International Journal of Enhanced Research in Management & Computer Applications, ISSN: 2319-7471
Vol. 3 Issue 2, February-2014, pp: (22-26), Impact Factor: 1.147, Available online at: www.erpublications.com

Implementation of IPV6 in Ad-Hoc Networks

Himanshu Saxena
Department of Electronics and Communication Engineering,
Jawaharlal Nehru Government Engineering College Sundernagar, (H.P.), India

Abstract: The paper presents issues concerning the construction of globally connected wireless networks based on the IPv6 protocol. Prospects of implementation of IPv6 in wireless networks and IPv6 features and mechanisms important in such applications are discussed. Concepts presented here apply to wireless ad hoc mesh networks. In ad hoc networks (MANETs), wireless nodes spontaneously collaborate to route packets among a multi-hop and versatile topology. While such networks have originally been considered as self-sufficient systems, it becomes clear that there is a growing interest in connecting them to the Internet. In such a hybrid ad-hoc network, one or more nodes act as gateways to the outside world. This situation requires the use of a global addressing scheme in order to allow end-to-end communications between MANET nodes and correspondents in the Internet.

Keywords: Mobile Ad hoc Networks, AODV, IPV6, MANET, Gateway.

I. INTRODUCTION

Ad-hoc networks are a new paradigm of wireless communication for mobile hosts where node mobility causes frequent changes in topology. Ad hoc networks are self- configurable and autonomous systems consisting of routers and hosts, which are able to support mobility and organize themselves arbitrarily [1].

This means that the topology of the ad hoc network changes dynamically and unpredictably. Moreover, the ad hoc network can be either constructed or destructed quickly and autonomously without any administrative server or infrastructure. Without support from the fixed infrastructure, it is undoubtedly necessary for people to distinguish the insider and outsider of the wireless network. That is to say, it is not easy for us to tell apart the legal and the illegal participants in wireless systems. Because of the above mentioned properties, the implementation of security infrastructure has become a critical challenge when we design a wireless network system [2].

A **wireless ad-hoc network** is a decentralized type of wireless network. The network is ad-hoc because it does not rely on a preexisting infrastructure, access points in managed wireless networks. Instead, each node participates in routing by forwarding data for other nodes, and so the determination of which nodes forward data is made dynamically based on the network connectivity.

Wireless ad-hoc networks can be further classified by their application:

- Mobile ad-hoc networks (MANET)
- Wireless mesh networks (WMN)
- Wireless Ad-hoc sensor networks (WASN)

A **mobile ad-hoc network** (**MANET**) is a self-configuring infrastructure less network of mobile devices connected by wireless. 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.

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. 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.

Ad-hoc Wireless Sensor Network (WSN) consists of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location.

Ad-hoc Network Routing Protocol: Being ad-hoc in nature, the Ad-hoc networks require special routing protocols. It is a 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 are not familiar with the topology of their networks. Instead, they have to discover it. The various routing protocols used in Ad-hoc networks are classified as follows:

Table-driven (Pro-active) routing: This protocol maintains a list of destination addresses for routing.

Reactive (on-demand) routing: This protocol finds a route on demand by flooding the network with Route Request packets.

Flow-oriented routing: This protocol finds a route on demand by following present flows and unicast consecutively when forwarding data for a new link.

Hybrid (both pro-active and reactive) routing: This protocol combines the advantages of proactive and of reactive routing. The routing is initially established with some proactively prospected routes and then serves the demand from additionally activated nodes through reactive flooding.

Hierarchical routing: This protocol, the choice of proactive and of reactive routing depends on the hierarchic level where a node resides.

If the nodes of Ad-Hoc networks are mobile and with wireless communication to maintain the connectivity, it is known as mobile ad hoc network (MANET) and require an extremely flexible technology for establishing communications in situations which demand a fully decentralized network without any fixed base stations, such as battlefields, military applications, and other emergency and disaster situations.

Although a stand-alone MANET is useful in many cases, a MANET connected to the Internet is much more desirable. As till now, most of the research concerning MANET has been done on protocols for autonomous mobile ad hoc networks. Thus, we require using those protocols of MANET along with basic internet protocols for the integration of mobile ad hoc networks and the Internet. Here, we want to integrate it with one of the highly efficient protocol being used for MANET. As per the discussions in [8] we have selected AODV (Ad Hoc On-Demand Distance Vector)[8].

In this paper the access to the Internet from a multi-hop wireless network is investigated. All communication between a mobile ad hoc network and the Internet must pass through the gateways. In the case for reactive routing protocols, the idea is to extend the route discovery messaging, so that it can be used for discovering not only mobile nodes but also gateways.

II. About IPV6

IPv4 addresses are 32 bits wide, which expands to a maximum of 4,294,967,296 unique addresses. IPv6 addresses are 128 bits wide, which expands to a maximum of 340,282,366,920,938,463,463,374,607,431,768,211,456 unique addresses, or 3.4×10^{38}. This is 4 times the number of bits or 79,228,162,514,264,337,593,543,950,336 times the number of IPv4 unique addresses. Given the Earth's population of around 7 billion people, this is 48,611,766,702,991,209,066,196,372,490 (4.8×10^{28}) addresses per person on the planet (see Table 4.1). Assuming the Earth's surface is 511,263,971,197,990 square meters, then this is 665,570,793,348,866,943,898,599 (6.6×10^{23}) addresses per square meter of the Earth's surface.

IPv6 addresses are represented as 8 fields of hexadecimal numbers (0–F), each field representing 16 bits using 4 hexadecimal digits and fields are separated by a colon ':' .

For example, 2001:0000:1234:0000:0000:C1C0: ABCD: 0876 is a valid address.
The following rules can be applied to address representations:

(a) Letters are case-insensitive. For example, 'AB09' equals 'ab09'.
(b) Leading zeros in a field are optional. For example, '00c1' equals 'c1'.
(c) Successive fields of '0' are represented as '::', but only once in an address.

There are three kinds of addresses that exist in IPv6: unicast, multicast and anycast.
Unicast addresses are used for communications between two nodes. A unicast address is a one-to-one address.
Multicast addresses are used for communications between one node and many nodes and
Anycast addresses are used for communications between one node and the nearest node among a group of nodes.

Multicast addresses start with 'ff' as the leftmost octet. Any other value of the leftmost octet ('00' to 'fe') identifies a unicast address. Anycast addresses are formed using the unicast address space, so they cannot be distinguished from unicast addresses.

III. Advantages of IPV6 over IPV4

As the global Internet is only supported by two protocols: IPV4 and IPV6 [5]. IPV6 protocol is pro-developmental in terms of ease of creating new technical solutions and new-quality applications. It is possible to increase the globalization of remote data collecting and control, in relation to the massive amount of terminal equipment.

- This also applies to the access to devices operating in wireless networks, the IPv6 features important for the provisioning of services in wireless networks, are:
- The size of the address space, important for operators servicing millions of subscribers.
- Powerful mobility, which allows nodes to move between subnets without breaking the existing session. Mobile IPv6 is more efficient than Mobile IPv4. With Mobile IPv6 a number of enhancements is related, such as hierarchical management of nodes mobility, subnet mobility within the Internet, rapid transfer of nodes between access routers.
- Auto-configuration features are enhanced (detection of neighbors and routers, announcing the network prefix).
- The use of header compression potentially makes IPv6 more efficient than IPv4 – which is particularly important in sensor networks.

IPv6 also offers higher level of security compared to IPv4 as a mandatory implementation of IPsec provides more options for securing networks and applications without the constraints imposed by NAT servers; there is defined a proposal of a standard for securing, with IPsec and IKEv21, the signaling between mobile nodes and home agents. It is possible to use the Secure Neighbor Discovery Protocol, which improves the safety of nodes auto-configuration which is particularly important in the radio interfaces. SEND protocol increases the security of neighbor discovery process. It's most important mechanisms are certification paths for routers authentication, and cryptographically generated addresses to verify the sender.

IV. AODV (Ad Hoc On-Demand Distance Vector) Protocol

The Ad Hoc On-Demand Distance Vector (AODV) Routing Protocol [6] provides on-demand route discovery in mobile ad hoc networks. Like most reactive routing protocols, route finding is based on a route discovery cycle involving a broadcast network search and a unicast reply containing discovered paths. AODV relies on per-node sequence numbers for loop freedom and for ensuring selection of the most recent routing path. AODV nodes maintain a route table in which next-hop routing information for destination nodes is stored. Each routing table entry has an associated lifetime value. If a route is not utilized within the lifetime period, the route is expired. Otherwise, each time the route is used, the lifetime period is updated so that the route is not prematurely deleted. When a source node has data packets to send to some destination, it first checks its route table to determine whether it already has a route to the destination. If such a route exists, it can use that route for data packet transmissions. Otherwise, it must initiate a route discovery procedure to find a route.
Each route entry keeps track of certain fields.

Some of these fields are:

- Destination IP Address: The IP address of the destination for which a route is supplied.
- Destination Sequence Number: The destination sequence number associated to the route.
- Next Hop: Either the destination itself or an intermediate node designated to forward packets to the destination.
- Hop Count: The number of hops from the Originator IP Address to the Destination IP Address.
- Lifetime: The time in milliseconds for which nodes receiving the RREP consider the route to be valid.
- Routing Flags: The state of the route; up (valid), down (not valid) or in repair.

Whenever a source node desires a route to a destination node for which it does not already have a route, it broadcasts a route request (RREQ) message to all its neighbors. The neighbors update their information for the source and create reverse route entries for the source node in their routing tables. A neighbor receiving a RREQ may send a route reply (RREP) if it is either the destination or if it has an unexpired route to the destination. If any of these two cases is satisfied, the neighbor unicasts a RREP back to the source. Along the path back to the source, intermediate nodes that receive the RREP create

forward route entries for the destination node in their routing tables. If none of the two cases mentioned is satisfied, the neighbor rebroadcasts the RREQ [7].

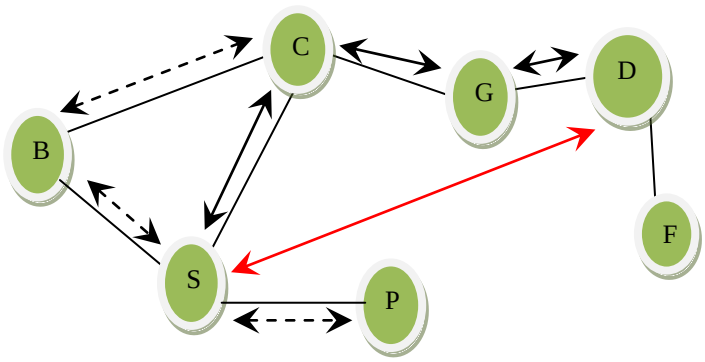

Fig. 1: Reactive AODV Routing Protocol.

The above figure represents a schematic diagram of an AODV protocol. If we have to transfer data from source node S to destination node D the source tries to establish the smallest and the most efficient route for this purpose. This route is decided by a vector table, this table represents the various information on the address of the source and destination along with the destination sequence number, lifetime etc. If the lifetime of a route has been expired or a new node has been introduced in the Ad-hoc network, the source node sends a RREQ message to all its neighboring nodes, here the neighboring nodes are node B, node C and node P. Here the nodes B and C forwards this message to their neighboring nodes C and G respectively, the node P has no other neighboring node hence the message expires at this node. The message reached at node G is then sent to node D and this node then sends a RREP message back through the same route. The RREQ message is not forwarded to node F as the destination has already been reached and RREP message is sent to the node S.

V. Combining IPV6 and AODV Protocols

The 128 bit IPV6 address is divided into three parts as shown in figure 2, the first part is the 48 bit prefix provided by ISP, the second part is 16 bit site subnets and the third part is the interface identifier also described as the unique MAC address of the device. The vast space of independent addresses of IPV6 allows us to easily counter the problem of data transfer from a node of one Ad-hoc network to the node of another Ad-hoc network, as there is less or rather no problem of repetition of IPV6 addresses. The access of an AODV node to the internet is given by selecting a master node or a gateway in the network and using it to communicate with the other global gateways.

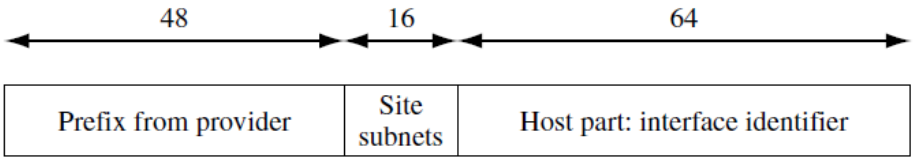

Fig. 2: Structure of IPV6 address.

As we know that the web servers or file servers can merely be considered as nodes connected at a fairly large distance and this node is also identified by its unique IPV6 address. Now the problem lies in connecting a reactive Ad hoc network to the internet in such a way that any remote nodes present is able to connect to the global IPV6 address of the server. Here we have to make one node of this MANET to be the master node i.e. the node which is connected to internet through global IPV6 configuration, other remaining nodes that can be referred to as slave nodes are a part of an anonymous Ad hoc network with independent addresses that can only be identified by the other nodes connected to this network. Now if we have a node D (figure 3) that has to communicate with a global server G1 then it requires such a method to request the master server to fetch the information from the global server G1 and send it to node D. This master server is often referred to as gateway. This routing request is referred to as Extended RREQ and RREP, and is similar to RREQ and RREP use in

AODV. The only difference is that it includes I-flag (Internet Global Address Resolution flag). This I-flag helps in the identification of the gateway.

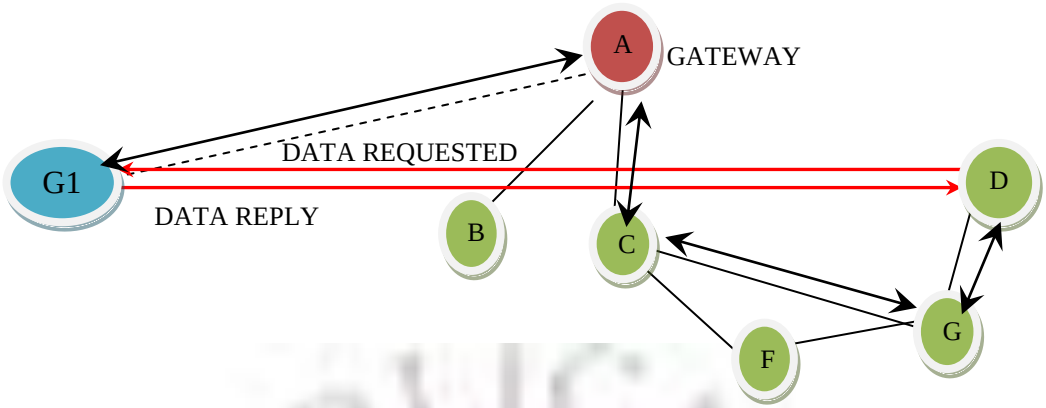

Fig. 3: MANET node D requesting and receiving data from global node G1 through gateway.

VI. Conclusion

In this paper it can be seen that however efficient an Ad hoc network be on its own, it can be used to communicate with any node on any other Ad hoc network through the use of IPV6. IPV6 is the most advantageous protocol for global internet and AODV being an efficient technique for an anonymous Ad hoc network can be combined to form such a network so that the connectivity of the nodes are enhanced.

The essential features of IPv6 and its extensions in support of the construction and operation of wireless networks are mechanisms for mobility, auto-configuration and security. Although theoretical work on the operation of ad hoc mesh networks is being carried for several years, their widespread use is limited.

References

[1]. Charles E. Perkins, "Ad-hoc networking".
[2]. Nadia Qasim, Fatin Said, and Hamid Aghvami, "PerformanceEvaluation of Mobile Ad Hoc Networking Protocols", World Congress on Engineering, 2008, pp. 219- 229.
[3]. Thomas S. Messerges, ohnas Cukier, Tom A.M. Kevenaar, Larry Puhl, Rene truik, Ed Callaway, "A Security Design for a General Purpose, Self-Organizing, Multihop Ad Hoc Wireless Network" 1st ACM Workshop Security of Ad Hoc and Sensor Networks Fairfax, Virginia 2003.
[4]. R. Shiva Kumaran, Rama Shankar Yadav, Karan Singh, " Multihop wireless LAN " HIT haldia March 2007.
[5]. S. Hagen, IPv6 Essentials. O'Reilly, 2006.
[6]. Perkins, C. and Royer, E. Multicast Ad Hoc On-Demand Distance Vector Routing (MAODV). IETF draft, 11 July 2000.
[7]. Hong X.; Xu K.; Gerla M. Scalable Routing Protocols for Mobile Ad Hoc Networks, IEEE Network, July/August 2002.
[8]. Himanshu Saxena and Reepika Sharma, A Review on Ad-Hoc Networks and its Security, ICAICTE Proceedings, November 2013.