A Wireless Network with Direct Connection between the Devices using Ad-Hoc Network

Mamta Kumari
M. Tech. Student
Department of Computer Science
B.I.T.S BHIWANI

Mr. Vipin Arora
Lecturer
Department of Computer Science
B.I.T.S BHIWANI

Abstract

This paper outlines experience with the implementation and deployment of wireless network with direct connection between the devices using Ad-hoc network. The work was prompted by the lack of published results concerning the issues associated with the implementation of ad-hoc network on actual wireless networks, as opposed to results of simulation experiments. I examined implementations of adhoc network is defined as the wireless network with direct connection between the devices. The connection is here been established dynamically while defining a session. While performing the communication, the communicating device discovers the other communicating device in the range so that effective communication will be drawn over the system. The search mechanism is performed till the target node is not identified.

Keywords: Wireless network, Ad-hoc Network, Topology, VANET, Routing Protocols

I. INTRODUCTION

To enable the infrastructure free communication as well as long distance communication, the multihop comm-unication is provided by mobile network. The next hop selection is here done based on the best node election in neighboring nodes. It requires the destination selection while moving through the intermediate nodes so that effective communication will be performed while forwarding through the nodes.

The network is ad hoc because it does not rely on a preexisting infrastructure, such asrouters in wired networks or access points in managed (infrastructure) wireless networks. Instead, each node participates in routing by forwarding data for other nodes, so the determination of which nodes forward data is made dynamically on the basis of network connectivity. In addition to the classic routing, ad hoc networks can use flooding for forwarding data.

Wireless mobile ad hoc networks are self-configuring, dynamic networks in which nodes are free to move. This paper shows the history of the ad-hoc networks and its development and its applications based on its decentralized nature of networks and it shows how the routing is done by mentioning the routing algorithms and how each one works then we move to the advantages and disadvantages of the ad-hoc networks then we go across the protocol stack.Wireless networks eliminate the complexities of infrastructure setup and administration, enabling devices to create and join networks "on the fly"-anywhere, anytime, for virtually any application.

The paper discusses our experience while wireless network with direct connection between the devices using MA-NET routing protocol .We examined both a public domain implementation of the Ad Hoc On-Demand Distance Vector (AODV)routing protocol and implemented our own version of the Destination-Sequenced Distance Vector (DSDV) routing protocol. The choice of routing protocols was pragmatically based on what (little) was available at the time this work was carried out. The AODV implementation was the freely available MAD-HOC implementation. This implementation was based on an earlier draft of the AODV protocol and includes some MAD-HOC specific extensions. Where AODV is referred to in this paper we mean the MAD-HOC implementation unless otherwise stated. At the time our work was carried out this was the only public domain MANET rout-ing protocol implementation that had a license suitable for our use and that we could get to compile, run and work on our network.

II. TYPES OF AD-HOC NETWORKS

An adhoc network is defined as the wireless network with direct connection between the devices. The connection is here been established dynamically while defining a session. While performing the communication, the communicating device discovers the other communicating device in the range so that effective communication will be drawn over the system. The search mechanism is performed till the target node is not identified. To perform the search flooding over the neighboring nodes will be done. The communication will be used with the neighbor selection so that effective communication will be drawn. The connection will be performed over the multiple nodes. There are different kind of network exist based on the application areas as well as network scenarios and the configuration. These network types are listed in figure 1.

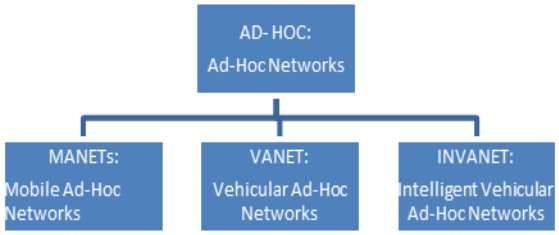


Fig. 1: Ad-hoc network type

A. Mobile Ad-Hoc Networks

A Mobile network is the infrastructure less network with mobile network that is configured automatically with the associated hosts and connected to the wireless devices in the form of arbitrary topology. These routers are free to move randomly over the network and can perform the communication in topology free network. The topology in such network change rapidly and on random basis or some times on the basis of the scenario used in the work. Here figure 1.1.1 is showing the dynamic topology network

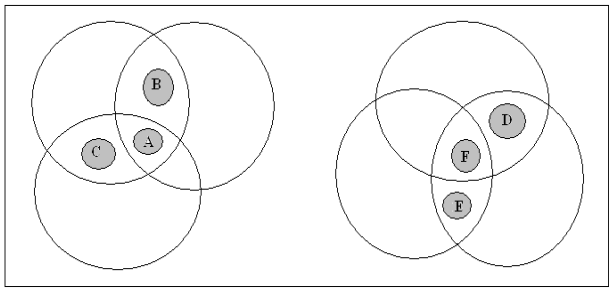


Fig. 1.1: Dynamic topology network

B. Vehicular Ad-Hoc Networks (Vanet)

VANET is the another advance form of mobile network in which the mobile devices are incorporated in the vehicles as well as in road side equipments. These kind of communication is performed on WLAM and provides the road safety along with collision free directional communication over the network. The network includes the warning analysis to avoid the collision. In the civil application scenarios, such kind of networks are commonly used. VANET is one of the promising type of network for civil applications under different scenarios. To perform the communication between the vehicles, the third party infrastructure, safety and conform of driving is required so that effective communication will be drawn. The system includes the driver assistance support system under the safety applications.

C. Intelligent Vehicular Ad-Hoc Networks (In-Vanet)

It is the improved form of vehicular network in which intelligent devices are connected to enable the communication among the vehicles. Here figure 1.3 is showing an intelligent vehicular adhoc network system. These kind of networks support different type of communication such as V2I, V2V etc. The road side access points are set as the control devices to control the communication over the network. This kind of network is expected to contribute to more efficient and safe communication so that information to driver can be conveyed in more effective way.

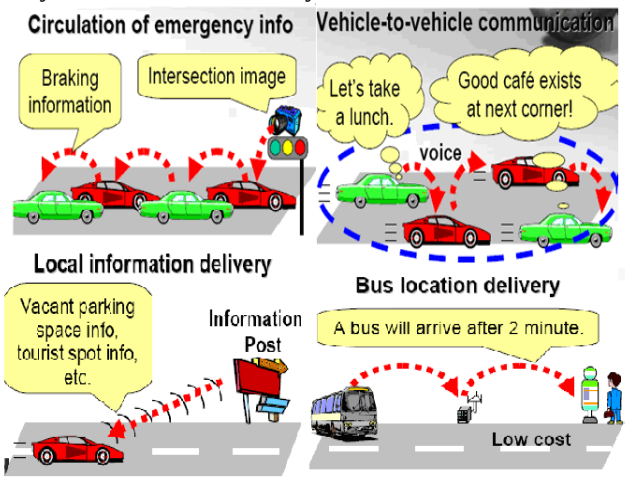


Fig. 1.3: Intelligent Transport Systems

III. AD-HOC NETWORKS MOBILE ROUTING PROTOCOLS

According to the type of communication performed over the ad-hoc network. There are different kind of protocol defined in the literature. These protocol types are difined under different aspects. The classification is here defined respective the formation of network and the communication performed over the network

Fig. 2: Ad-hoc network protocols

A. Table Driven Routing Protocol

Table Driven Routing Protocols, also known as Proactive Protocols, work out routes in the background independent of traffic demands. Each node uses routing information to store the location information of other nodes in the network and this information is then used to move data among different nodes in the network. This type of protocol is slow to converge and may be prone to routing loops. These protocols keep a constant overview of the network and this can be a disadvantage as they may react to change in the network topology even if no traffic is affected by the topology modification which could create unnecessary overhead. Even in a network with little data traffic, Table Driven Protocols will use limited resources such as power and link bandwidth therefore they might not be considered an effective routing solution for Ad-hoc Networks. Fisheye State Routing is an example of a Table Driven Protocol.

There are basically two kinds of table driven next-hop routing protocols:

1) Link-state algorithms:

Each node maintains a view of network topology, with a cost for each link. Link costs are broadcasted. Each node updates its topology and applies a shortest-path algorithm to find the next-hop for each destination.

-Short-lived routing loops (because some link states received from other nodes can be incorrect and this can cause a short-time loops)

- Complex
- Requires large storage and requires competition, periodically.
- Not suitable for ad-hoc networks.

2) Distance-Vector algorithms:

Each node maintains, for every destination, a set of distances to get that destination. The neighbor with the minimum distance is selected for that destination. Periodically broadcasts its routing table, containing the best next-hop for each destination, to each of its neighbors.

- Efficient, easier to implement and requires less storage according to Link-State algorithm.
- Originally produces short-lived and long-lived loops. But, modifications are proposed to handle this problem. One of them is internodal coordination, but is suitable for fixed networks. DSDV uses sequence numbers to handle this problem.

3) Destination Sequenced Distance Vector Algorithm(DSDV)

Each node keeps a routing table.

Simplified routing table structure for DSDV:

List of all accessible nodes	Hop-count	Sequence number (originated by the dest.)

- Each node advertises its routing table to all of its neighbors, periodically.
- Receiving nodes use the most recent sequence number among different update packets, if same sequence number appears, then it uses the data with the best-metric (small hop-count).
- One of the most important parameters is the time selected between update broadcasts.

- If a next-hop in the route of a node is broken, that link is identified by ∞, which is a specific case, and the update packet for the destination replacing that route is processed immediately and broadcasted among the network.
- It is possible to get an update broadcast, then another update with the same sequence number with a better metric. In this case, both the first, and then immediately after that, the second route update should be broadcasted to all neighbors of that node, and the received nodes updates their routing table and broadcasts to their own neighbors, so on. This scheme causes an update fluctuation through whole network, which consumes the network bandwith and processing power. So, this should be handled. To handle this problem, a node waits for a specific time, which is enough to receive the best-route update, then it broadcasts the best one, to its neighbors.
- It is not required and efficient to broadcast the whole routing table at each period. For this reason each node maintains two routing tables, full routing table, and the incremental table. Incremental table contains the most recent route modifications since the previous broadcast, and it is used for advertising route updates as long as the incremental table gets bigger. In that case, the full routing table is broadcasted instead.

B. On Demand Routing Protocol

On Demand Routing Protocols, also known as Reactive Protocols, establish routes between nodes only when they are required to route data packets. There is no updating of every possible route in the network instead it focuses on routes that are being used or being set up. When a route is required by a source node to a destination for which it does not have route information, it starts a route discovery process which goes from one node to the other until it arrives at the destination or a node in-between has a route to the destination. On Demand protocols are generally considered efficient when the route discovery is less frequent than the data transfer because the network traffic caused by the route discovery step is low compared to the total communication bandwidth. This makes On Demand Protocols more suited to large networks with light traffic and low mobility. An example of an On Demand Protocol is Dynamic Source Routing.

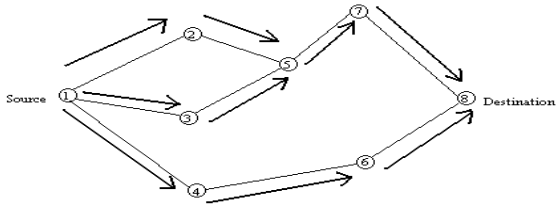
1) Cluster based Routing Protocols

In Cluster Based Routing protocol (CBRP) ,the nodes are divided into clusters. To form the cluster the following algorithm is used. When a node comes up, it enters the "undecided" state, starts a timer and broadcasts a Hello message. When a cluster-head gets this hello message it responds with a triggered hello message immediately. When the undecided node gets this message it sets its state to "member". If the undecided node times out, then it makes itself the cluster-head if it has bi-directional link to some neighbor otherwise it remains in undecided state and repeats the procedure again. Clusterheads are changed as infrequently as possible. Each node maintains a neighbor table. For each neighbor, the neighbor table of a node contains the status of the link (uni- or bi-directional) and the state of the neighbor (cluster-head or member). A cluster-head keeps information about the members of its cluster and also maintains a cluster adjacency table that contains information about the neighboring clusters. For each neighbor cluster, the table has entry that contains the gateway through which the cluster can be reached and the cluster-head of the cluster.

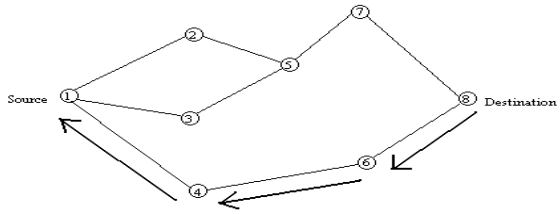
2) Ad hoc On-demand Distance Vector Routing

Ad hoc On-demand Distance Vector Routing (AODV) is an improvement on the DSDV algorithm discussed in section 2.1. AODV minimizes the number of broadcasts by creating routes on-demand as opposed to DSDV that maintains the list of all the routes.

To find a path to the destination, the source broadcasts a route request packet. The neighbors in turn broadcast the packet to their neighbors till it reaches an intermediate node that has a recent route information about the destination or till it reaches the destination (Figure 4a). A node discards a route request packet that it has already seen. The route request packet uses sequence numbers to ensure that the routes are loop free and to make sure that if the intermediate nodes reply to route requests, they reply with the latest information only.



(a) Propogation of Route Request (RREQ) Packet



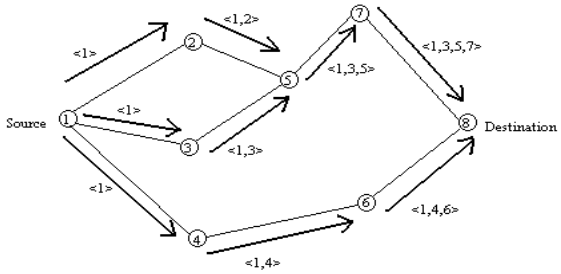
(b) Path taken by the Route Reply (RREP) Packet

Fig. 2.2.2.1: Route discovery in AODV

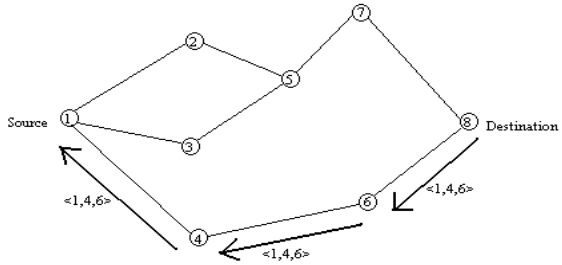
If the source moves then it can reinitiate route discovery to the destination. If one of the intermediate nodes move then the moved nodes neighbor realizes the link failure and sends a link failure notification to its upstream neighbors and so on till it reaches the source upon which the source can reinitiate route discovery if needed.

3) Dynamic Source Routing Protocol

The Dynamic Source Routing Protocol is a source-routed on-demand routing protocol. A node maintains route caches containing the source routes that it is aware of. The node updates entries in the route cache as and when it learns about new routes. A route reply is generated when either the destination or an intermediate node with current information about the destination receives the route request packet. A route request packet reaching such a node already contains, in its route record, the sequence of hops taken from the source to this node.



(a) Building Record Route during Route Discovery



(b) Propogation of Route Reply with the Route Record

Fig. Creation of record route in DSRP

4) Temporally Ordered Routing Algorithm

The Temporally Ordered Routing Algorithm (TORA) is a highly adaptive, efficient and scalable distributed routing algorithm based on the concept of link reversal .TORA is proposed for highly dynamic mobile, multihop wireless networks. It is a source-initiated on-demand routing protocol. It finds multiple routes from a source node to a destination node. The main feature of TORA is that the control messages are localized to a very small set of nodes near the occurrence of a topological change. To achieve this, the nodes maintain routing information about adjacent nodes. The protocol has three basic functions: Route creation, Route maintenance, and Route erasure.

Each node has a quintuple associated with it -

- Logical time of a link failure
- The unique ID of the node that defined the new reference level
- A reflection indicator bit
- A propagation ordering parameter
- The unique ID of the node

5) Associativity Based Routing

The Associativity Based Routing (ABR) protocol is a new approach for routing proposed in . ABR defines a new metric for routing known as the degree of association stability. It is free from loops, deadlock, and packet duplicates. In ABR, a route is selected based on associativity states of nodes. The routes thus selected are liked to be long-lived. All node generate periodic beacons to signify its existence. When a neighbor node receives a beacon, it updates its associativity tables. For every beacon received, a node increments its associativity tick with respect to the node from which it received the beacon. Association stability means connection stability of one node with respect to another node over time and space. A high value of associativity tick with respect to a node indicates a low state of node mobility, while a low value of associativity tick may indicate a high state of node mobility. Associativity ticks are reset when the neighbors of a node or the node itself move out of proximity. The fundamental objective of ABR is to find longer-lived routes for ad hoc mobile networks. The three phases of ABR are Route discovery, Route reconstruction (RRC) and Route deletion.

6) Signal Stability Routing

Signal Stability-Based Adaptive Routing protocol (SSR) presented in [Dube97]is an on-demand routing protocol that selects routes based on the signal strength between nodes and a node's location stability. This route selection criterion has the effect of choosing routes that have "stronger" connectivity. SSR comprises of two cooperative protocols: the Dynamic Routing Protocol (DRP) and the Static Routing Protocol (SRP).

The DRP maintains the Signal Stability Table (SST) and Routing Table (RT). The SST stores the signal strength of neighboring nodes obtained by periodic beacons from the link layer of each neighboring node. Signal strength is either recorded as a strong or weak channel. All transmissions are received by DRP and processed. After updating the appropriate table entries, the DRP passes the packet to the SRP.

C. Hybrid Routing Protocol

Hybrid Routing Protocols combine Table Based Routing Protocols with On Demand Routing Protocols. They use distance-vectors for more precise metrics to establish the best paths to destination networks, and report routing information only when there is a change in the topology of the network. Each node in the network has its own routing zone, the size of which is defined by a zone radius, which is defined by a metric such as the number of hops. Each node keeps a record of routing information for its own zone. Zone Routing Protocol (ZRP) is an example of a Hybrid routing protocol.

IV. SECURITY

Ad-hoc networks are highly vulnerable to security attacks and dealing with this is one of the main challenges of developers of these networks today. The main reasons for this difficulty are;

"Shared broadcast radio channel, insecure operating environment, lack of central authority, lack of association among nodes, limited availability of resources, and physical vulnerability."

Generally, when considering the security of a network, we examine it under the headings; availability, confidentiality, authentication, integrity and non-repudiation. Availability refers to the fact that the network must remain operational at all times despite denial of service attacks. Confidentiality ensures that certain information is never disclosed to certain users. Authentication is the ability of a node to identify the node with which it is communicating. Integrity guarantees that a message is never corrupted when transferred. Non-repudiation states that the sender of the message cannot deny having sent it. An ad-hoc network has extra security requirements caused by its lack of proper infrastructure and the dynamic relationship between the nodes in the network. Because of the lack of infrastructure, accountability is very difficult to determine as there is "no central authority which can be referenced when it comes to making trust decisions about other parties in the network."

The dynamic relationship between the nodes leaves very little opportunity for the nodes to form trust relationships with each other. In an ad-hoc network, nodes must act as both terminals and routers for other nodes. Because there are no dedicated nodes, a secure routing protocol is needed. Multi hop routing protocols are usually employed. These can lead to problems due to non-cooperating nodes and denial of service attacks.

A. Denial of Service Attacks

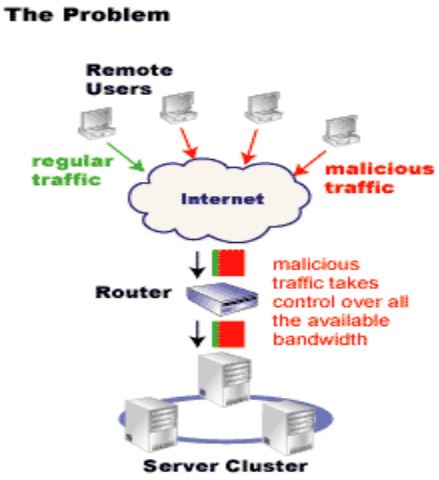


Fig. Denial of service attacks.

These problems are not easily solved and routing protocols for ad-hoc networks are still under active research.

Confidentiality is also a major issue in ad-hoc networks but it is one that can be solved more easily. Cryptography is one of the most common and reliable means to ensure confidentiality.

"It is the study of the principles, techniques, and algorithms by which information is transformed into a disguised version which no unauthorized person can read, but which can be recovered in its original form by an intended recipient."

Another issue to be considered is protecting the information that is actually stored on the device as the more portable the device, the easier it is to tamper with in general. We must also attempt to retain confidentiality of identity and location which will become more important in the ubiquitous computing environment. Ad-hoc networks require a high level of security, but because of the nature of these networks, this can often be difficult to provide. Therefore, it is an issue which requires a lot more research if these networks are to continue to thrive.

V. FUTURE OF AD-HOC NETWORK

Mobile ad hoc networks are the future of wireless networks. Why? Because they're practical, versatile, simple, easy to use and inexpensive! We will be living in a world where our network instantly updates and reconfigures itself to keep us connected anywhere we go.

These networks provide a new approach for wireless communication and by operating in a license free frequency band prove to be relatively inexpensive.

With the current trend of society's demand for information at out fingertips, we will see our future living environments requiring communication networks between the many devices we use in day to day living, allowing them to talk to each other.

For example devices like personal digital assistants and mobile phones being able to receive instant messages from a home device. Such as a refrigerator sending a message to a PDA to update its shopping list; notifying that it's run out of milk. Or washing machines and ovens sending a report to say the clothes are finished or the chicken's cooked.

Likewise, in education ad hoc networks may be deployed for student laptops interacting with the lecturer during classes. Also wireless public access for dense urban areas (Nokia RoofTopT): A wireless broadband solution for residential markets, based on a multi-hop Ad-Hoc (mesh) networking. *See diagram below*

Or similarly, ad hoc networks for cars, sending instant traffic reports and other information. Sensors and robots forming multimedia network that allows remote visualization and control, multiple airborne routers (from tiny robots to blimps) automatically providing connectivity and capacity where needed (e.g., at a football game); an ad hoc network of spacecrafts around and in transit between the Earth and Mars.

A. Nokia RoofTopT Wireless Routing

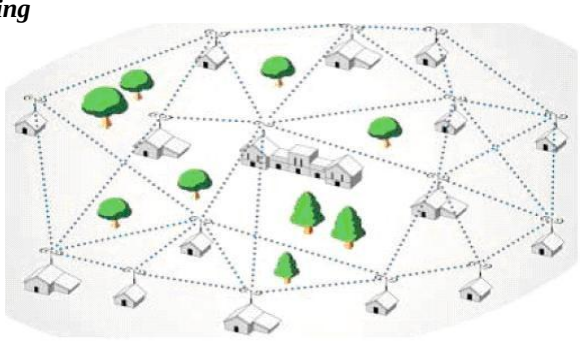


Fig. Nokia RoofTopT Wireless Routing

1) WAND

Closer to home, in Trinity College Dublin itself, the WAND venture, Wireless Ad hoc Network for Dublin, is underway. WAND, is a project that is currently in progress to aid research in the area of ad-hoc networks. The project is run by the Distributed Systems Group of Trinity College, in collaboration with Media Lab Europe.

WAND is arranged as a large scale test bed for ad-hoc networks protocols and applications, covering a 2km route from Trinity to Media Lab Europe. *See diagram below*

This route will be routed with custom-built wireless-enabled embedded PCs. Along this stretch, the embedded PCs will be placed in apartments, shops, on traffic lights and in phone booths providing a minimum level of connectivity.

The PCs form a sparse population of wireless network nodes. This sparse coverage is constantly available and the embedded PCs can be configured to create a variety of network models.

Other devices with wireless connectivity may also connect to the network via the implementation of mobile nodes.

2) 2km Route from Trinity to MLE

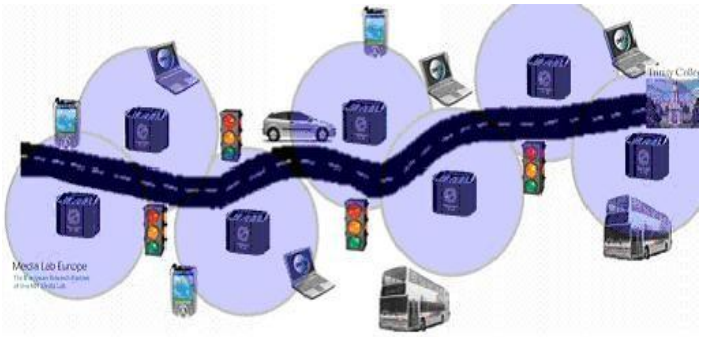


Fig. 4.2: 2km route from Trinity to MLE

Many factors lead us to believe that ad-hoc is the wireless network of the future. Due to the network not requiring any base station makes them indispensable in disaster relief situations or military war zones. Also energy issues have moved us from using a single long wireless link (as in cellular) to a mesh of short links (as in ad-hocnetworks).

To sum up, ad-hoc networks will be the future of our wireless networks.

VI. CONCLUSION

In this paper we have outlined our implementation and de-ployment experiences with MAD-HOC's AODV and DSDV. Our experiments have provided insights into the real world deployment of MANETs and highlight issues that require further investigation. These are:

After researching Ad-hoc networks in depth, we believe that they will be the future of wireless networking. It is true that performance suffers as the number of devices grows and large ad-hoc networks become difficult to route and manage. However, much time is being devoted to achieving routing stability, and a few technical issues need to be solved before they become common place. The area of ad hoc networks is a very fast growing area, and due to the vast research in them, we are seeing these problems disappear and they are coming into a world of their own.

REFERENCES

[1] R. K. Ahuja, T. L. Magnanti, and J. B. Orlin. Network Flows, theory, Algorithms, and Applications. Prentice-Hall, 1993.
[2] S. H. Bae, S.-J. Lee, and M. Gerla. Unicast performance analysis of the ODMRP in a mobile ad-hoc network testbed. In Proceedings of IEEE ICCCN'2000, Las Vegas, USA, 2000.
[3] P. Basu and T. D. C. Little. Task-based self-organisation in large smart spaces:issues and challenges. In DARPA/NIST/NSF Workshop on Research: Issues in Smart Computing Environment, Atlanta, USA, 1999.
[4] P. Bhagvat, C. Bisdjikian, P. Kermani, and Naghshineh. Smart connectivity for smart spaces. In DARPA/NIST/NSF Workshop on Research: Issues in Smart Computing Environment, Atlanta, USA, 1999.
[5] J. Broch, D. A. Maltz,. B. Johnson, Y.-C. Hu, and J.Jetcheva. A performance comparison of multi-hop wireless ad-hoc network routing protocols. In Proceedings of the 4th ACM/IEEE Internation Conference on Mobile Computing and Networking (MOBICOM'98), Dallas, Texas, Oct. 1998.
[6] M. S. Corson and V. Park. An internet MANET encapsulation protocol (IMEP) speci cation. Internet Draft: draft-ietf-manet-imep-spec-00.txt, Nov. 1997.
[7] S. R. Das, R. Castaneda, and J. Yan. Simulation based performance evaluation of mobile, ad hoc network routing protocols. In Proceedings of Seventh International Conference on Computer Communications and Networks (ICCCN'98), 1998.
[8] S. R. Das, C. Perkins, and E. M. Royer. Performance comparison of two on-demand routing protocols for ad-hoc networks. In Proceedings of IEEE INFOCOM'200, Tel-Aviv, Israel, 2000.
[9] R. Dube, C. D. Rais, K.-Y. Wang, and S. K. Tripathi. Signal stability based adaptive routing (SSA) for ad-hoc mobile networks. IEEE Personal Communications, 4(2):36{45, Feb. 1997.
[10] K. Fall and K. Varadhan. The VINT project. ns notes and documentation. http://www.isi.edu/nsnam/ns/.
[11] J. J. Garcia-Luna-Aceves, D. Beyer, and T. Frivold. Wireless internet gateways (WINGS). In Proceedings IEEE Milcom'97, Monterey, CA, 1997.
[12] M. Gerla, G. Pei, and S. J. Lee. Wireless, mobile ad-hoc routing. In IEEE/ACM FOCUS, New Brunswick, USA, May 1999.
[13] H. Hashemi. The indoor radio propagation channel. Proceedings of the IEEE, 81(7), July 1993.
[14] Lawrence Berkeley National Lab. Libpcap: User-level packet capture library. ftp://ftp.ee.lbl.gov/libpcap-0.4.tar.Z, Feb. 1997.
[15] F. Lilieblad, O. Mattsson, P. Nylund, D. Ouchterlony, and A. Roxenhag. MAD-HOC AODV Implementation. Telecommunications Systems Lab, Techical Report. http:// .ssvl.kth.se/.
[16] D. A. Maltz, J. Broch, J. Jetcheva, and D. B. Johnson. The e ects of on-demand behavior in routing protocols for multi-hop wireless ad-hoc networks. IEEE Journal on Selected Areas in Communications special issue on mobile and wireless networks, Aug. 1999.
[17] D. A. Maltz, J. Broch, and D. B. Johnson. Experiences designing and building a multi-hop wireless ad-hoc network testbed. Techical Report, CMU-CS-99-11, Mar. 1999.
[18] D. A. Maltz, J. Broch, and D. B. Johnson. Lessons from a full-scale multihop wireless ad hoc network testbed. IEEE Personal Communications, 8(1), Feb. 2001.
[19] Merit Network Inc. Multi-threaded routing toolkit. MRT Programmers Guide. http://www.merit.edu/mrt/mrt doc/.
[20] C. Perkins and P. Bhagvat. Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers. ACM Computer Communications Review, pages 234{244, Oct. 1994.
[21] C. E. Perkins, E. M. Royer, and S. R. Das. Ad hoc on-demand distance vector (AODV) routing. draft-ietf-manet-aodv-06.txt, July 2000.