International Journal of Current Engineering and Technology
©2016 INPRESSCO®, All Rights Reserved

E-ISSN 2277 – 4106, P-ISSN 2347 – 5161
Available at http://inpressco.com/category/ijcet

Research Article

Mobile and Ubiquitous Computing in Wireless Ad Hoc Networks

Kailash Aseri[†*] and Arun J B[‡]

[†]Faculty of Engineering & Technology, Jodhpur National University, Jodhpur (Rajasthan), India
[‡]Directorate of Technical Education, Jodhpur (Rajasthan), India

Accepted 21 Feb 2016, Available online 26 Feb 2016, **Vol.6, No.1 (Feb 2016)**

Abstract

Ad hoc and ubiquitous computing have established broad concentration with the hotheaded growth of wireless communication. These expertises are advantageous for many applications, such as offering innovative high bandwidth accessibility for users, and are expected to offer more stimulating and capable services. In order to satisfy these diverse applications, the design issues of various wireless networks such as ad hoc, sensor, and mesh networks are extremely complicated and there are a number of technique challenges that need to be explored, involving every layer of the OSI protocol stack. This paper mainly focuses with the analysis on mobile and ubiquitous computing in wireless ad hoc networks.

Keywords: *Ad hoc network, wireless communication, wireless networks, protocol*

Introduction

There are two major types of wireless ad hoc networks: Mobile Ad Hoc Networks (MANETs) and Smart Sensor Networks (SSNs). A MANET is an autonomous collection of mobile users that communicate over relatively bandwidth constrained wireless links. Since the nodes are mobile, the network topology may change rapidly and unpredictably over time. The network is decentralized, where all network activities including discovering the topology and delivering messages must be executed by the nodes, i.e., routing functionality will be incorporated into mobile nodes.

Significant applications of MANETs include establishing survivable, efficient, dynamic communication for emergency/rescue operations, disaster relief efforts, and military networks which cannot rely on centralized and organized connectivity. A smart sensor network consists of a number of sensors spread across a geographical area. Each sensor has wireless communication capability and sufficient intelligence for signal processing and networking. Some examples of smart sensor networks are the following: Military sensor networks to detect enemy movements, the presence of hazardous material. Environmental sensor networks to detect and monitor environmental changes. Wireless traffic sensor networks to monitor vehicle traffic on a highway or in a congested part of a city. Wireless surveillance sensor networks for providing security in a shopping mall, parking garage, or other facility.

An ad hoc mobile network is an autonomous sys-tem consisting of mobile hosts that do not rely on the presence of any fixed network infrastructure. Depending on the nodes' geographical positions, their transceiver coverage patterns, transmission power levels, and co-channel interference levels, a network can be formed and unformed on the fly. This ad hoc network topology changes as mobile hosts migrate, disappear (failure or depletion of battery capacity), or adjust their transmission and reception characteristics. The main characteristics of ad hoc networks are:

Bandwidth constraint and variable link capability: Wireless links have significantly lower capacity than wired links. Due to the effects of multiple accesses, multipath fading, noise, and signal interference, the capacity of a wireless link can be degraded over time and the effective throughput may be less than the radio's maximum transmission capacity.

Vibrant topology: Nodes are free to move about arbitrarily. In addition, radio propagation conditions change rapidly over time. Thus, the network topology may change randomly and rapidly over unpredictable times.

Power constrained nodes: Mobile nodes rely on batteries for proper operation. Since an ad hoc network consists of several nodes, depletion of batteries in these nodes will have a great influence on overall network performance. Therefore, one of the most important protocol design factors is related to device energy conservation.

Limited security: Mobile wireless networks are generally more vulnerable to security threats than wired networks. The increased possibility of

*Corresponding author: **Kailash Aseri** is a Research Scholar; **Dr. Arun J B** is working as Assistant Director eavesdropping, spoofing, and denial-of-service (DoS) attacks should be carefully considered when an ad hoc wire-less network system is designed.

Multi-hop communications: Due to signal propagation characteristics of wireless transceivers, ad hoc networks require the support of multichip communications; that is, mobile nodes that cannot reach the destination node directly will need to relay their messages through other nodes.

Review of Literatures

Ad hoc networks are new paradigm of networks offering unrestricted mobility without any underlying infrastructure. An ad hoc network is a collection of autonomous nodes or terminals that communicate with each other by forming a multihop radio network and maintaining connectivity in a decentralized manner. In the ad hoc networks, there is no fixed infrastructure such as base station or mobile switching. Since the nodes communicate over wireless links, they have to contend with the effects of radio communication, such as noise, fading, and interference. In addition, the links typically have less bandwidth than in a wired network. Each node in a wireless ad hoc network functions as both a host and a router, and the control of the network is distributed among the nodes. The network topology is in general dynamic, because the connectivity among the nodes may vary with time due to node departures, new node arrivals, and the possibility of having mobile nodes (Zheng Yan, 2001).

Compared to wired networks with static nodes, ad hoc networks require a highly adaptive rout-ing scheme to cope with the high rate of topology changes. This implies that the routing protocol should propagate topology changes and compute updated routes to the destination.

Table-driven
On-demand
Hybrid (Zheng Yan, 2001; Vesa Kärpijoki, 2000)

Table-driven protocols attempt to continuously update the routes within the network so that when a packet needs to be forwarded, the route is already known and can immediately be used. The families of distance-vector or link-state algorithms are examples of table-driven schemes. On the other hand, on-demand schemes invoke a route discovery procedure only on a need basis. Thus, when a route is needed, some sort of glob-al or localized search procedure is employed.

Secure routing analysis

Ad Hoc routing protocols can be divided into three classes (Vesa Kärpijoki, 2000). *Table-driven* or *proactive* protocols require the periodical refreshing or updating of the routing information so that every node can operate with consistent and up -to-date routing tables. The advantage of the proactive approach is that once a route is formed, its use is efficient. But the pure proactive protocols do not suite the ad-hoc networks due to the heavy routing information exchange. *Source-initiated on-demand driven* or *reactive* protocols, in contrary, do not periodically update the routing information - the data is propagated to the necessary nodes only when necessary.

Secure aware ad hoc routing (SAR)

Secure aware ad hoc routing (SAR) in [2] introduces security properties as a negotiable metric to discover secure routes in an ad hoc network. Quality of protection offered by the discovered route directly affects the security of data packets exchanged between the nodes on a particular route. Routing information, such as route updates and route propagation messages, is also protected using this way. The security properties, such as time stamp, sequence number, authentication password or certificate, integrity, confidentiality, non-repudiation, etc. have a cost and performance penalty associated with it, therefore effect the secure route discovery.

Power-Efficient Mechanism of Ad Hoc Routing

At the network layer, routing algorithms must select the best path to minimize the total power needed to route packets on the network and maximize the lifetime of all nodes. We shall present four variations of route selection schemes to achieve one or both of these goals.

Minimum Total Transmission Power Routing (MTPR)

In wireless communications, radio propagation can be modeled effectively with a $1/d^n$ transmit power roll off (usually, n = 2 for short distance and n = 4 for longer distance). For successful transmissions, the signal-to-noise ratio (SNR) received at a host n_j should be greater than a specified pre-detection threshold $\square_j$. This threshold $\square_j$ is closely related to the bit error rate (BER) of the received signal. For successful transmissions from a host n_i to n_j, the SNR at host n_j should satisfy the following equation:

$$SNR_j \,\square\, \frac{P_i G_{i,j}}{\sum_{k \neq i} P_K G_{k,j} \;\square\square\; \eta\, \square_j} \Psi_j (BER), \qquad (1)$$

Where P_i is the transmission power of host n_i, $G_{i,j}$ is the path gain between hosts n_i and n_j (i.e., $G_{i,j}1/d_i^n,_j$), and $\square_j$ is the thermal noise at host n_j. Therefore, the minimum transmission power is dependent on interference noise, distance between hosts, and desired BER. To obtain the route with the minimum total power, the trans-mission power $P(n_i, n_j)$ between hosts n_j and n_j can be used as a metric [6]. The total transmission power for route l, P_l, can be derived from $D-1$ $P_l \,\square \sum P$

$(n_i, n_n$ ⍰1 $)$ for all node n_i ,where n_0 and n_D are the source and destination nodes, respectively.

Conclusion

Due to the underlying wireless medium and the infrastructure-less nature, the communication between a pair of nodes is relatively unstable. Existing techniques compensate for the instability of wireless links by employing packet retransmissions, network coding, opportunistic routing, multiple paths, or route fixes.

References

Zheng Yan (2001), Security in Ad Hoc Networks

Vesa Kärpijoki (2000): Signalling and Routing Security in Mobile and Ad -hoc Networks, May, 2000,<http://www.tml.hut.fi/Opinnot/Tik -110.551/2000/papers/signalling_security/index.html >.

S. Singh and C. S. Raghavendra (July 1998.), PAMAS-Power Aware Multi-Access protocol with Signaling for Ad Hoc Net-works, ACM Commun. Rev.

C.-K. Toh, Georgia Institute of Technology, Maximum Battery Life Routing to Support Ubiquitous Mobile Computing in Wireless Ad Hoc Networks

V. D. Park and M. S. Corson (1997), A Highly Adaptive Dis-tributed Routing Algorithm for Mobile Wireless Net-works, IEEE INFOCOM '97, Kobe, Japan.

C. E. Perkins and E. M. Royer (Feb. 1999), Ad-Hoc On-Demand Dis-tance Vector Routing, Proc. 2nd IEEE Wksp. Mobile Comp. Sys. and Apps..