



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 2, February 2015

Performance Issues in Mobile Adhoc Networks

P.B.Selvapriya¹, K.C.Maheswari², V.Hemalatha³

Assistant Professor, Department of CSE, N.S.N. College of Engineering and Technology, Karur, Tamilnadu, India^{1,2,3}

ABSTRACT: A MANET is a type of ad hoc network that can change locations and configure itself on the go. Since MANETS are mobile, they use wireless connections to connect to various networks. It can be a standard Wi-Fi connection, or another medium such as a cellular or satellite transmission. It is an autonomous system which changes dynamically over time. In this paper we discuss about their characteristics and protocols used for communicating with other devices. Adhoc network should not only find the good path for its data travel but also adapt to changes in topologies. In this paper all the information of Mobile Ad Hoc Network which include the history of ad hoc, wireless ad hoc, wireless mobile approaches and types of Mobile Ad Hoc networks, performance issues are discussed.

KEYWORDS: Wireless Ad hoc networks, mobility, ad hoc network routing protocols, wireless mobile approaches, Manet, mobile ad-hoc sensor network, Ad hoc applications.

I. INTRODUCTION

Due to the recent development of communication wireless links and standards are emerging into boom. Mobile Ad Hoc Network (MANET) is a completely wireless connectivity through the nodes constructed by the actions of the network with a limited bandwidth and other features, network members may be connected with Personal Digital Assistant (PDA), laptops, mobile phones, digital cameras, MP3 players, and so on. Mobility is the term used to denote actions hosts roaming in a different domain; they can retain their own fixed IP address, without the need to constantly changing, IP address. Mobile IP nodes deal with IP address management of foreign agent and Home Agent to the Mobile Node. Ad Hoc Network to be provided by Mobility is a fully wireless, can be any mobile network infrastructure, without a base station, all the nodes can be any link, every node simultaneously take Router work with the Mobile IP completely different levels of Mobility.

Three features must be present in an application for it to deserve the ad hoc label:

- *Mobility:* in order to be able to use the application everywhere, the user should not be limited by range. The range limit is set by the business logic of the application.
- *Peer-to-Peer:* direct communication between peers is mandatory. This means that the client/server relationship is defined in an ad hoc manner by the application logic (direct interaction between the pieces of software).
- *Collocation:* all logical interactions between applications must result in a physical interaction between users. This means that in order to be called an ad hoc application, the service has to be location-based.

II. RELATED WORK

The paper^[1] investigated the effects of mobility on TCP performance in mobile ad hoc networks. Through simulation it was noted that TCP throughput drops significantly when node movement causes link failures, due to TCP's inability to recognize the difference between link failure and congestion. It made this point clearer by presenting several specific examples, one of which resulted in zero throughput, the other, in an unexpected rise in throughput with an increase in speed. A new metric, expected throughput was introduced which provides more accurate means of performance comparison by accounting for the differences in throughput when the number of hops varies. Then the metric was used to show how the use of explicit link failure notification (ELFN) can significantly improve TCP performance, and gave a performance comparison of a variety of potential ELFN protocols.

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 2, February 2015

This paper^[9] describes that the performance issues can be classified in three main categories, namely; Configurations that lead to long-term fairness issues in which some flows suffer from starvation while other flows capture the whole channel bandwidth, Configurations that result in short-term fairness issues where the frames are emitted in bursts and Configurations that result in overall throughput decrease, where a part of the network capacity is not used and thus wasted.

III. WIRELESS ADHOC NETWORKS

An adhoc network is a local area network (LAN) that is built spontaneously as devices connect. Instead of relying on a base station to coordinate the flow of messages to each node in the network, the individual network nodes forward packets to and from each other. An adhoc network is made up of multiple “nodes” connected by “links.” Links are influenced by the node's resources (e.g., transmitter power, computing power and memory) and behavioral properties (e.g., reliability), as well as link properties (e.g. length-of-link and signal loss, noise, etc.). Since links can be connected or disconnected at any time, a functioning network must be able to cope with this dynamic restructuring, preferably in a way that is timely, efficient, scalable, reliable and robust.

The network must allow any two nodes to communicate by relaying the information via other nodes. A “path” is a series of links that connects two nodes. Various routing methods use one or two paths between any two nodes; flooding methods use all or most of the available paths.



Fig 1. Wireless Adhoc Network

IV. COMPARISON OF AD HOC WIRELESS LAN AND INFRASTRUCTURE WIRELESS LAN

Most Wi-Fi networks function in infrastructure mode. Devices on the network all communicate through a single access point, which is generally the wireless router. For example, let's say you have two laptops sitting next to each other, each connected to the same wireless network. Even when sitting right next to each other, they are not communicating directly. Instead, they are communicating indirectly through the wireless access point. They send packets to the access point probably a wireless router and it sends the packets back to the other laptop. Infrastructure mode requires a central access point that all devices connect to.

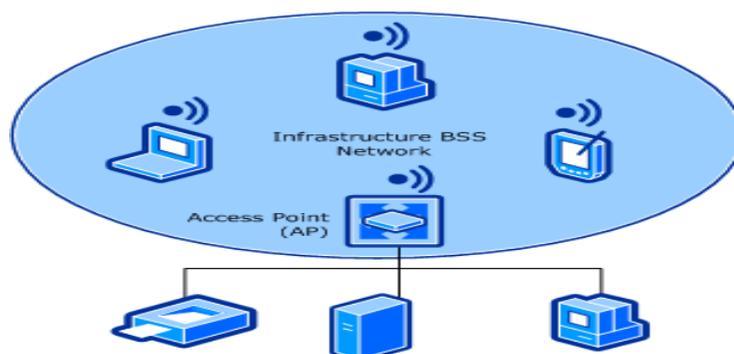


Fig 2. Infrastructure wireless LAN



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 2, February 2015

Infrastructure mode is ideal if you are setting up a more permanent network. Wireless routers that function as access points generally have higher-power wireless radios and antennas so they can cover a wider area. If you're using a laptop to set up a wireless network, you'll be limited by the power of the laptop's wireless radio, which won't be as strong as a router's. Ad-hoc mode is also known as "peer-to-peer" mode. Ad-hoc networks don't require a centralized access point. Instead, devices on the wireless network connect directly to each other. If you set up the two laptops in ad-hoc wireless mode, they'd connect directly to each other without the need for a centralized access point. Ad-hoc mode can be easier to set up if you just want to connect two devices to each other without requiring a centralized access point. For example, let's say you have two laptops and you are sitting in a hotel room without Wi-Fi. You can connect them directly with ad-hoc mode to form a temporary Wi-Fi network without needing a router. The new Wi-Fi Direct standard also builds on ad-hoc mode, allowing devices to communicate directly over Wi-Fi signals.

V. BASICS OF MOBILE AD HOC NETWORKS

A mobile ad-hoc network can also be used to provide crisis management services applications. In Mobile ad hoc network applications, packets generated by other nodes are forwarded to their destination. These nodes are often energy-constrained that is, battery-powered devices with a great diversity in their capabilities. Furthermore, devices are free to join or leave the network and they may move randomly, possibly resulting in rapid and unpredictable topology changes. In this energy-constrained, dynamic, distributed multi-hop environment, nodes need to organize themselves dynamically in order to provide the necessary network functionality in the absence of fixed infrastructure or central administration.

The specific characteristics and complexities impose many design challenges to the network protocols. In addition, these networks are faced with the traditional problems inherent to wireless communications such as lower reliability than wired media, limited physical security, time-varying channels, interference, etc. Despite the many design constraints, mobile ad hoc networks offer numerous advantages. First of all, this type of network is highly suited for use in situations where a fixed infrastructure is not available, not trusted, too expensive or unreliable. Because of their self-creating, self-organising and self-administering capabilities, ad hoc networks can be rapidly deployed with minimum user intervention.

VI. PERFORMANCE ISSUES

To judge the merit of a routing protocol, one needs metrics which both qualitative and quantitative to measure its suitability and performance. These metrics should be independent of any given routing protocol.

Qualitative properties of MANET routing protocols:

- **Distributed operation:** This is an essential property, but it should be stated nonetheless.
- **Loop-freedom:** It is not required for certain quantitative measures (i.e. performance criteria), but generally desirable to avoid problems such as worst-case phenomena, e.g. a small fraction of packets spinning around in the network for arbitrary time periods. Ad hoc solutions such as TTL values can bound the problem, but a more structured and well-formed approach is generally desirable as it usually leads to better overall performance.
- **Demand-based operation:** Instead of assuming an uniform traffic distribution within the network (and maintaining routing between all nodes at all times), let the routing algorithm adapt to the traffic pattern on a demand or need basis. If this is done intelligently, it can utilize network energy and bandwidth resources more efficiently, at the cost of increased route discovery delay.
- **Proactive operation:** The flip-side of demand-based operation. In certain contexts, the additional latency demand-based operation incurs may be unacceptable. If bandwidth and energy resources permit, proactive operation is desirable in these contexts.
- **Security:** Without some form of network-level or link-layer security, a MANET routing protocol is vulnerable to many forms of attack. It may be relatively simple to snoop network traffic, replay transmissions, manipulate packet headers, and redirect routing messages, within a wireless network without appropriate security provisions. While these concerns exist within wired infrastructures and routing protocols as well, maintaining the "physical" security of the transmission media is harder in practice with MANETs. Sufficient security protection to prohibit disruption of modification of protocol operation is desired.



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 2, February 2015

- **Sleep period operation:** As a result of energy conservation, or some other need to be inactive, nodes of a MANET may stop transmitting and/or receiving (even receiving requires power) for arbitrary time periods. A routing protocol should be able to accommodate such sleep periods without overly adverse consequences. This property may require close coupling with the link-layer protocol through a standardized interface.
- **Unidirectional link support:** Bidirectional links are typically assumed in the design of routing algorithms, and many algorithms are incapable of functioning properly over unidirectional links. Nevertheless, unidirectional links can and do occur in wireless networks. Oftentimes, a sufficient number of duplex links exist so that usage of unidirectional links is of limited added value. However, in situations where a pair of unidirectional links (in opposite directions) form the only bidirectional connection between two ad hoc regions, the ability to make use of them is valuable.

Quantitative properties of MANET routing protocols:

- **End-to-end data throughput and delay:** Statistical measures of data routing performance (e.g., means, variances, distributions) are important. These are the measures of a routing policy's effectiveness i.e., how well it does its job as measured from the external perspective of other policies that make use of routing.
- **Route Acquisition Time:** A particular form of external end-to-end delay measurement of particular concern with "on demand" routing algorithms which is the time required to establish route(s) when requested.
- **Percentage Out-of-Order Delivery:** An external measure of connectionless routing performance of particular interest to transport layer protocols such as TCP which prefer in-order delivery.
- **Efficiency:** If data routing effectiveness is the external measure of a policy's performance, efficiency is the internal measure of its effectiveness. To achieve a given level of data routing performance, two different policies can expend differing amounts of overhead, depending on their internal efficiency. If control and data traffic must share the same channel, and the channel's capacity is limited, then excessive control traffic often impacts data routing performance. It is useful to track several ratios that illuminate the internal efficiency of a protocol in doing its job (there may be others that the authors have not considered).
- **Average number of data bits transmitted/data bit delivered:** This can be thought of as a measure of the bit efficiency of delivering data within the network. Indirectly, it also gives the average hop count taken by data packets.
- **Average number of control bits transmitted/data bit delivered:** This measures the bit efficiency of the protocol in expending control overhead to delivery data. Note that this should include not only the bits in the routing control packets, but also the bits in the header of the data packets. In other words, anything that is not data is control overhead, and should be counted in the control portion of the algorithm.
- **Average number of control and data packets transmitted/data packet delivered:** Rather than measuring pure algorithmic efficiency in terms of bit count, this measure tries to capture a protocol's channel access efficiency, as the cost of channel access is high in contention-based link layers [15].

In networking context, the essential parameters that should be varied include:

- **Network size:** Measured in the number of nodes.
- **Network connectivity:** The average degree of a node (i.e. the average number of neighbors of a node).
- **Topological rate of change:** The speed with which a network's topology is changing
- **Link capacity:** Effective link speed measured in bits/second, after accounting for losses due to multiple access, coding, framing, etc.
- **Fraction of unidirectional links:** How effectively does a protocol perform as a function of the presence of unidirectional links?
- **Traffic patterns:** How effective is a protocol in adapting to non-uniform or bursty traffic patterns?
- **Mobility:** When and under what circumstances, is temporal and spatial topological correlation relevant to the performance of a routing protocol?
- **Fraction and frequency of sleeping nodes:** How does a protocol perform in the presence of sleeping and awakening nodes?



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 2, February 2015

VII. EXISTING AD HOC PROTOCOLS

An ad hoc routing protocol is a convention, or standard, that controls how nodes decide which way to route packets between computing devices in a mobile ad hoc network. In ad hoc networks, nodes do not start out familiar with the topology of their networks; instead, they have to discover it. The basic idea is that a new node may announce its presence and should listen for announcements broadcast by its neighbors. Each node learns about nodes nearby and how to reach them, and may announce that it, too, can reach them. Some of the existing protocols are:

- Pro-active (table-driven) routing
- Reactive (on-demand) routing
- Flow-oriented routing and Multicast routing
- Adaptive (situation-aware) routing
- Hybrid (both pro-active and reactive) routing
- Hierarchical routing protocols
- Host Specific Routing protocols
- Geographical routing protocols
- Power-aware routing protocols
- Geographical multicast protocols (Geo casting)

VIII. APPLICATIONS OF AD HOC NETWORKS

The various applications of Ad hoc Networks:

- **Business Environments:** It can be used in where there is a need for collaborative computing might be more important outside the office environment than inside, such as in a business meeting outside the office to brief clients on a given assignment.
- **Game theory:** It deals with multi-person decision making, in which each decision maker tries to maximize his utility. Crisis management services applications.
- **Tactical networks:** Military communication and operations, Automated battlefields Emergency services, Search and rescue operations, Disaster recovery, Replacement of fixed infrastructure in case of environmental disasters, Policing and firefighting, Supporting doctors and nurses in hospitals and in Commercial & civilian environments.
- **E-commerce:** Electronic payments anytime and anywhere.
- **Business:** Dynamic database access and mobile offices
- **Vehicular services:** Road or Accident Guidance, Transmission of Road & Weather Conditions, Taxi Cab Network, Inter-Vehicle Networks, Trade Fairs, Shopping Malls, Networks of Visitors at Airports, Home & Enterprise
- **Home/office wireless networking:** Conferences, meeting rooms, Personal area networks(PAN), Personal networks(PN), Networks at construction sites
- **Education:** Universities and campus settings, Virtual classrooms, Ad hoc communications during meetings or lectures.
- **Entertainment:** Multi-user games, Wireless P2P networking, Outdoor Internet access, Robotic pets, Theme parks, Sensor networks.
- **Home applications:** Smart sensors and actuators embedded in consumer electronics
- **Body Area Networks (BAN):** Data tracking of environmental conditions, animal movements, chemical/biological detection.
- **Context aware services:** Follow-on services like call-forwarding and mobile workspace.
- **Information services:** Location specific services and time dependent services.
- **Infotainment:** Touristic information, Coverage extension, Extending cellular network access, linking up with the Internet, intranets, etc.

IX. CONCLUSION

The inherent unpredictability in a network whose nodes move poses a challenge to routing and mobility functions if they are to deliver data consistently between the network nodes. The most attractive property of an ad hoc networking model is perhaps its independence from centralized control and, thus, the increased freedom and flexibility it gives the user. Due to its inherent flexibility, ad hoc networking is easy to deploy and would fit nicely into, say, an office setting, where users could set up ad hoc networking groups using fewer LAN access points and potentially less transmitting power. The ad hoc network functionality will also enable the interconnection of different users' devices for



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 2, February 2015

instance, to facilitate larger ad hoc working groups. The intrinsic ability to create generic, small-scale, ad hoc networks in portable devices represents an entirely new area for future ad hoc based applications.

REFERENCES

- [1] B.S. Bakshi, P. Krishna, D.K. Pradhan and N.H. Vaidya, Improving performance of TCP over wireless networks, in International Conference on Distributed Computing Systems, May 1997.
- [2] Ajay Mahimkar, R. K. Shyamasundar “S-MECRA A Secure Energy-Efficient Routing Protocol for Wireless Ad Hoc Networks” IEEE 2004.
- [3] Alia Fourati, Khaldoun Al Agha, Hella Kaffel Ben Ayed “Secure and Fair Auctions over Ad Hoc Networks”, Int. J. Electronic Business, 2007.
- [4] Anand Patwardhan, Jim Parker, Michaela Iorga, Anupam Joshi, Tom Karygiannis, “Secure Routing and Intrusion Detection in Ad Hoc Networks”, 3rd International Conference on Pervasive Computing and communications (PerCom 2005), Kauai Island, Hawaii.
- [5] I. Aad, J.-P. Hubaux, and E.-W. Knightly, “Denial of Service Resilience in Ad Hoc Networks”, Proc. MobiCom, 2004.
- [6] Bissias, G.D., Liberatore, M., Jensen, D., Levine, B.N., “Privacy vulnerabilities in encrypted HTTP streams” In Proc. Privacy Enhancing Technologies Workshop (PET 2005).
- [7] C. E. Perkins, E. M. Royer, and S. R. Das, “Ad Hoc On-Demand Distance Vector (AODV) Routing,” IETF Mobile Ad Hoc Networks Working Group, Internet Draft, work in progress, 17 February 2003.
- [8] Bing Wua, Jie Wua, Eduardo B. Fernandez, Mohammad Ilyasa, Spyros Magliveras, “Secure and efficient key management in mobile ad hoc networks” Journal of Network and Computer Applications , 937–954, 2007.
- [9] F. Anjum, Anup K. Ghosh, Nada golmie, Paul kolodzy, Radha poovendran, Rajeev shorey, d. Lee, j-sac, “Security in Wireless Ad hoc Networks”, IEEE journal on selected areas in communications, vol. 24, no. 2, February 2006.
- [10] H.-A. Wen, C.-L. Lin, and T. Hwang, “Provably Secure Authenticated Key Exchange Protocols for Low Power Computing Clients,” Computers and Security, vol. 25, pp. 106-113, 2006.
- [11] Haiyun Luo, Petros Zerkos, Jiejun Kong, Songwu Lu, Lixia Zhang, “Self-securing Ad Hoc Wireless Networks”, 7th IEEE Symp. on Comp. and Communications (ISCC), Taormina, 2002.
- [12] Hongmei Deng, Wei Li, and Dharma P. Agrawal, “Routing Security in Wireless Ad Hoc Networks”, IEEE Communications Magazine October 2002.
- [13] Huaizhi Li Zhenliu Chen Xiangyang Qin, “Secure Routing in Wired Networks and Wireless AdHoc Networks” IEEE, 2004.
- [14] Huaizhi Li, Mukesh Singha, “Trust Management in Distributed Systems” IEEE Computer Society February 2007.

BIOGRAPHY



P.B.Selvapriya received her B.E. (Computer Science and Engineering) degree from Avinashilingam University, Coimbatore in 2008 and M.E. (Computer Science and Engineering) degree from Anna University, Chennai in 2012. She is presently working as Assistant Professor in the department of Computer Science and Engineering at N.S.N College of Engineering and Technology, Karur. She has more than 3 years of experience in teaching. She has published and presented more than 9 papers in various International and national journals and conferences. Her research interests are Computer Networks, Software Testing and Advanced Computer Architecture.



K.C.Maheswari received her B.E. (Computer Science and Engineering) degree from Anna University, Coimbatore in 2009 and M.E. (Computer and Communication Engineering) degree from Anna University, Chennai in 2012. She is presently working as Assistant Professor in the department of Computer Science and Engineering at N.S.N College of Engineering and Technology, Karur. She has more than 3 years of experience in teaching. She has published and presented more than 5 papers in various International and national journals and conferences. Her research interests are Design and Analysis of Algorithms, Data Structures, Theory of Computation and Mobile Ad hoc Networks.



V.Hemalatha received her B.E. (Computer Science and Engineering) degree from Bharathidasan University, Tiruchirapalli in 2004 and M.E. (Software Engineering) degree from Anna University, Chennai in 2007. She is presently working as Assistant Professor in the department of Computer Science and Engineering at N.S.N College of Engineering and Technology, Karur. She has more than 8 years of experience in teaching. She has published and presented more than 10 papers in various International and national journals and conferences. Her research interests are Software Engineering, Image Processing, Computer Networks and Database Management Systems.