INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS
ISSN 2320-7345

WIRELESS COMMUNICATION FOR MOBILE AD-HOC NETWORK

R.K.Gayathri[1], E.Saranya[2],M.Santha[3],V.P.Muthukumar[4]

[1]M.Phil, Department of computer science,gritgayathri@gmail.com
[2]M.Phil, Department of computer science,saranvicky.16@gmail.com
[3]Assistant professor, Department of computer science,shanthaa30@gmail.com
[4]Assistant professor, Department of computer science,rajiperisamy@gmail.com
[1,2,3,4] Vivekanandha College of Arts and Sciences for Women (Autonomous),Namakkal.

,

ABSTRACT

Ad hoc wireless internet refers to any set of networks where all devices have equal status on a network and free to associate with any other ad hoc network device in link range. The ad hoc wireless internet extends the services of the internet to the end users over an ad hoc wireless network. Internet-based ad hoc networking is an emerging technology that supports self-organizing, networking infrastructures. The technology enables an autonomous system of nodes, which can operate in isolation or be connected to the greater Internet. Based on a service discovery protocol, our models achieve secure, trusted, anonymous, efficient, and economical communications between unfamiliar parties. Ad hoc networks are designed to operate in widely varying environments, from forward-deployed temporary military settlements, battlefields and broadband internet services in rural regions.

Keywords: Ad-hoc wireless networks, Mobile ad hoc network, Multi hop mobile ad hoc, Bluetooth ad-hoc networks for voice, Routing protocol, Anti-jamming.

1. INTRODUCTION

Wireless ad-hoc networks do not require any fixed equipment or infrastructures such as routers, switches, access points, base stations, and cables. Nodes communicate with each other through radio signals to organize a network and transmit data from one node to another. We address the problem of control-channel jamming attacks in multi-channel ad hoc networks. To avoid this threat sender may want to send multiple copies through multiple disjoint paths .In such situations, wireless ad hoc networks are expected to accommodate real-time multimedia traffic for remote monitoring, video conferencing, and VoIP (Voice over IP) communications. Packets which are transmitted over a wireless ad-hoc network may include file transfer, e-mail, and Web and real-time traffic as remote monitoring, video conferencing, and VoIP. It has been recognized that the effective network capacity of a single-channel and multi-hop wireless network using the normal IEEE 802.11.

Ad hoc networking enables wireless devices to network with one another, when access to the Internet is unavailable. It enables a wide range of powerful applications, from instant conferencing between notebook PC users to emergency and military services. Wireless communication should be possible without routers, base stations or Internet Service Providers. An ad-hoc network might consist of several home-computing devices, as well as a notebook computer that must exist on home and office networks without extra administrative work. Key applications of ad-hoc networking are conferencing, home networking, emergency services, Personal Area Networks, Bluetooth, and more.A wireless ad hoc network consists of mobile nodes that are powered by batteries. The routers are free to move randomly and organize themselves arbitrarily making the network's wireless topology change rapidly and unpredictably. Such a network may operate in a standalone fashion, or may be connected to the larger Internet.

2. AD-HOC WIRELESS NETWORKS

This vision of embeddable wireless connectivity has been in development for several years at AT&T Laboratories Cambridge in the context of the Pico net project and is also being pursued, although with emphasis on different aspects, by several other groups including Home RF IrDA which uses infrared instead of radio and Bluetooth . Everyone including potential users knows that wireless networking is more prone to passive eavesdropping attacks. But it would be highly misleading to take this as the only, or even the main, security concern. In this paper we investigate the security issues of an environment characterized by the presence of many principals acting as network peers in intermit tent contact with each other. To base the discussion on a concrete example we shall consider a wireless temperature sensor. Nearby nodes may be authorized to request the current temperature, or to register a watch that will cause the thermometer to send out a reading when the temperature enters a specific range. We wish to make our thermometer useful in the widest range of environments including environmental monitoring, industrial process control and medicine. We will therefore consider how we can enable our thermometer to support all the security properties that might be required, including on dentiality, integrity and availability. Contrary to academic tradition, however, we shall examine them in the opposite order, as this often and certainly in our case reflects their actual importance. First, however, we have to mention some of the resource constraints under which such networks operate.

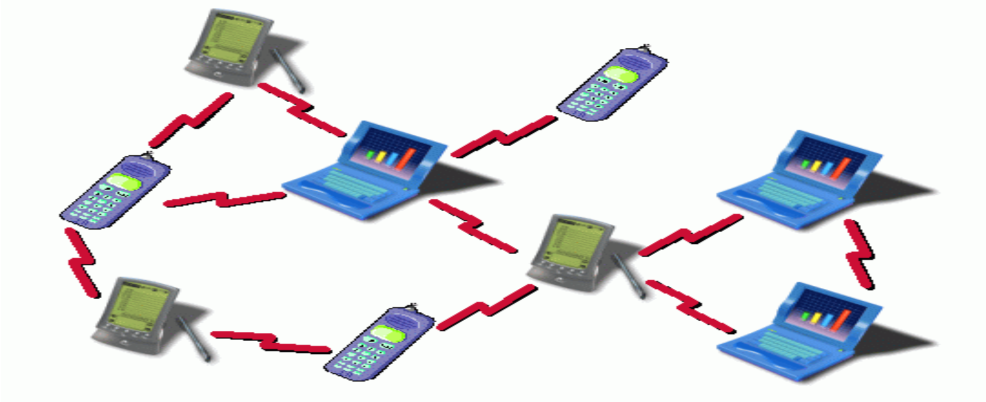

FIG: A MODEL OF AD-HOC WIRELESS NETWORKS

The performance of TCP degrades in Ad Hoc networks. This is because TCP has to face new challenges due to several reasons specific to these networks: lossy channels, hidden and exposed stations, path asymmetry, network partitions, route failures, and power constraints. The sending rate of a TCP connection is regulated by two distinct mechanisms, the flow control and the congestion control. Although these mechanisms are similar, in the sense that both attempt to prevent the connection from sending at an excessive rate, they have specific purposes. Flow control is implemented to avoid that a TCP sender overflows the receiver’s buffer. Thus, the receiver advertises in every ACK transmitted a window limit to the sender.

Lossy channels:
The main causes of errors in wireless channel are the following:
1. Signal attenuation
2. Doppler shift
3. Multipath fading

3. AD-HOC PATH ASYMMETRY

Path asymmetry in Ad Hoc networks may appear in several forms like bandwidth asymmetry, loss rate asymmetry, and route asymmetry.

1) BANDWIDTH ASYMMETRY:

Satellite networks suffer from high bandwidth asymmetry, resulting from various engineering tradeoffs such as power, mass, and volume, as well as the fact that for space scientific missions, most of the data originates at the satellite and flows to the earth. The return link is not used, in general, for data transferring. For example, in broadcast satellite networks the ratio of the bandwidth of the satellite-earth link over the bandwidth of the earth-satellite link is about 1000 On the other hand in Ad Hoc networks, the degree of bandwidth asymmetry is not very high. For example, the bandwidth ratio lies between 2 and 54 in Ad Hoc networks that implement the IEEE 802.11 version g protocol .The asymmetry results from the use of different transmission rates.

2) LOSS RATE ASYMMETRY:

This type of asymmetry takes place when the backward path is significantly more lossy than the forward path. In Ad Hoc networks, this asymmetry is due to the fact that packet losses depend on local constraints that can vary from place to place. Note that loss rate asymmetry may produce bandwidth asymmetry.

3) ROUTE ASYMMETRY:

Unlike the previous two forms of asymmetry, where the forward path and the backward path can be the same, route asymmetry implies that distinct paths are used for TCP data and TCP ACKs. This asymmetry may be artifact of the routing protocol used. Route asymmetry increases routing overheads and packet losses in case of high degree of mobility. Because when nodes move, using a distinct forward and reverse route increases the probability of route failures experienced by TCP connections. However, this is not the case of static networks or networks that have low degree of mobility, like the case of a network with routes of high lifetime compared to the session transfer time.

4. IMPROVING TCP PERFORMANCE IN MULTI HOP MOBILE ADHOC NETWORK

The contention on the wireless channel. TCP unfairness. The first two problems are the main causes of TCP performance degradation in MANETs, and the other two problems are the main causes of TCP performance degradation in SANETs. Based on these four problems, the proposals that aim to improve TCP performance over Ad Hoc networks are regrouped in four sets. The proposals are classified in two categories: cross layer proposals and layered proposals. In cross layer the TCP and underlying protocol work jointly.
There are two approaches of cross layer

1. Evolutionary approaches
2. Revolutionary approaches

For example if the routing layer experiences the routing failure then it sends feedback to TCP. On receiving the notification the TCP enters into freezing state. TCP stops sending packets. After the route is established TCP goes to normal state. In layered, the issues are addressed at any one of the OSI layer. Layered concept is primarily used in wired network. Ad hoc network oppose layered protocol because of dynamic nature, infra structure less architecture, limited resources, and mobility of nodes, time varying stable links and topology.

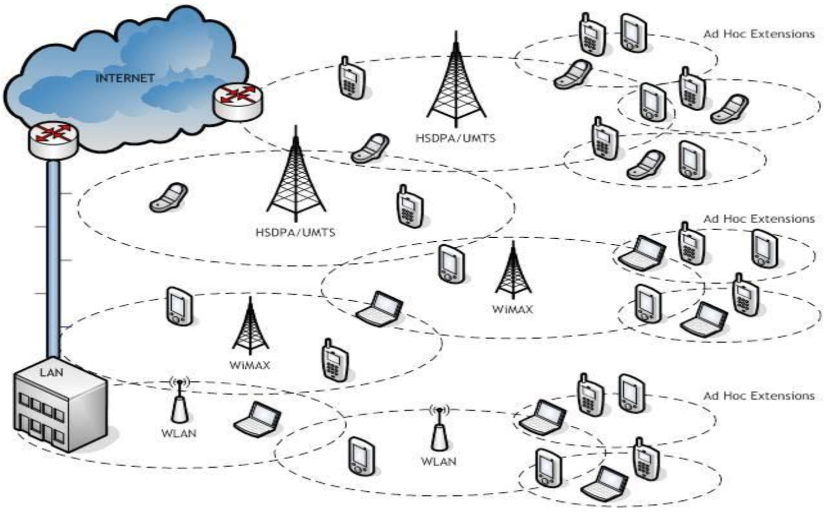

FIG: WLAN ARCHITECTURE

5. MOBILE ADHOC NETWORK

In an ad hoc network, the topology changes very frequently, as nodes may join and leave the network. Thus routing in ad hoc networks has to be different from routing in wired networks to handle the issue of mobility, frequently changing topology, route breaks, low band-width and high delay, interference, limited energy of mobile nodes etc. A variety of routing algorithms for multi hop ad hoc networks have been proposed. These protocols should have characteristics like minimal control and processing overhead, multichip routing capability, dynamic topology maintenance etc. Routing protocols are mainly classified as proactive and reactive routing protocols.

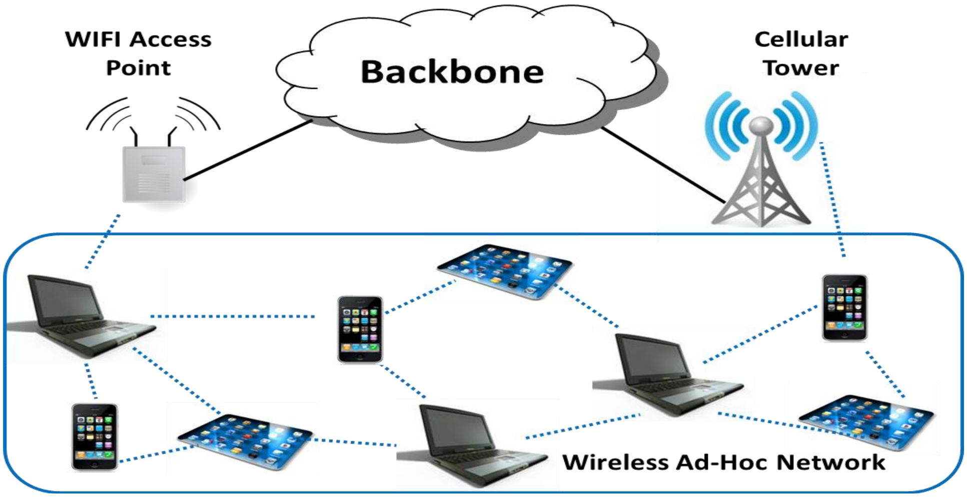

FIG: WI-FI COMMUNICATIONS

Mobile Ad hoc networks have special characteristics, such as highly variable connectivity, mobility, disconnection, location dependency, energy and resource constraints, low bandwidth etc. So existing P2P networks cannot be directly deployed in such environments. New protocol or modifications to existing ones are required to facilitate P2P data sharing and dissemination over MANET.

6. BLUETOOTH BASED AD-HOC NETWORKS FOR VOICE

Bluetooth (IEEE 802.15.1) is a short-range wireless communications technology originally intended to replace the cables connecting portable and/or fixed devices while maintaining high levels of security. It operates at a frequency of 2.4GHz with bandwidth of few Mbit/s. Each interface can have 7 simultaneous connections. One distinguishes three classes of Bluetooth interfaces depending on their transmission power and potential range.

Bluetooth is thus a technology for short-range networking of few elements. In general, there is a human mediated association of the devices: the person wanting two devices to interoperate has to physically manipulate the devices in order to allow the association. A typical example is a user wanting to pair his hands-free apparatus with a mobile phone.The technology was originally designed for short range personal area networks, but the widespread use of Bluetooth interfaces in consumer portable electronics has opened the
Door to new forms of exploitation.

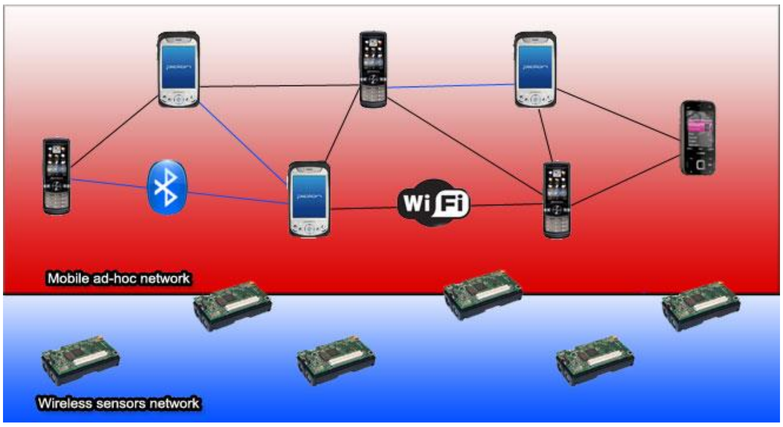

FIG: BLUETOOTH COMMUNICATION

Transmission [FKW02] can be used for transmitting audio using synchronous connection oriented (SCO) links. When we use Blue-tooth as a physical layer for a MANET, we will have several constraints like connected-oriented nature of bluetooth, no broadcast capability, restricted number of connections, long connection set-up time etc. To overcome these problems, a new protocol Bluetooth Scatternet Routing (BSR) has been developed. It is a reactive routing protocol similar to AODV or Dynamic Source Routing (DSR) but keeps additional information on the state of links and tries to avoid long delays due to inquiry or connection setup. The first approach tried to make P2P networking feasible in a mobile environment is JXME[Aro02] based on JXTA. JXTA technology developed by SUN micro systems is a set of open, generalized peer-to-peer protocols that allows any connected device e.g. cell phone to PDA on the network to communicate.

7. LOCATION BASED ROUTING PROTOCOL (LOR)

When a source node wants to transmit a packet, it gets the location of the destination first and then attaches it to the packet header. Due to the destination node’s movement, the multihop path may diverge from the true location of the final destination and a packet would be dropped even if it has already been delivered into the neighbourhood of the destination. To deal with such issue, additional check for the destination node is introduced. At each hop, the node that forwards the packet will check its neighbour list to see whether the destination is within its transmission range. In conventional opportunistic forwarding, to have a packet received by multiple candidates, either IP broadcast or an integration of routing and MAC protocol is adopted.

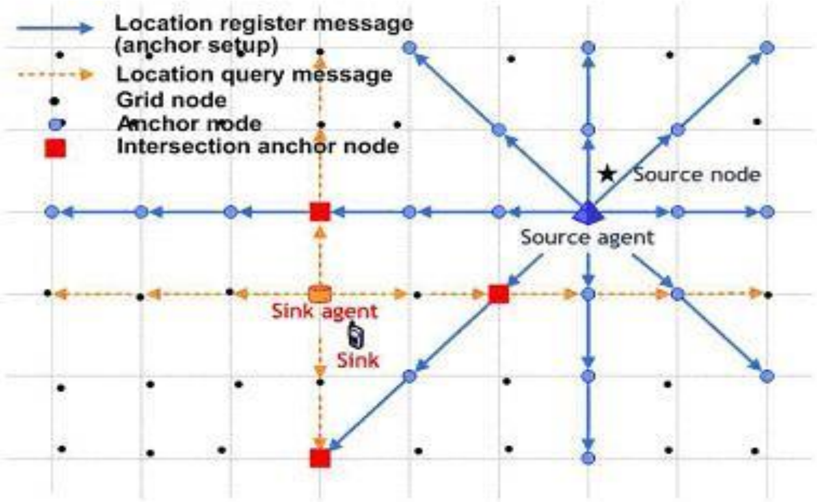

FIG: LOR PATH

The former is susceptible to MAC collision because of the lack of collision avoidance support for broadcast packet in current 802.11, while the latter requires complex coordination and is not easy to be implemented. If a packet with the same ID is received again, it will be discarded. Otherwise, it will be forwarded at once if the receiver is the next hop, or cached in a Packet List if it is received by a forwarding candidate, or dropped if the receiver is not specified. The packet in the Packet List will be sent out after waiting for a certain number of time slots or discarded if the same packet is received again during the waiting period (this implicitly means a better forwarder has already carried out the task).

8. INTRUSION DETECTION IN MOBILE ADHOC NETWORK

Intrusion detection involves the runtime gathering of data from system operation, and the subsequent analysis of the data; the data can be audit logs generated by an operating system or packets “sniffed” from a network. We limit our focus to intrusion detection based on behaviour, we think it is a more efficient, lightweight and easily scalable solution to Intrusion Detection in MANETs. Intrusion Detection Systems based on behaviour can be broadly classified into these categories: anomaly detection, signature or misuse detection, and specification based detection. In signature-based intrusion detection [5][10], the data is matched against known attack characteristics. In anomaly detection find out the normal behaviour of systems, usually established through automated training, are compared with the actual activity of the system to flag any significant deviation. In specification-based detection [7][8], the correct behaviours of critical objects are manually abstracted and crafted as security specifications, which are compared with the actual behaviour of the objects. This paper describes intrusion detection for mobile ad hoc networks. we employ Behavioural-based techniques to monitor the ad hoc on-demand distance vector (AODV) routing protocol, a widely adopted ad hoc routing protocol. AODV is a reactive and stateless routing protocol that establishes routes only as desired by the source node. AODV is vulnerable to various kinds of attacks.

9. ANTI-JAMMING METRICS AD HOC NETWORKS

Several metrics were previously proposed to evaluate the effectiveness of a jammer in impacting the throughput of the network. To mitigate the impact of jamming, we adopt a *dynamic* control channel allocation strategy, whereby each cluster establishes and maintains its own control channel. The impact of long-range jamming attacks can be significantly reduced by varying the spatial and temporal frequency allocation of the control channel. Such a design would also reduce the delay and communication overhead of the control channel re-establishment process, since it requires only local coordination.

10. SECURITY IN WIRELESS ADHOC NETWORKS

In this type of network, security is not a single layer issue but a multilayered one. We have focused on network layer where the possible attacks are most vulnerable. Some of the attacks that we tried to address are Black hole, Gray hole, Wormhole, Jellyfish attack, Spoofing and Sybil attack. Due to the above mentioned network layer threats, the transmission of extremely sensitive information via one single path is not advisable as the information can easily be lost or hacked if the individual path is not fully trusted. To avoid this threat, sender may want to send multiple copies through multiple disjoint paths. But this increases the risk of information leakage. Shared cryptography tries to address this concern. Share is a copy of a original data in which some bits are present and some bits are missing. It transmits different shares of the information via multiple disjoint paths at different interval of times. It forces the shares received individually to co-operate for reconstructing the information at the receiving end. This not only reduces the risk of information leakage but also reduces the chance of several possible network level attacks.

11. ROUTING MECHANISM FOR WIRELESS AD-HOC NETWORKS

Wireless ad-hoc network consisting of nodes equipped with K (KP2) wireless network interfaces. The same number K of wireless channels out of more than or equal to K candidates is available for wireless communication. We assign wireless channels to interfaces with no overlap. Without loss of generality, we number channels and interfaces from 0 to K _ 1, while assigning the same number to the coupled channel and interface and numbering is the same among nodes. On the best-effort channel, the OLSRv2 with extension for our proposed mechanism operates for proactive physical routing and bandwidth information dissemination.

Since we focus on the infrastructure deployed in the region, we assume that the network is immobile and static. At least, the topology is stable and unchanged while a session is active. Nevertheless, condition of wireless communication can dynamically change by fading or some other environmental effects.
For example, assume that node 1 receives a real-time packet destined to neighboring node 2 with the destination IP address of 192.168.0.2. If node 1 selects the interface wlan1 to transmit the packet for its availability, the destination IP address in the packet is changed to 192.168.1.2 accordingly. Then the packet is sent from node 1 to node 2 on channel.
An example of wireless channel and IP address assignment.

IF	Ch.	IP addr– node 1	IP addr–node 2	IP addr–node 3
wlan0	1	192.168.0.1/24	192.168.0.2/24	192.168.0.3/24
wlan1	6	192.168.1.1/24	192.168.1.2/24	192.168.1.3/24
wlan2	1	192.168.2.1/24	192.168.2.2/24	192.168.2.3/24

When a packet arrives at a logical intermediate node, it is encapsulated with a new IP header indicating the next logical hop node. In this way, real-time packets traverse a logical path over a network maintained by a physical routing protocol, OLSRv2.

12. CONCLUSIONS

We examined that arise in an ad-hoc wireless network of mobile devices. When a packet is received, the data link layer of a node measures the bandwidth and delay for its link, along with channel busyness ratio. The receiver r sends this information along with the acknowledgement packet to the sending node n1, encapsulated by link and physical layer headers. This will give rise to many new applications and services. Where there are mobile nodes, forwarding of data to the correct recipient cannot be done without the use of a routing algorithm. We addressed the problem of control-channel jamming in multi-channel ad hoc networks, under node compromise. We proposed a randomized distributed channel establishment scheme that allows nodes to select a new control channel using frequency hopping. We implemented our proposal to the experimental system and confirmed that our proposal worked at an actual environment.

13. REFERENCES

[1] H.Balakrishnan, S.Seshan, E.Amir and R.Katz,"Improving TCP/IP performance over wireless networks" in Proc. of ACM MOBIHOC, Berkley, USA, 1995, pp. 2-11

[2] Z. Fu, P. Zerfos, H. Luo, S. Lu, L. Zhang, and M. Gerla, "The impact of multihop wireless channel on TCP throughput and loss'," in Proc. of IEEE
INFOCOM, San Francisco, USA, Apr. 2003, pp.1744--1753.

[3] K. Xu, M.Gerla, and S. Bae, "Effectiveness of RTS/CTS handshake in IEEE 802.11 based Ad Hoc networks," Ad Hoc Networks Journal, Elsevier, vol. 1, no. 1, Jul. 2003 , pp. 107–123.

[4] Kai Chen, Yuan Xue, Klara Nahrstedt, "On Setting TCP's Congestion Window Limit in Mobile Ad Hoc Networks" in Communications, 2003. ICC '03. IEEE International Conference on 11-15 May 2003 Volume: 2, pp.1080- 1084.

[5] Hongqiang zhai, Xiang chen and Yuguang fang ," Improving transport layer performance in multihop Ad Hoc networks by exploiting MAC layer information" in IEEE transaction on wireless communication, vol 6, no 5 ,may 2007,pp. 1692-1701.

[6]Barr R., Z.J. Haas and R.V. Renesse, "Scalable Wireless Ad hoc Network Simulation", in Handbook on Theoretical and Algorithmic Aspects of Sensor, Adhoc Wireless and Peer-to-Peer Networks, pp. 297-311, 2005.

[7] Macro Conti Stefano Basagni (2004) Mobile Ad hoc Networking. John Wiley and Sons inc.