Per User Spectrum Performance Analysis in Wireless Ad-Hoc Network

Deepak Kumar Mahapatro
Dept. of CSEA IGIT Sarang

Ramesh Kumar Sahoo
Dept. of CSEA IGIT Sarang

Srinivas Sethi
Dept. of CSEA IGIT Sarang

ABSTRACT
Ad-Hoc network is a self-organizing wireless network in which collection of wireless mobile nodes (devices) dynamically forming a temporary network without the use of any existing network infrastructure or centralized administrationi.e.chaotically decentralised.It is a ubiquitous type of computing often referred to as pervasive/invisible computing. It can randomly deploy with no advance planning.In this paper it has been analyzed the performance of Spectrum at each node in terms of Packet Delivery Ratio (PDR) and Throughput subject to Number of Interruptions occurred during transmission.

General Terms:
Algorithm, Networking

Keywords:
Ad-Hoc Network; Spectrum Analysis; Throughput; Packet Delivery Ratio;

1. INTRODUCTION
Wireless networks transmit and receive data via radio frequencies used as an alternative to the conventional cables [2]. Wireless Networking devices can operate in the following modes:

- **Infrastructure mode**
  Wireless networking links a wireless network to a wired ethernet network.An infrastructure mode wireless networking seeks for a wireless access point (AP).To join the WLAN, the AP and all wireless clients must be configured to use the same SSID (Service Set Identifier, i.e. name of the wireless network sought for by the clients).The AP is then connected to the wired network to permit desired access to these wireless clients.
- **Infrastructure less mode**
  The Ad-Hoc mode of communication in which wireless devices communicate with each other in direct manner. This mode of operation let's all the wireless devices within the range of each other to discover and communicate in P2P (peer-to-peer) fashion and central access points are not sought for .Assembling an ad-hoc wireless network involves configuring each wireless adapter for ad-hoc mode and using the same SSID.

Generally speaking ad hoc networking indicates application based unstructured communication configuration in two forms: (a) without using any underlying networking or making use of a highly flexible predetermined structure and (b) using a specially designed dynamic mechanism so that the application network is kept free from any dominating infrastructure's bottlenecks, normally imposed by the rigid disciplines set by underlying infrastructure. The latter group, if designed properly with minimum imposed interference, will give sufficient freedom to help the application systems benefit from effective features enabled by the underlying infrastructure [4].Basically the most natural features of ad hoc networking is built upon its inherent dynamic connectivity, where some simple and relax routing or interconnecting mechanism frees application networking from any possible firm and rigid dominating networking complexities. That is, when the network from its traditional 'strong structure' got weaken, as a result it got loosened up the control elements in the system. This can remove some of infrastructural dependencies over the required connectivity, which in turn enables the ad hoc networking to freely use its own reliable strategies to regain any lost controls due to the disappearance of intensive embedded controlling elements in the system. The firm-control has always been in the nature of traditional systems imposed by the centralized network management [4].Each node in an ad hoc network intercommunicates with each other with single-hop path, multi-hop path or a hybrid way of communication in a peer-to-peer fashion. Each intermediate node present in-between the pair of communicating nodes acts as router. Thus the nodes of an ad hoc network operate both as host as well as router. The nodes in the ad hoc network have the power to change their geographical location according to their need i.e. highly mobile, and so the creation of routing paths may affected because of the addition and deletion of nodes. The topology of the network may change randomly, rapidly, and unexpectedly due to mobility of nodes.

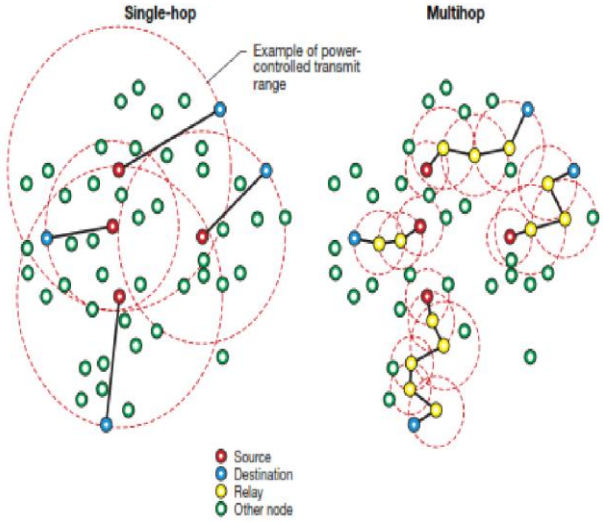

Fig-1: Comparison of multi-hop networking with single-hop networking. Both examples have an identical distribution of network nodes

As we seen in introduction, classification of Wireless networks are infrastructure network and infrastructure less (ad hoc) networks and According to their application types of Wireless ad hoc networks are:

A **wireless mesh network** (**WMN**) is a communications network made up of radio nodes organized in a mesh

topology. Wireless mesh networks often consist of mesh clients, mesh routers and gateways. The mesh clients are often laptops, cell phones and other wireless devices while the mesh routers forward traffic to and from the gateways which may but need not connect to the Internet. The coverage area of the radio nodes working as a single network is sometimes called a mesh cloud. Access to this mesh cloud is dependent on the radio nodes working in harmony with each other to create a radio network. Wireless mesh networks can be implemented with various wireless technology including 802.11, 802.15, 802.16, cellular technologies or combinations of more than one type. Mesh networks may involve either fixed or mobile devices. The solutions are as diverse as communication needs, for example in difficult environments such as emergency situations, tunnels, oil rigs, battlefield surveillance, high speed mobile video applications on board public transport or real time racing car telemetry. Some current applications: a. U.S. military forces are now using wireless mesh networking to connect their computers, mainly ruggedized laptops, in field operations. b. Electric meters now being deployed on residences transfer their readings from one to another and eventually to the central office for billing without the need for human meter readers or the need to connect the meters with cables.

A **wireless sensor network (WSN)** consists of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, humidity, motion or pollutants and to cooperatively pass their data through the network to a main location [16]. The more modern networks are bi-directional, also enabling control of sensor activity. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on. Application of Wireless Sensor Network includes area monitoring which is a common application of WSNs. In area monitoring, the WSN is deployed over a region where some physical and environmental phenomenon like temperature, sound, pressure etc. is to be monitored. A military example is the use of sensors to detect enemy intrusion; a civilian example is the geo-fencing of gas or oil pipelines[16].

A **Mobile Ad-Hoc Network** (MANET)is a self-configuring infrastructure less network of mobile devices connected by wireless links. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger Internet [16]. Different protocols are then evaluated based on measure such as the packet drop rate, the overhead introduced by the routing protocol end-to-end packet delays, network throughput etc. Furthermore MANET can be categorised into three types, **a.**Vehicular Ad-Hoc Network (VANET) is a technology that uses moving cars as nodes in a network to create a mobile network. VANET turns every participating car into a wireless router or node, allowing cars approximately 100 to 300 meters of each other to connect and, in turn, create a network with a wide range [16]. As cars fall out of the signal range and drop out of the network, other cars can join in, connecting vehicles to one another so that a mobile Internet is created. It is estimated that the first systems that will integrate this technology are police and fire vehicles to communicate with each other for safety purposes.**c.** Internet Based Mobile Ad-hoc Networks (iMANET) are ad-hoc networks that link mobile nodes and fixed Internet-gateway nodes. In such type of networks normal ad hoc routing algorithms don't apply directly. Wireless networks can generally be classified as wireless fixed networks, and wireless, or mobile ad-hoc networks. MANETs are based on the idea of establishing a network without taking any support from a centralized structure. By nature these types of networks are suitable for situations where either no fixed infrastructure exists, or to deploy one is not possible. **b.** Intelligent vehicular ad-hoc networks (InVANETs) defines an intelligent way of using Vehicular Networking [16]. InVANET integrates on multiple ad-hoc networking technologies such as WiFi IEEE 802.11, WAVE IEEE 1609, WiMAX IEEE 802.16, Bluetooth, IRA, ZigBee for easy, accurate, effective and simple communication between vehicles on dynamic mobility. Effective measures such as media communication between vehicles can be enabled as well methods to track the automotive vehicles is also preferred. InVANET helps in defining safety measures in vehicles, streaming communication between vehicles, infotainment and telematics.

In traditional networks and early wireless networks, the network connection was based on a hierarchical architecture to construct a stable topology. The static infrastructure provided a series of security mechanisms and strategies, such as encryption, authentication, access control and rights management, firewalls, etc. Ad hoc networks still apply basic security requirements, such as confidentiality, integrity, availability and authenticity; nevertheless, they cannot sacrifice a lot of power for complex calculations considering the energy consumption of wireless transmission and radio spectrum resources [7]. In addition, limited by the node's hardware resources, a robust security protection mechanism was difficult to achieve. As ad hoc network resources were so limited, many traditional network security policies and strategies could not be directly applied, so numerous modifications to the existing security methods and strategies were required. Moreover, the ad hoc network nodes act both as routers and as communication end points are easy victims of passive eavesdropping, active message insertions, and denial of service and battery-exhaustion attacks. In dealing with multiple threats to network environments, the use of cryptographic keys has been one trustworthy solution. Specific key management strategies are required to maintain ad hoc network robustness [6].

With the ever-growing capabilities of the information communication technologies (ICT), there are always more choices and even more selectivity capabilities to develop new embedded superior applications in new forms of smart nodes at the user and service ends for more reliable and dependable connections, where many superior new scenario-based applications can be established using localized self-controlled agent-style processes than ever before. They can be used for controlling and monitoring systems using superlight, reliable and simple intelligent microcontrollers to maintain many sophisticated operations including effective interconnections, reliable routings, fault-tolerant networking while maintaining the required quality, security and efficiency of the systems.

In this paper it has been analyzed the spectrum performance in ad-hoc network using NS-2 simulator.

The rest of the paper is started with related works in section 2,followed by Experiment in NS-2 environment in section

3.Results analysis has been discussed in section 4. Finally conclusion is discussed in section 5.

2. RELATED WORKS

It throws light upon the Authenticated Routing for Ad hoc Networks (ARAN) protocol that uses public key cryptography, a managed-open environment with a minimum of security provisions like authentication, message integrity, non-repudiation [1]. Here the nodes need to obtain a public key certificate issued by a common certificate authority, Route discoveryi.e. the source circulates a digitally signed Route Discovery Packet (RDP) and the corresponding destination responds by sending a digitally signed Route Reply Packet (REP) back to the source [1].

Implementation of various techniques have been highlighted like protection against blackhole attack, SAR protocol which uses AODV as a platform, Integrated security metric within the RREQ and RREP packets [13]. The discovered routes guarantee "quality of protection" [2].User identity is bound with an associated trust level i.e. impersonating attacks can thereby be prevented with stronger access control mechanisms. For each trust level, a simple shared secret is used to generate a symmetric encryption/decryption key. Moreover, SAR comes with a package of cryptographic techniques such as encryption, digital signature etc [9].

Here it conceptualises protection against wormhole attacks and packet leashes [3]. Packet leashes constitute of, (i) Geographical i.e. the receiver of the packet is within a certain distance from the sender and each node has to know its own location. It is a must for all nodes have loosely synchronized clocks.(ii)Temporal i.e. the packet carries an upper bound on its lifetime restricting the maximum travel distance, and nodes need to have clocks tightly synchronised to a time of transmission time plus speed of light or expiration time for the packet.

3. EXPERIMENT WITH NS-2 ENVIRONMENT

Table-1: Simulation Parameters

Sl. No.	Parameters	Values
1.	No. Of Nodes	100
2.	Seed	1
3.	Grid	1000x1000
4.	Max. Conn.	1
5.	Rate	6000kbps
6.	Max. Packets	1,00,000
7.	Packet Size	1500
8.	CS Range	2.5

It has used theNetwork Simulator-2 (NS-2)forsimulation and to find the performance of the spectrum in terms of Throughput and Packet Delivery Ratio at node level. It has calculated the effects on performance of spectrum and data transmission due to No. of Interruptions occurred at each node of ad-hoc network. These interruptions occurred due to various factors like noise, interference, heat, unreachable distance or failure of nearest node.

Here the performance of spectrum has been evaluated by simulations through NS-2. The simulation is carried out with random topology. The source node and destination nodes have been considered in a single ad-hoc network but work in different spectrum bands and the Simulation Parameters for ad-hoc network have been carried out the simulation as per table-1.

4. PERFORMANCE ANALYSIS

In order to calculate the interference power in ad-hoc networks, the density and distribution of the interfering nodes must be known. With the increase in the density of nodes, more nodes will fall within the prohibited transmission areas resulting in a nonlinear increase in density of interfering nodes with the increase in the density of nodes. In case of ad-hoc network, nodes have limited ranges for transmission and each node acts as a router i.e. nodes are both traffic sources/sinks and intermediate forwarders. Tthroughput is the measure of rate of successful delivery of message over a communication channel.

Here it has been observed that no. of interruptions during transmission isalways directly related to throughput whereas PDR depends on various other factors such as delay resulting some variations in some nodes. PDR is also directly proportional to no. of interruptions but with exception of some exceptional nodes, it is due to some factors like delay. Exceptions occurred at nodes27, 30, 35, 36, 51, 52, 54, 59, 60, 72, 73, 76.

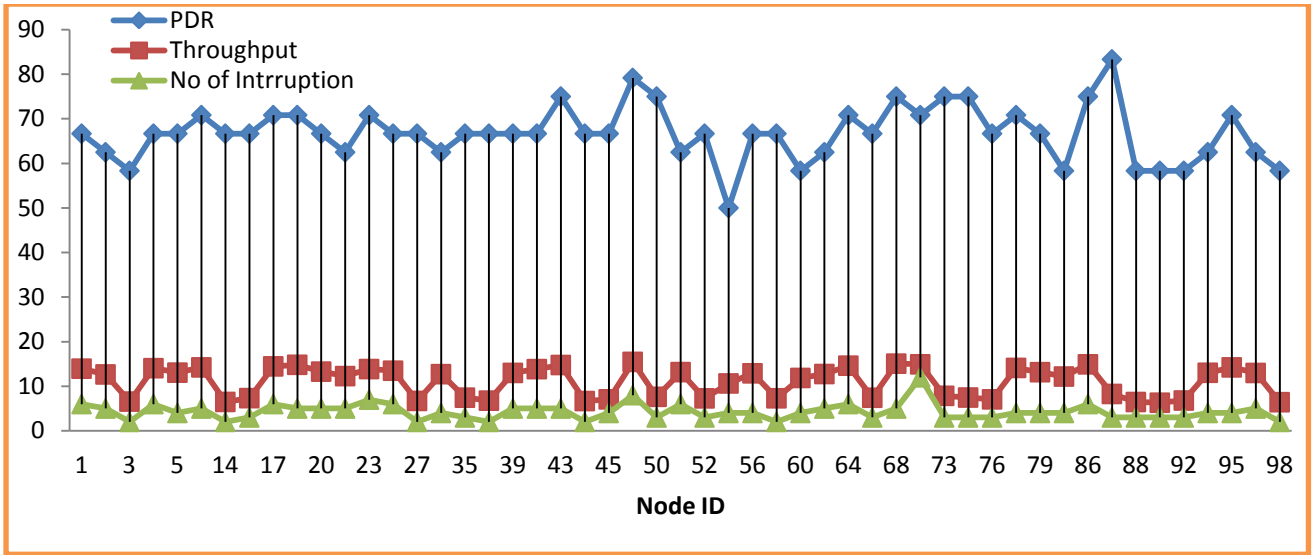

Fig-2: Spectrum Performance Analysis at each Node

Furthermore the possible factors affecting PDR can be classified in terms of their following attributes [6][13][16]:-

A. Source

a. Internal: system noises (thermal noise, shot noise, transit-time noise)

b. External: external noises (atmospheric noise, industrial noise, extra-terrestrial noise),different infrastructural obstacles, sun light ray

B. Type

a. Passive: Traffic monitoring, eavesdropping

b. Active: Disruption in service, alteration of data, dynamic change in route information

C. Mechanisms of attack

a. Basic mechanisms: Resource consumption and disruption in routing

b. Security mechanisms: Key management

D. Layers at which they occur

a. Physical layer: Communication jamming, eavesdropping, message interception

b. Data link layer: traffic analysis and monitoring, service disruption

c. Network layer:

i. Route discovery: Routing table overflow, message flooding, , routing cache poisoning

ii. Route maintenance: fake control messages

iii. Data forwarding: Black hole attack, wormhole attack

iv. Other complex attacks: Sleep bereaving, disclosing location of all nodes

d. Transport layer: Session hijacking

e. Application layer: Rejection RREQ of other nodes, Mobile virus, worm attack

5. CONCLUSION

Ad hoc networks are very much useful in many application environments and it doesn't need anyinfrastructure support. It is more effective to build a communication network in smaller areas (building organizations, conferences, etc.). It can be set up using ad hoc networking technologies. These networks can also set up in applications domains like communication systems in battlefields and disaster recovery areas like flood, cyclone. These are the areas where it is quite difficult to set up a communication system with fixed centralized set up like base station and centralized access point. Similarly communications using a network of sensors or using floats over water are other applications.

In this paper appropriate results has been obtained for PDR, throughput with subject to no of interruptions, but with some exceptional nodes where PDR hasvariations from its expected rate as per respective throughput. It's due to some external factors discussed in this paper. The objective of this paper is satisfied with the intended results obtained.

6. FUTURE SCOPE

The increasing use of collaborative applications and wireless devices like cell phones, laptops they can be further added to the needy and the usage of ad hoc networks. Iinfrastructure mode of communication is always ideal if you're setting up a more permanent network. Each wireless router that functions as access points at ad hoc network generally have higher power wireless radios, base stations and antennas so they can cover a wider area for communication. An ad hoc based distributed system makes it possible to envision the emergence of distributed pattern of features that could hardly be thought of. i.e. Features such as distributed intelligence, distributed security, distributed control and many more new and superior distributed application technologies can emerge that require a better understanding and pass over onto researchers to take on board for future technological innovations [6]. A Major challenge towards implementation of this network technology is to make guarantee the quality of service (QoS) in such a network, that too even more difficult in case the nodes are too mobile. Much work remains to be done on cost-effective implementation issues to bring the promise of ad hoc networks within the reach of the public.

7. ACKNOWLEDGEMENT

I would like to thank all those people who made thispaper possible and an unforgettable experience for me. Iavail this opportunity to express my gratitude and whole hearted thanks to Guide **Prof. Srinivas Sethi,** and also thank him for the systematic guidance and friendly advices during the paper work.

I acknowledge my overwhelming gratitude and sincere thanks to **Mr. Ramesh Kumar Sahoo** who giving me supportand encouragement whenever I was in need.

8. REFERENCES

[1] "A secure Routing Protocol for Ad Hoc Networks", Kimaya Sanzgiri, Bridget Dahill, Brian Neil Levine, Clay Shields, Elizabeth M. Belding-Royer, Oct 2001

[2] Seung Yi, Prasad Naldurg, Robert Kravets,"Security-Aware Ad Hoc Routing for Wireless Networks", Aug 2001

[3] Yih-Chun Hu, Adrian Perrig, David. B. Johnson,"Packet Leashes: A Defense Against Wormhole Attacks in Wireless Ad Hoc Networks", IEEE INFOCOM 2003

[4] Adam Burg, "Ad hoc network specific attacks", Seminar on Ad hoc networking: concepts, applications, and security, Technische University at Munchen, 2003

[5] Matias Korman, "Minimizing interference in ad-hoc networks with bounded communication radius", doi:arXiv:1102.2785v5 [cs.CG] 29 Jun 2012

[6] Ashima Rout, Srinivas Sethi, "Throughput Analysis of Spectrum in Cognitive Radio Ad Hoc Network", International Journal of Application or Innovation in Engineering & Management (IJAIEM), Volume 2, Issue 6, June 2013

[7] Kim, W., & Gerla, M. "Cognitive multicast with partially overlapped channels in vehicular ad hoc networks" in Proc. Of Ad-Hoc Networks, 2013.

[8] Hao Yang, Haiyun Luo, Fan Ye, Songwu Lu, Lixia Zhang, "Security in Mobile Ad Hoc Networks: Challenges and Solutions", IEEE Wireless Communications, February 2004

[9] D. Bil`o and G. Proietti. "On the complexity of minimizing interference in ad-hoc and sensor networks. Theoritcal Computer. Sci., 402(1):43–55, 2008.

[10] K. Buchin. "Minimizing the maximum interference is hard. CoRR, doi:abs/0802.2134, 2008.

[11] Su, H., & Zhang, X. (2008); IEEE Journal on Selected Areas in Communications, 26(1), 118–129.

[12] Timmers,M., Pollin, S., Dejonghe, A.,Van der Perre, L.,&Catthoor, F. (2010); IEEE Transactions on Vehicular Technology, 59(1), 446–459.

[13] Akyildiz IF, Lee WY, Vuran MC, Mohanty S. (2006) "NeXt generation/dynamic spectrum access/cognitive radio wireless networks: a survey", computer networks, Vol. 50, no. 13, pp. 2127–2159

[14] Ms. Monika G. Ghorale, Prof. A. O. Bang,"Wireless Ad-Hoc Networks: Types, Applications, Security Goals", International Journal of Advent Research in Computer and Electronics (IJARCE) (E-ISSN: 2348-5523) Special Issue, National Conference "CONVERGENCE 2015", 28 March 2015

[15] Vanita Rani, Dr. Renu Dhir,"A Study of Ad-Hoc Network: A Review" International Journal of Advanced Research in Computer Science and Software Engineering 3(3), March - 2013, pp.135-138.

[16] https://en.wikipedia.org/wiki/Wireless_ad_hoc_network