Feasibility of IP address and Suffix for Multi-hop Wireless Mesh Network

S V Vambase
Research Scholar,
Dept. of Computer Science
VTU Jnana Sangama , Belagavi,
Karnataka, INDIA
santosh.vambase@gmail.com

S R Mangalwede
Professor,
Dept. of Computer Science and Engineering,
Gogte Institute of Technology,
Belagavi, Karnataka, INDIA
srmangalwede@gmail.com

***Abstract*—The deployment of DGs in distribution grid of electrical network can be made to enhance the availability of electricity. To distribute the energy over network, communication between various components is must. This paper extends the previous work carried out by authors. In this article, the authors focus on the network layer and propose a novel approach- Varying IP address for multi-hop Wireless Mesh Network (WMN). In IPv6 most of the addresses remain unassigned. The proposed addressing scheme ensures the considerable reduction in Packet header by reducing address length. The authors also focus on adapting proposed approach for existing network topologies. This article also briefs the suitability of existing routing protocols for proposed addressing scheme. The authors shrink IPv6 address by 16 bytes and suggest an extension header hence conclude with the analysis.**

Keywords—DGs, Varying IP address, MAC address, Multihop mesh network, OSG

I. INTRODUCTION

The IPv4 and IPv6 are designed to carry user data up to 65535 octets. The length of packet header in IPv4 varies from 20 octets to 60 octets and in IPv6, the packet length is 40 bytes excluding the extension headers. Presently, the Internet of Things (IoT) with limited computing capability is used to produce significant data over the network. The authors focus on aggregation of IoT and Distributed Generation Systems (DGs) [1] to form multi-hop WMN for DGs. The length of payload structure [2] for DGs is 16 bytes. However, it can vary as needed. The authors also focus on IPv6 protocol header to propose a novel protocol header that reduces the source and destination address by 8 bytes each respectively. The proposed protocol is adaptable to existing topologies by inducing minimal modification. It also defines a new extension header.

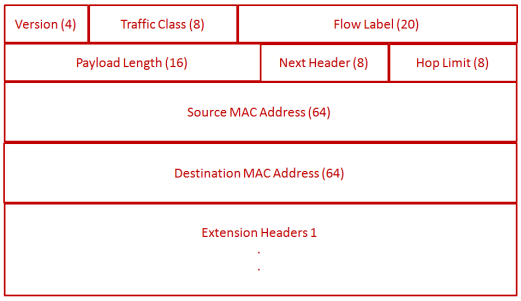

Figure 1. The proposed packet header.

The source MAC address [4] and destination MAC address [4] are mapped with GPS coordinates consisting of 4 byte latitude and 4 byte longitude. The fig. 1 depicts the structure of proposed IP packet header. The fields namely, Version, Traffic Class, Flow Label, Payload Length, Next Header and Hop Limit are similar to the fields defined in IPv6 packet header. Moreover, the logical address of source and destination assigned through Location Information Server instead of respective IP address for routing.

Furthermore, the article elaborates various aspects of proposed protocol in separate sections. The section II discusses the limitations of IPv6 addressing. Section III discusses the extension header of proposed protocol. Section IV describes the routing mechanism and network discovery. The section V elaborates benefits of proposed approach over IPv4. Finally, section VI concludes the work.

II. ADDRESS PREFIX IN IPV6

The IPv6 address space enables 2^{128} addresses that can be allocated to nodes and set interfaces. However, IPv6 addresses with certain prefix remain unused. It is analyzed that nearly 72% of the IPv6 addresses are unassigned. The Table 1 lists the various IPv6 prefixes allocations and fraction of total address space that are unused.

Table 1. Allocation of Prefixes in IPv6.

Prefix	**Fraction of IPv6 Address space**
0000 0001	1/256
0000 011, 1111 110	1/128 each
0000 1, 1111 0	1/32 each
0001, 1110	1/16 each
010, 011, 101, 110	1/8 each
1111 10	1/64
1111 1110 0	1/512

(Source: oracle documentation)

In reality, the proposed approach considers the address scalability and the address space needed for multi-hop WMN in the context of DGs deployment on electrical network [1-3]. This article excludes the unused address space thereby minimizing traffic overhead.

III. PROPOSED ADDRESSING SCHEME AND EXTENSION HEADER

The proposed address format is 64 bits long. Like IPv6, the proposed address acts as an identifier for single node under unique GPS location. However, the set of nodes can be

distinguished by Destination Options in proposed packet header. Unlike in IPv4, the address in proposed format can be assigned to interfaces, rather than hosts and routers. The address refers to a single node and hence a node on proposed network can be identified by any unicast address on the network. A single address can be assigned multiple interfaces. The proposed address format consists of different types: unicast, anycast, and multicast. In proposed addressing scheme the multicast address replace broadcast address.

The proposed scheme provides sufficient addresses such that atleast one node can be placed in 1 sq. mt. of area. The number of nodes per unit area depends on the density of GPS coordinates per unit area. Moreover, the extension header enables multiple nodes to have same address but different *Suffix*. The nodes with same IP address can be identified uniquely using *Suffix Address*. In the proposed addressing scheme, the node can be identified either by address or by combining address with interface. Hence, the length of node identifier increases with increase in number of nodes per unit geographical coordinates (IP address). If needed, the density of nodes for a given IP address can be increased up to 65536. The extension header - Destination Options provides the details of node density. Practically, the assignment of hierarchical address involves the accessibility to Location Information Server (LIS). The proposed addressing scheme provides enough address space for the multi-hop WMN. The fig. 2 depicts the details of address in proposed approach.

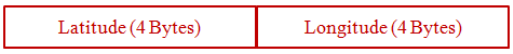

Figure 2. Format of proposed Physical (MAC) Address [4].

In IPv4, the router processes the various options in the packet header and in IPv6, the "options" are placed in extension header(s). The proposed protocol adopts the feature of extension header, and places the proposed extension header in the later part of proposed packet header. The length of proposed extension header is not constant and may vary as per the user needs. However, the total number of "options" in a packet is 40 bytes or more. The proposed extension header in a packet will be processed when it reaches to destination node. This strategy enhances the throughput of router. The proposed protocol integrates all features of IPv6 such as authentication and security encapsulation along with reduction in address length. The part of packet overhead that includes only extension header and upper layer protocol is in the integer multiple of 8 octets. This alignment enhances performance when handling subsequent extension headers. The authors review various extension headers currently defined in IPv6 and propose a new extension header for Destination Options.

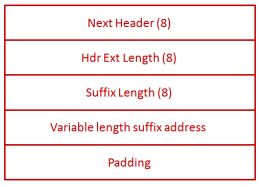

Figure 3. The extension header for proposed addressing scheme.

The fig. 3 depicts the proposed extension header: Destination Options suitable for proposed packet header. The two fields *Next Header* and *Header Extension Length* are similar to those in IPv6. The 8 bit *Suffix Length* defines the total number of hosts/interfaces connected in given unit area. Although, *Suffix Length* is 8 bits, it can be extended further to fulfill the necessity. The variable length *Suffix Address* is the absolute identifier used to identify a node/interface on network.

Like DNS server, an application server is needed to assign *Suffix Address* to the node/interface. The node/interface when accesses the LIS, the LIS makes an record entry in application server. The record comprises of two fields: the IP address and MAC address of node/interface. The LIS also ensures that, for a given pair of GPS coordinates, the first node receives only IP address in proposed format. However, the subsequent nodes receive IP address and respective *Suffix Address*.

IV. Routing Mechanism and Neighbor Discovery

Routing in proposed protocol is almost similar to IPv6 and IPv4 routing under CIDR. The extension headers defined in IPv6 are suitable for proposed packet header and hence the existing routing protocols can be used in proposed multi-hop Wireless Mesh Network.

The proposed protocol ensures the reliable communication by resolving various issues. The services in proposed protocol to solve each of the issues are as below:

Router discovery – Locating available routers on the proposed network.

Suffix Address– It is an optional part of logical address. It can be used to identify the unique node in set of nodes under given GPS coordinate.

Network Parameter – A node on network can determine the link parameters and Internet parameters for effective communication between nodes..

Address configuration – Nodes can request LIS (Location Information Server) to get address and configure automatically.

Address resolution – The address of a node comprises of the proposed logical address (64-bit) and optional *Suffix Address*.

Computing Next-hop – The routing algorithm performs routing table lookup and finds the next node (router/destination) that is nearest to destination.

Node unreachable – Each node can determine that a neighbor is out of reach. If the neighbor is router, an attempt to alternate default router can be made. Later, the address resolution can be performed again for both routers and hosts.

Duplicate address –The LIS performs mapping on allocated address and node's physical address. It then ensures the unique address allocation to a node.

Redirect – A router/intermediate node performs the look up on routing table and informs the next node so as to reach a particular destination. This can be achieved based on *Suffix Address*.

Table 2. Type and purpose of ICMP messages.

Type	Purpose
Router solicitation	Host can send router solicitation when the interface is enabled. It causes router to advertise immediately.
Router advertisement	It contains suffix used for determination of node or auto-configuration of node, TTL and so on.
Neighbor collection	To verify neighbor connectivity. Used for duplicate address detection.
Neighbor advertisement	Announcement of change in hardware address.
Redirect	It informs host to choose better path for a destination on-link.

The neighbor discovery can be performed using Internet Control Message Protocol (ICMP). The different ICMP packets and respective purpose are listed in Table 2.

V. Comparison With IPv4

In the proposed protocol, the neighbor discovery protocol comprises of three operations defined in IPv4 namely: ARP, ICMP Router Discovery, and ICMP Redirect. The neighbor discovery protocol detects the dead gateway thereby avoiding the requirement of possible algorithm at each host. It also provides all the improvements bundled in IPv6 over the set of IPv4 protocols.

The base protocol includes Router discovery and the Router advertisement contain MAC addresses. It also resolves the router's MAC address. Configuring the subnet mask is not required because the IP addresses are allocated in geographical hierarchy. Routers can advertise an MTU for nodes. The nodes in proposed network are synchronized to use the same MTU. Multiple suffixes can be allocated under same geographical location. Each host acquires the available neighbor's suffix.

Unlike IPv4, the recipient's redirect message in proposed protocol presumes that the new node is connected for packet relay. In IPv4 protocol, based on network mask, if the next-hop is not connected on network, the host ignores redirect messages causing loss of packet. The process of Redirect in proposed protocol is similar to the XRedirect facility and is suitable for unicast and multicast.

The proposed protocol also focuses on detection of node un-reachability, to provide improvements in network efficiency. A node can change its MAC address if and only if it is relocated. The proposed neighbor discovery protocol detects partial link failures and propagates the traffic to nodes with complete connectivity. The advertisement packets sent by router does not define any preference.

The hosts in proposed network preserve the router association based on hardware address for identifying routers uniquely on the network. This feature is needed for advertisement of routers and to airt the messages. In IPv4 network, the off-link nodes can transmit Internet Control Message Protocol (ICMP) and messages of router advertisement. In proposed protocol, the process of neighbor discovery can be protected from attack (off-link nodes) by possessing maximum hop limit of 255. Further, the security mechanism can be used in address resolution at ICMP layer.

In the proposed protocol, the host does not maintain the sequence of addresses and hence does not need general function. The packet containing sequence of addresses is formed. It is then secured and by appropriate mechanism and delivered to respective node. This strategy ensures nodes to trace the routes.

VI. Conclusion

In this article, the authors highlight the significance of IP address based on GPS coordinates and suitability of existing routing protocols for the proposed multi-hop WMN. The proposed addressing scheme also incorporates the various features of IPv6 and hence advantages over IPv4.

Unlike IPv6, the proposed address length is 64 bit, the number of nodes is not limited to 2^{64}. However, the number of nodes on network can be increased by assigning *Suffix* to each IP address. The length of *Suffix* can be varied as per the requirement.

The proposed model ensures the total number of nodes accommodated per unit area is between 1 to 2^n where n is number of bits representing Suffix Address.

The proposed protocol can be simulated using the NS3 simulator.

References

[1] S V Vambase, S R Mangalwede, "A novel cross layer wireless mesh network protocol for distributed generation in electrical networks", IEEE, ISBN: 978-1-4799-6629-5, 2014, Pg: 885-888.

[2] S V Vambase, S R Mangalwede, "ATM based WMN architecture for Distributed Generation systems in electrical networks", IEEE, ISBN: 978-1-4673-7910-6, 2016, Pg:119-123.

[3] S V Vambase, S R Mangalwede, "WMN Routing Scheme to Reduce the Traffic Overhead based on GPS-Addressing", GRENZE, ISBN: 978-81-931119-9-4, 2017, Pg: 401-405.

[4] S V Vambase, S R Mangalwede, "IP Reuse on GPS Mapped MAC for Multi-hop Mesh Network", IEEE, 2018.

[5] Rajkumar C. Shikkeri, P. S. Khanagoudar and G. M. Patil, "I-WMN: Intelligent System for Wireless Mesh Networks", ERCICA, ISBN: 978-93-510710-2-0, 2013, Pg: 332-337.

[6] Raja Kumar Murugesan, Sureswaran Ramadass, "IPv6 address distribution: An alternative approach" IEEE, 2010, Pg: 252 – 257.

[7] J. Gnana Jayanthi, S. Albert Rabara, "IPv6 Addressing Architecture in IPv4 Network", IEEE, 2010, Pg: 461 – 465.

[8] Raja Kumar Murugesan, Rahmat Budiarto ; Sureswaran Ramadass, "Performance Improvement of IPv6 Packet Transmission through Address Resolution using Direct Mapping", IEEE, 2008, Pg: 164 – 169.

[9] Bahaa Araji, Deniz Gurkan, "Embedding Switch Number, Port Number, and MAC Address (ESPM) within the IPv6Address", IEEE, 2014, Pg: 69 - 70J.

[10] Gnana Jayanthi, S. Albert Rabara' "IPv4 addressing architecture in IPv6 network", IEEE, 2010, Pg: 282 – 287.

[11] Raja Kumar Murugesan, Sureswaran Ramadass, "The Country Internet Registry (CIR) model: An alternative approach for the allocation and distribution of IPv6 Addresses", IEEE, 2009, Pg: 216 – 220.

[12] Supriyanto Praptodiyono ; Raja Kumar Murugesan, et. al. "Security mechanism for IPv6 stateless address autoconfiguration", IEEE, 2015, Pg: 31 – 36.

[13] Zhan Jun, Yang Bo, Men Aidong, "Address allocation scheme of wireless sensor networks based on IPv6", IEEE, 2009, Pg.597 – 601.

[14] Justin P. Rohrer, Blake LaFever, et.al., "Empirical Study of Router IPv6 Interface Address Distributions", IEEE, 2016, Pg: 36 - 45.

[15] Yong Cui ; Qi Sun ; Ke Xu ; et. al., “Configuring IPv4 over IPv6 Networks: Transitioning with DHCP”, IEEE, 2014, Pg: 84-88.
[16] J.-H Lee, “Cross-layered IPv6 neighbor discovery scheme over WLAN mesh networks”, IEEE, 2009, Vol: 13 , Issue: 12, Pg: 992-994.
[17] Arturo Azcorra ; Michal Kryczka ; Alberto Garcia-Martinez, “Integrated routing and addressing for improved IPv4 and IPv6 coexistence”, IEEE , 2010 , Vol: 14 , Issue: 5, Pg: 477 – 479.
[18] Samad S. Kolahi ; Peng Li, “Evaluating IPv6 in Peer-to-Peer 802.11n Wireless LANs”, IEEE, 2011, Vol: 15 , Issue: 4, Page s: 70 - 74.