hop routing

If there is no direct link between the source and destination then path is dynamically discovered using some routing protocols. This path will include one or more hops to reach the destination so data are transferred using these multiple hops.

1.3.2. Mobile nodes

Nodes are free to move arbitrarily; thus, the network topology which is typically multihop--may change randomly and rapidly at unpredictable times. Adjustment of transmission and reception parameters such as power may also impact the topology.

1.3.3. No fixed infrastructure

It does not require any centralized router all host can work as a router. So it does not require any backbone. That is why it is known as infrastructure free network.

1.3.4. Power-constrained operation

Nodes in a MANET may rely on batteries for their energy, For these nodes, the most important system design criteria for optimization may be that of power conservation.

1.3.5. Interhop Routing

It can be easily understood with the help of a scenario that is shown in the following figure 1.6 'S' wants to communicate with nodes 'D'. They are communicating using '1' intermediate nodes

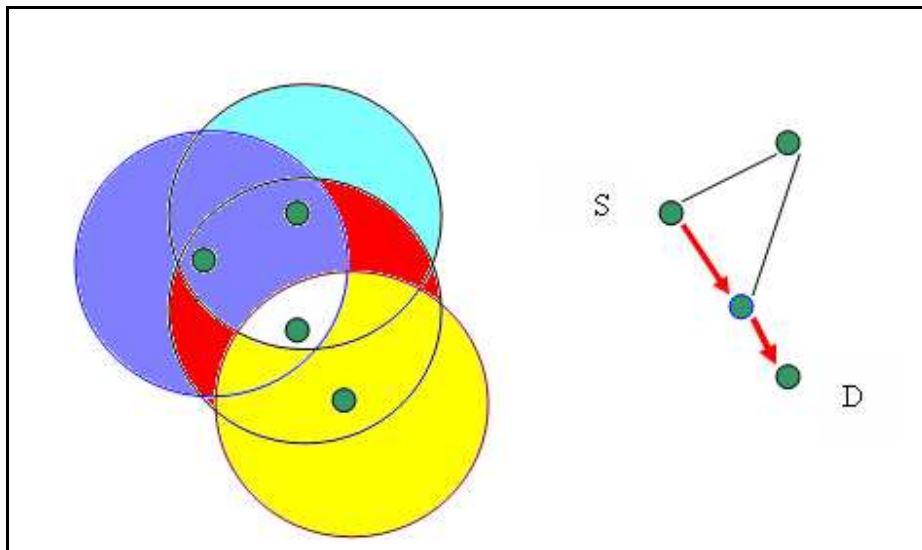


Figure 1.6: Routing between 'S' to 'D' at time t_1

As nodes are mobile so it may be the case that the path earlier may not exist and any other path has to be discovered. It is shown in the following figure.

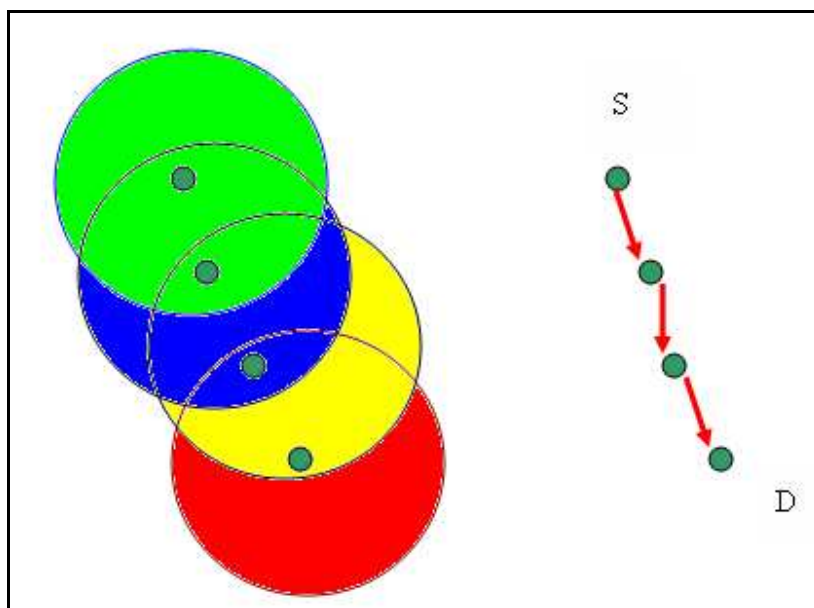


Figure 1.7: Showing the new path at time t_2

Hence it can be seen that in figure 1.6 only one intermediate hops, but in the next figure 1.7 two inter hops are required to transfer the data. The new path must be dynamically discovered. This is what the complexity of MANET [7-8].

1.4. Components of a Mobile Ad Hoc Network in the Real-World

We need to define our abstract representation of such class of networks, making explicit all the components that can be considered in the simulation model. Our representation includes the following main components.

A set of mobile devices, called nodes, with processing and wireless transmission capabilities powered by on-board batteries the number of nodes participating to the network is in general not constant; at any time nodes can leave or join the network. In addition to the transmission capabilities, nodes can be also equipped with devices for geographic localization (e.g., GPS) or other optional devices of different nature.

Since nodes are communication devices, their internal architecture is defined in terms of the OSI protocol stack. This means that node communications are regulated by the characteristics associated to the OSI protocol layers: physical, data link, medium access control (MAC), network, transport, session, presentation, application.

Communications happen through a wireless interface. Therefore, the physical and technological aspects of radio emission, propagation and reception have to be explicitly taken into account. While emission and reception are strictly related to the physical characteristics of the node radio device, radio propagation is affected by the physics of the environment in which the network is placed.

The network is seen as embedded in an environment with well-defined physical characteristics which affect both the propagation of the radio signals and the mobility patterns of the nodes.

Every node is associated to a single user which moves inside the environment. Therefore, node mobility patterns depend on the characteristics of both the users and the environment.

Node energy power relies on the use of on-board batteries. Every action involving the use of the radio channel, as well as the same fact that the device is switched on, has an energetic cost which affects the available energy power.

Users generate data traffic in terms of open sessions between pairs or groups of users.

1.5. Overview of Routing Techniques

Two different architectures exist for an ad hoc network: flat and hierarchical. Flat networks are the simplest because all MNs are “equal”. Flat networks require each MN to participate in the forwarding and receiving of packets depending on the implemented routing scheme. Hierarchical networks use a tiered approach and consist of two or more tiers. The bottom layer consists of MNs grouped into smaller networks. A single member from each of these groups acts as a gateway to the next higher level. Together, the gateway MNs create the next higher tier. When an MN belonging to group A wants to interact with another MN located in the same group, routing is the same as in a flat ad hoc network. However, if an MN in group A wants to communicate with another MN in group B, more advanced routing techniques incorporating the higher tiers must be implemented [5-6].

A routing protocol must determine the most efficient path between source and destination nodes so that packets may be sent throughout a network. A routing protocol must address the following issues:

1. **Scalability:** ability to support a large number of nodes & networks
2. **Ability to adapt to a varying topology & traffic levels** in terms of speed and efficiency
3. **Route discovery**
4. **Route maintenance**

Routing protocols can be classified in three categories:

1. **Centralised or Distributed**
2. **Adaptive or Static**
3. **Reactive or Proactive or Hybrid**

A centralised protocol involves all decisions being made at a centre node whereas a distributed one includes all nodes in the routing decision. With an adaptive protocol route information can be modified as a consequence of network status, such as traffic levels or topology changes, whereas static based protocols update route information at periodic intervals. Reactive protocols perform route discovery when needed (on demand protocols) and proactive protocols undertake route discovery before it is needed using routing tables that are updated periodically (table driven protocols). A hybrid protocol, such as Zone Routing protocol, combines the features of both reactive and proactive schemes to make a more efficient protocol. Standard routing protocols (those used in fixed networks) are based on either Distance Vector (DV) or Link State (LS) algorithms.

DV based routing protocols, such as ARPANET and RIP, are classed as being decentralised and static and are based on the Distributed Bellman-Ford (DBF) algorithm. LS routing protocols, such as OSPF, are based on Dijkstra's shortest path algorithm. These protocols involve each node sustaining a complete map of the network topology and the cost to reach each destination node.

Conventional routing protocols, based on DV and LS techniques, were designed for static infrastructure based network topologies and node mobility was not considered. For mobile networks, unlike rigid networks, periodic transmission of topology information is required for efficient routing and this wastes battery power. As nodes must both send and receive this information it makes conservation of energy difficult. Also, periodic transmission wastes network bandwidth as routing information will often not change from one update to the next. In a static infrastructure based network node links are considered bi-directional and of equal quality but this may not be the case for ad-hoc networks, thus routes determined by standard protocols may be only unidirectional. Some of these problems have been approached and solved but conventional protocols as such still remain unsuitable for ad-hoc networks but have been used as a basis for designing MANET routing protocols.

1.6. Problems Associated With Ad-Hoc Routing

The main problem with ad-hoc networking is how to send a message from one node to another with no direct link. The nodes in the network are moving around unpredictably, and it is very challenging which nodes that are directly linked together. The topology of an ad-hoc network is constantly changing and it is very difficult for routing process. There are two main approaches for routing process in ad hoc networks.

The first approach is a pro-active approach which is table driven and uses periodic protocols. This means that all nodes have tables with routing information which are updated at intervals. The second approach is re-active, source-initiated or on-demand. This means that every time a message is sent it first has to find a path by searching the entire network. There are many different protocols that are in accordance with the two different routing approaches. Different protocols are specialized in different aspects of the routing such as finding a short path, low overhead communication and load-balancing [3-4].

1.7. Infrastructure

An Ad-hoc network is an infrastructure less network. Unlike traditional networks there is no pre-deployed infrastructure such as centrally administered routers or strict policy for supporting end-to-end routing. The nodes themselves are responsible for routing packets. Each node relies on the other nodes to route packets for them. Mobile nodes in direct radio range of one another can communicate directly, but nodes that are too far apart to communicate directly must depend on the intermediate nodes to route messages for them [8-9].

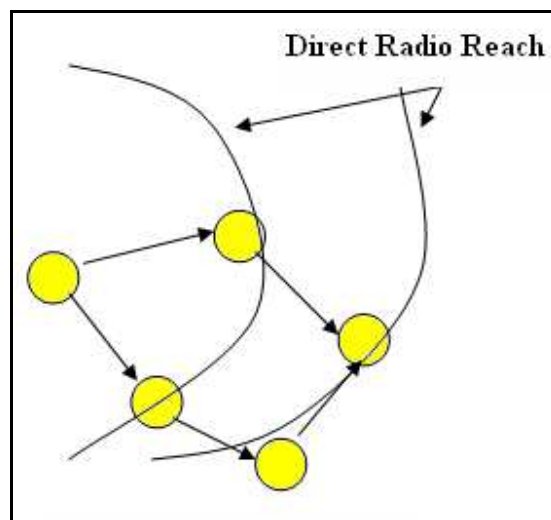


Figure 1.8: Routing in Ad-hoc networks

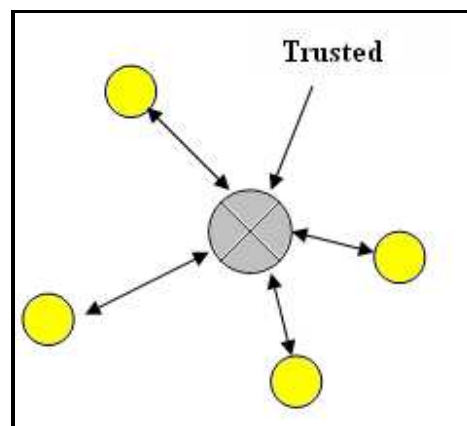


Figure 1.9: Routing in traditional networks using router

1.8. Frequent Changes in Network Topology

Ad-hoc networks contain nodes that may frequently change their locations. Hence the topology in these networks is highly dynamic. This results in frequently changing neighbours on whom a

node relies for routing. As a result traditional routing protocols can no longer be used in such an environment. This mandates new routing protocols that can handle the dynamic topology by facilitating fresh route discoveries.

1.9. Problems Associated with Wireless Communication

As the communication is through wireless medium, it is possible for any intruder to tap the communication easily. Wireless channels offer poor protection and routing related control messages can be tampered. The wireless medium is susceptible to signal interference, jamming, eavesdropping and distortion. An intruder can easily eavesdrop to know sensitive routing information or jam the signals to prevent propagation of routing information or worse interrupt messages and distort them to manipulate routes. Routing protocols should be well adopted to handle such problems [9].

1.10. Problems with Existing Ad-Hoc Routing Protocols

1.10.1. Implicit trust relationship between neighbours

Current Ad-hoc routing protocols inherently trust all participants. Most Ad-hoc routing protocols are cooperative by nature and depend on neighbouring nodes to route packets. This naive trust model allows malicious nodes to paralyze an Ad-hoc network by inserting erroneous routing updates, replaying old messages, changing routing updates or advertising incorrect routing information. While these attacks are possible in fixed network as well, the Ad-hoc environment magnifies this makes detection difficult.

1.10.2. Throughput

Ad-hoc networks maximize total network throughput by using all available nodes for routing and forwarding. However a node may misbehave by agreeing to forward packets and then failing to do so, because it is overloaded, selfish, malicious or broken. Misbehaving nodes can be a significant problem. Although the average loss in throughput due to misbehaving nodes is not too high, in the worst case it is very high.

1.10.3. Attacks using modification of protocol fields of messages

Current routing protocols assume that nodes do not alter the protocol fields of messages passed among nodes. Routing protocol packets carry important control information that governs the behavior of data transmission in Ad-hoc networks. Since the level of trust in a traditional Ad-hoc network cannot be measured or enforced, enemy nodes or compromised nodes may participate directly in the route discovery and may intercept and filter routing protocol packets to disrupt communication. Malicious nodes can easily cause redirection of network traffic and DOS attacks by simply altering these fields. The attacks can be classified as remote redirection attacks and denial of service attacks. Let us look at them now.

i) Remote redirection with modified route sequence number (AODV)

Remote redirection attacks are also called black hole attacks. In the attacks, a malicious node uses routing protocol to advertise itself as the shortest path to nodes whose packets it wants to intercept. Protocols such as AODV instantiate and maintain routes by assigning monotonically increasing sequence numbers to routes towards a specific destination. In AODV, any node may divert traffic through itself by advertising a route to a node with a destination sequence number greater than the authentic value [10].

ii) Redirection with modified hop count (AODV)

A redirection attack is also possible in certain protocols, such as AODV, by modification of the hop count field in route discovery messages. When routing decisions cannot be made by other metrics, AODV uses the hop count field to determine a shortest path. In AODV, malicious nodes can attract route towards themselves by resetting the hop count field of the RREP to zero. Similarly, by setting the hop count field of the RREP to infinity, routes will tend to be created that do not include the malicious node [8-10].

Once the malicious node has been able to insert itself between two communicating nodes it is able to do anything with the packets passing between them. It can choose to drop packets to perform a denial of service attack, or alternatively use its place on the route as a first step in man-in-the-middle attack.

iii) Denial of service with modified source routes

DSR is a routing protocol, which explicitly states routes in data packets. These routes lack any integrity checks and a simple denial-of-service attack can be launched in DSR by altering the source routes in packet headers. Modification to source routes in DSR may also include the introduction of loops in the specified path. Although DSR prevents looping during the route discovery process, there are insufficient safeguards to prevent the insertion of loops into a source route after a route has been salvaged.

1.10.4. Attacks Using Impersonation

Current Ad-hoc routing protocols do not authenticate source IP address. A malicious node can launch many attacks by altering its MAC or IP address. Both AODV and DSR are susceptible to this attack.

1.10.5. Attacks using fabrication

Generation of false routing messages is termed as fabrication messages. Such attacks are difficult to detect.

Summary

Ad hoc networks do not require a pre-existing architecture for communication purposes and do not rely on any type of wired infrastructure. Two different architectures exist for an ad hoc network: flat and hierarchical. Flat networks are the simplest because all MNs are “equal”. Flat networks require each MN to participate in the forwarding and receiving of packets depending on the implemented routing scheme. Hierarchical networks use a tiered approach and consist of two or more tiers. Current routing protocols assume that nodes do not alter the protocol fields of messages passed among nodes. Routing protocol packets carry important control information that governs the behavior of data transmission in Ad-hoc networks. Since the level of trust in a traditional Ad-hoc network cannot be measured or enforced, enemy nodes or compromised nodes may participate directly in the route discovery and may intercept and filter routing protocol packets to disrupt communication.

References:

1. S. Chakrabarti, Satyabrata, and A. Mishra Virginia. "Quality of Service in Mobile Ad Hoc Networks", *The Handbook of Ad hoc Wireless Networks*, (M. Ilyas, Editor), CRC Press, (2002).
2. "Research Challenges for Ad hoc mobile wireless networks, University of Essex, 2005".
3. "An Overview of Mobile Ad Hoc Networks: Applications and Challenges" (PDF).
4. Murthy, C. Siva Ram; Manoj, B. S. (May 2004). *Ad hoc Wireless Networks: Architectures and Protocols*. Prentice Hall PTR. ISBN 9780133007060.
5. Toh, C. K. (1997). *Wireless ATM & Ad Hoc Networks*, 1997, Kluwer Academic Press. ISBN 9780792398226.
6. A. K Shukla & C K Jha(2014) Simulation based assessment of realistic mobility pattern in ad hoc networks *International. J. Computer. Applications*.
7. A. K. Shukla, C. K. Jha, N. Saxena and S. K. Biswash, "The analysis of AODV, based on mobility model," 2013 3rd IEEE International Advance Computing Conference (IACC), 2013, pp. 440-443, doi: 10.1109/IAdCC.2013.6514266.
8. Arvind Kumar Shukla, C K Jha and Shashi Kant Sharma. Article: The Analysis of Mobility Models based on Routing Protocols. *IJCA Proceedings on National Conference on Recent Trends in Engineering and Management NCRTEM:19-23*, August 2013.
9. Arvind Kumar Shukla, C K Jha and Deepak Sharma. Article: An Estimation of Routing Protocols in Mobility Models used for Ad Hoc Networks: Simulation Study. *IJCA Proceedings on International Conference on Advances in Computer Application 2013 ICACA 2013:21-27*, February 2013.
10. Arvind Kumar Shukla, Ck Jha and Deepak Sharma. Article: The Efficiency Analysis of Mobility Model using Routing Protocols. *IJCA Proceedings on International Conference on Advances in Computer Applications 2012 ICACA (1):6-10*, September 2012.

ABOUT THE EDITORS



Dr. Susheel Kumar Singh obtained his B.Sc. from University of Allahabad, Allahabad. He has completed his M.Sc. in Electronics as well as M.Sc. in Physics from University of Lucknow, Lucknow. He was awarded his doctorate in Physics from University of Lucknow. Currently he is serving as Assistant Professor, Department of Physics at HLYB P.G. College, Associated to University of Lucknow, Lucknow. He has authored 04 Text book for UG and PG Students and published 07 Edited Book. He has published more than 20 research paper in prestigious international journals. He has organised more than 20 Conference/FDP/Workshop with Collaboration of National and International Institutes. Dr. Singh is General Secretary of prestigious Educational Society named by MKSES Educational Society Lucknow, UP, India. He has great research passion in the area of Material Science. Dr. Singh participated and presented his research work in many National and International Conferences.



Dr. Bhuvan Bhasker Srivastava, Associate Professor & Head, Department of Physics, Shia P.G. College, Lucknow (Associated College of University of Lucknow). He has authored 02 Text Books for UG and PG Students. He is the editor of five books He is famous for applying various innovative methods of teaching physics. He has published 23 research papers in prestigious international journals. He has organised many Conference, FDP and Workshops with Collaboration of National and International Institutes. He has delivered several Invited talks and presented his research work in various National and International Conference. Dr. Srivastava is Life Members of Indian Science Congress, Indian Association of Physics Teachers (IAPT), Material Research Society of India (MRSI). Dr. Srivastava has got many Awards namely “Best Faculty Award” from Global Academic Research Excellence Award (GAREA-2021), “Harish Chandra Karmathta Award” and “Pratibhagita Samman from sewayojan Nideshalay, Lucknow, UP. Various leading Newspapers have published news under the Headlines of “BlackSe White Ki Aur”, “City Ke Rancho” & “Nahi Banna Hai Chatur and “Guru Ji Khas Teaching Bemisal” in connection with his unique teaching style.



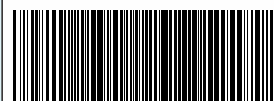
Prof. (Dr.) C.K. Dixit M.Sc, M.Phil, Ph.D. FICS, FPAS, MMR (Singapore), D.Sc (California USA), D.sc (south Africa) known personality, who has more than 21 years of teaching and research experience. He has served as Professor, HOD & Dean, in renowned institutes and universities. Prof. Dixit has done extensive research in the field of Nano Science, Material Science, Semiconductor, Transistor Circuitry, Microelectronics, VLSI Fabrication and Solid State Physics/Electronic Devices. Prof. Dixit has associated with IISc Bangalore, SCL Chandigarh and research laboratories in USA, UK, Netherland, Singapor, China, Turkey, Taiwan, Brazil and Germany. Prof. Dixit has published more than 76 research paper & 12 books & Prof. C.K. Dixit is currently working as Dean, Faculty of Science & Technology and Head Department of Physics at Dr. Shakuntala Misra National Rehabilitation University Mohan Road, Lucknow. Prof. C.K. Dixit received “Best professor award” given by Dewang Mehta National Education Awards and also he received “Best educationist award” given by Economic Growth Foundation New Delhi in 2017. Young Scientist Award in 2019 in educational Summit CEGR New Delhi & Best Dean Award in 2019 by international Council of American research, International lifetime achievement award by ICAR, U.S.A. Professor dixit is advisor of different American and Indian universities




MKSES PUBLICATIONS LUCKNOW, INDIA

Address: Head office: 1st Floor, Building No-85A,
(Nanak Arcade Near Shani Mandir, Parag road,
LDA Colony, Kanpur Road, Lucknow-226012
Mobile No: +919838298016, +918299547952
office Land line No: +91 5223587193
E-mail: mkespublication@gmail.com
Website : mksespublications.com

ISBN 978-93-91248-76-5



Available on 



PRICE
INR (₹): 299/-
USD (\$) : 10/