AN OVERVIEW OF AUTO-CONFIGURATION PROTOCOLS IN MOBILE AD HOC WIRELESS MULTI-HOP NETWORK

Adel R. Alharbi

Computer Engineering Department, University of Tabuk, Saudi Arabia

ABSTRACT

An ad hoc wireless IP multi-hop network is a collection of wireless IP protocol capable nodes that start in an unknown physical formation in the vicinity of a wireless IP portal to a wired IP network. While some wireless nodes might be in radio (wireless) range of the portal, other nodes might only be in radio range of one or more other nodes that in turn may in range of the portal and/or other wireless nodes. IP data-grams would travel from one node to another until the data-gram is delivered to the portal or the destination node. All wireless nodes are assumed to be one or more hop away from the wireless IP portal. This paper reviews an auto-configure method of a mobile ad hoc network and to route IP traffic using existing mobile ad hoc network routing protocols. This method have the best characteristics in protocol overhead, robustness, convergence time, and scalability. The optimal mobile ad hoc network routing protocol can be chosen which best meets these characteristics for the given topology and operational profile. Finally, this method will efficiently use the address space allotted to the DHCP server.

KEYWORDS

Wireless LAN, communication systems routing, mobile communications, auto-configuration protocols, MANET.

1. INTRODUCTION

A Mobile Ad Hoc Network (MANET) is a collection of mobile nodes that interact through wireless connections between themselves. Unlike standard networks, no existing infrastructure is needed by a MANET, as nodes depend on each other to function themselves, forming what is called multi-hop communication [1].

Conventional wireless networks, such as 802.11, are not used in a multi-hop environments such as a MANET [2]. Mobile network topology can alter rapidly and unpredictably. There may be differences in node and link capability, frequent transmission failures, and lack of security [3]. Due to the fact that an ad hoc network is usually created by battery-operated mobile, the restricted resources of the nodes must be taken into consideration. In addition, the multi-hop environment of a MANET makes traditional IP address auto-configuration infeasible [4]. While there have been many proposed solutions, there are still questions of merging two or more MANETs, or partitioning a MANET into two or more MANETs [5]. How will the IP addresses be divided to allow efficient routing of IP messages?

The ad hoc nodes need to configure their interfaces with local addresses that are valid within the ad hoc network to communicate directly with each other. In addition, ad hoc nodes may need to

Natarajan Meghanathan et al. (Eds) : ICCSEA, WiMoA, SCAI, SPPR, InWeS, NECO - 2019
pp. 47-55, 2019. © CS & IT-CSCP 2019 DOI: 10.5121/csit.2019.91804

set worldwide routing addresses to connect on the Internet with other mobiles. An ad hoc network provides itself from the IP layer angle as a multi-hop level 3 (L3) network made up of a set of connections [1].

This paper is organized into several sections, including this introduction. Section 2 outlines the characteristics of a wireless MANET. Section 3 overviews the differences between IP and mobile IP and routing protocols. Next, section 4 describes the multi-hop MANET auto- configuration method performance characteristics. Section 5 discuss the auto-configuration of a multi-hop MANET. Finally, Section 6 of the paper draws together the conclusion and future work of our work.

2. MANET CHARACTERISTICS

There are several characteristics of a wireless MANET (distinct from a wired network) which present unique challenges to any routing protocol and auto-configuration method used in the network.

2.1. Dynamic Time Varying Performance

A mobile radio interface can exhibit very dynamic time varying performance such as packet error rate (PER) and data rate [4]. As a result MANETs need to use robust protocols which would function better in such a dynamic and time varying environment.

2.2. Radio Link

A radio link can only exists between a wireless (MANET) node and its closest neighbors which are in radio range of each other. Because of the mobile nature of the network, any of these wireless nodes can move out of range or into range of another wireless node, and thus forming a new level 2 (L2) link topology. In addition most radio links are simplex links by nature that require either some sort of TDMA or CDMA access method.

Because each node in a MANET has a limited number of neighbors that it can send message packets, the practice in most MANETS is to give enough nodes in a MANET the ability to route messages. Practically each MANET node will need to have a direct radio link to at least one MANET router in order to guaranteed rout-ability to every other node in the MANET.

2.3. Asymmetric Reach-Ability

Many radio links exhibit asymmetric reach-ability. This is described as a connection in which non-reflective and /or non-transitive accessibility is part of normal activity [6]. Figure 1, shows the wireless links between four MANET nodes. The larger circles represent the effective range of the radios on each of the MANET nodes. Non-reflexive reach-ability means packets from node A can reach node C, but packets from node C can not reach node. This could occur because the radio in node A is stronger RF signal than the radio in node C therefore C can hear A, however A cannot hear C. Similarly, from node A reach node B, and packets from node B reach node D, but packets from node A do not reach node D.

2.4. Distributed and/or Centralized Management

The dynamic time varying performance and asymmetric reach-ability will add latency to most forms of centralized management in MANETs. As a result many protocols will attempt to utilize some form of distributed processing for network management and routing.

2.5. Routing Protocol

There are multiple routing protocols that are currently defined in [7], [8], [9], [10]. Each of these routing protocols provides different characteristics which affect the MANET. In addition, most of these protocols can use the hardware address for routing messages in a MANET. It can be assumed that no auto-configuration is needed to assign the hardware address and the hardware

address of each node is unique. But in order to inter-operate with an IPv4 network each node will need to be assigned a unique IPv4 address. It is during auto- configuration of the MANET where the unique IPv4 addresses are assigned to MANET nodes.

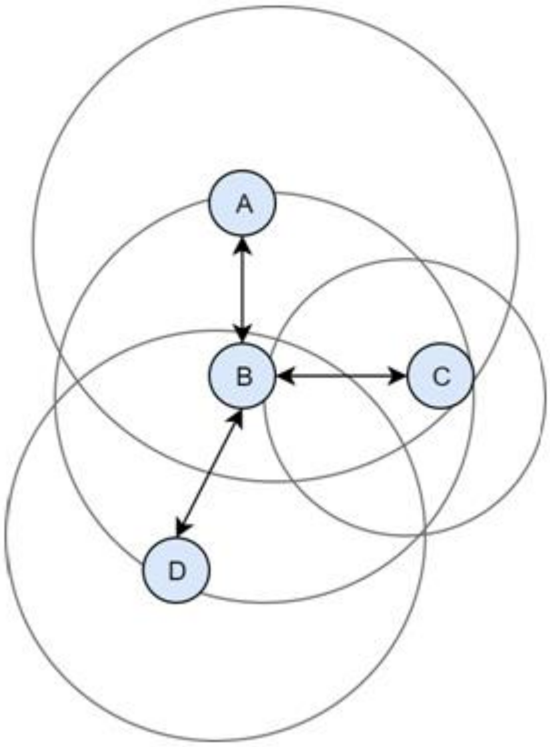

Figure 1. The Wireless Links Between Four MANET Nodes.

3. BACKGROUND

3.1. IP and Mobile IP

IPv4 describes the fourth iteration of the Internet Protocol (IP) and represents the most widely used network layer protocol under the TCP/IP protocol. Originally adopted in September 1981, IPv4 has become the internet standard, but it was not until August 2002 that the mobile standard was adopted by the Internet Engineering Task Force. IPv4 depends on a unique address to identify a node for communication, and with an Ethernet connection, the nodes address does not need to change because the physical location always remains the same. If the node were to start moving, however, the IP address must remain the same, or the packets intended for that node will never correctly reach their destination. Mobile IP allows for nodes to travel from one point of attachment to another without changing IP addresses (or the home address) [11].

Mobile IP works by using a home agent and a foreign agent to route messages. As the mobile node travels, a local care-of address is assigned to it, provided by the foreign agent. Once assigned a care-of address by a foreign agent, the mobile node sends a Registration Request back to its home node. The home node uses a table to keep track of the foreign agent and care-of address of the mobile node as well as the static IP address given to the node (known as the home address). Once a packet is sent to the home address of the mobile node, the home agent intercepts it and locates the mobile node on its registration table. The home agent then adds a new IP header onto the already existing header to route the packet to the new care-of location and tunnels the packet through the foreign agent, where the new header is de-capsulated, and the packet is delivered to the mobile node as if it were located at the home address [11]. Figure 2 presents an overhead view of IP mobility support for IPv4. By allowing the mobility of the node to be transparent to other higher level protocols, the node can easily go from different points of attachment without losing communication; however, MANETs lack the foreign agent needed to assign a care-of address over multiple hops.

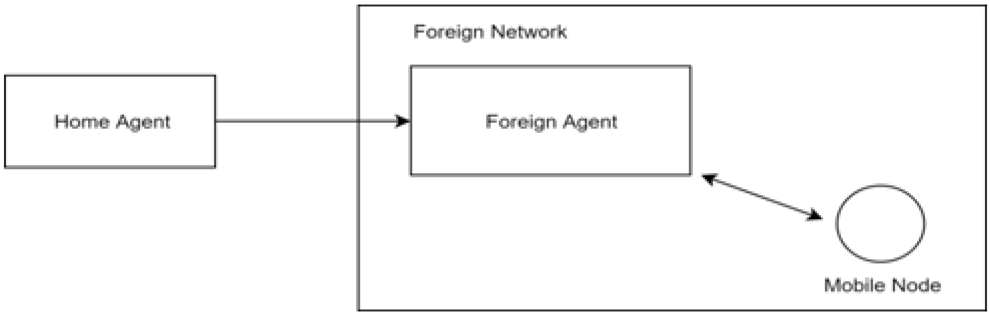

Figure 2. An Overhead View of IP Mobility Support for IPv4.

3.2. Experimental Routing Protocols

There are some experimental routing algorithms for MANETs that will be discussed here. A brief overview of each along with some advantages and disadvantages are given as follows:

1) Ad Hoc On-Demand Distance Vector (AODV): The AODV routing algorithm is a reactive protocol, that is, it only determines the path the packets will take when a connection is needed. Once a connection is needed, the node checks its route table to see if a path has already been established. If one has not, or if the path in the table is no longer valid, the node generates a route request, which propagates through the surrounding nodes until the desired destination is found (either by reaching the destination node itself or a node that has an active rout in its route table), in which case a route reply is sent back to the original node. The message can then be sent through the path that contains the smallest distance (that is, the least number of hops). Each node keeps a table of the active routes [7].

The main advantage of the AODV is the on demand nature of the protocol, which eliminates some of the overhead necessary in a proactive system that require both power and bandwidth to operate; however, the tables are not guaranteed to contain the best possible route, as the configuration may change over time but is not necessarily updated as quickly in the route tables. These stale table entries may also cause inconsistencies in the overall routing, but for sensor based networks, AODV offers a good solution.

2) Dynamic Source Routing (DSR): The DSR protocol is also reactive, but unlike the AODV algorithm, the DSR protocol relies on source routing in lieu of a routing table contained in the

source node and each intermediate node. The DSR protocol uses route discovery and route maintenance to create a source route and determine the validity of that route over time by sending out route requests from the source node and establishing a path by the route reply that comes from the destination [8].

The DSR protocol has similar advantages and disadvantages to the AODV protocol in that the on demand nature eliminates a significant amount of the overhead required but stale route caches can result in poorer performance or inconsistencies. The DSR protocol also tends to have a greater delay than protocols which are table based, but DSR offers an adequate solution for sensor based networks.

3) Optimized Link State Routing (OLSR): The OLSR protocol is proactive, meaning it maintains a full table of the topology of all nodes in the network and computes the optimal paths to send packets locally. Since the protocol cannot be set up exactly like a standard link-state routing protocol due to the lack of a real link in ad-hoc networks, multipoint distribution relays (MPRs) are used to forward broadcast messages and to establish the link state information that is to be used. MPRs are chosen from the nodes in the network, and not every node is an MPR. By using MPRs, the number of control messages that have to be sent out is limited and the number of possible links is limited, since a link can only exist between pairs of MPRs [9].

In an ideal situation, the OLSR protocol would be able to quickly determine the optimal path to send a packet; however, the protocol is not really ideal for networks using low power sensors since a large amount of power and bandwidth are required to propagate data throughout the network and establish the optimal paths for the packets to travel. The OLSR protocol offers the best path, however, and can be used quite effectively in networks using laptops or other higher power devices [12].

4) Topology Broadcast based on Reverse-Path Forwarding (TBRPF): The TBRPF protocol, like the OLSR, is a proactive link-state routing protocol, but each node only keeps track of part of its source tree to neighbors. Route discovery and maintenance only keeps track of the changes in the status of the neighbor nodes, reducing the size of routing messages, allowing for more frequent updates to the nodes routing tables [10].

By reducing the size of the routing message, the TBRPF protocol allows for the link-state type protocols to be better adapted to smaller networks; however, even with the reduced size of the routing messages, the protocol still would require a larger amount of power than is ideal for a sensor based network. TBRPF would be ideal in smaller laptop networks that have higher powered devices but lack the network size required to use and OLSR protocol.

4. Multi-Hop MANET Auto-Configuration Method Performance Characteristics

Much work has been done to determine what performance characteristics should be considered when evaluating MANET auto-configuration mechanisms [13]. The characteristics outlined include:

4.1. Protocol Overhead

Since radio interfaces normally have a lower bandwidth than wired interfaces a small protocol overhead is desired. And since auto-configuration requires the flooding of the network with auto-configuration request messages, then an optimal auto-configuration method would require minimal protocol overhead.

4.2. Robustness

Certain auto-configuration methods might assume the availability of a reliable L2 link. MANETs do not offer a reliable L2 radio link and any unreliable links would add latency to the auto-configuration solution. A robust auto-configuration method would minimize the latency added by unreliable links.

4.3. Convergence Time

The time required for a MANET node to get a unique IPv4 address, or the time required for the whole network to be supplied with unique IPv4 addresses is known as the convergence time. A good auto-configuration method would minimize convergence time of a MANET node or network.

4.4. Scalability

The scalability of the MANET auto-configuration method is also an important consideration. The auto-configuration method would have to scale from networks of less than 10 nodes to networks of over 10,000 nodes.

4.5. Address Space Utilization

How efficiently the auto-configuration method assigns IPv4 addresses is another important consideration of an auto-configuration method.

5. AUTO-CONFIGURATION OF A MULTI-HOP MANET

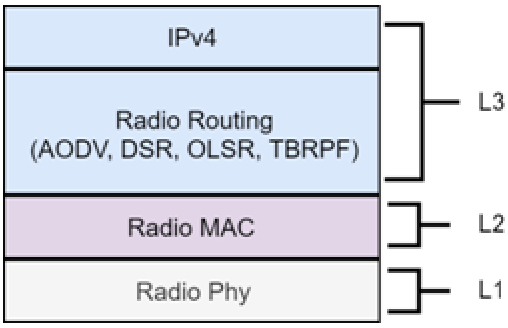

Figure 3. The First Three Layers of the MANET Radio Protocol Stack.

As it was mentioned before that the MANET will use one of the routing protocols, this lead us to assume the efficiency at which these protocols operate in the MANET environment, then the IP traffic can be encapsulated in a MANET routed packet. Figure 3 shows the protocol stack for such a con- figuration [14]. This provides a simpler implementation that allows the MANET to take advantage of the best radio MAC and routing protocol for its particular operational profile and MANET characteristics. On the another hand, the data flow of IP packets will either be into or out of the MANET to an Internet network. This assumption can be made for MANETS which can a more efficient radio routing algorithm (AODV, DSR, OLSR, TBRPF, etc.) to route from one MANET node to another, and the only time that an IP packet will be sent is when data needs to be routed into or out of the MANET. In fact, each MANET will need one or more MANET border node(s) (MBN) each of which shall have two interfaces, one MANET and the other shall be a wired interface to the MANET gateway. Otherwise, the MANET gateway can be incorporated in the MBN if there is only one MBN in the MANET [15].

These MBNs will receive radio routed IP packets and forward them onto the MANET gateway. It will also receive IP packets from the MANET gateway and start routing the packets towards the destination node. If an incoming IP packet is not able to be routed to its destination node on the MBNs MANET segment, then the packet will be re-routed through the MANET router and then broadcast to the other MBN(s). If the packet is routed successfully, the MANET gateway must update its routing table to reflect the new section of MBN MANET where the IP address of the destination is located [15].

Two types of MANET nodes will construct the rest of the MANET. The first type is a MANET routing node (MRN) [16]. These nodes will route radio packets with the desired routing protocol, and can also serve as a source and/or sink of data packets. The other type is a MANET endpoint (MEP) that do not route radio packets but server as a source or sink for packets. Notice that the IP network links form a tree network while the radio protocol links form a mesh network as it show in figure 4.

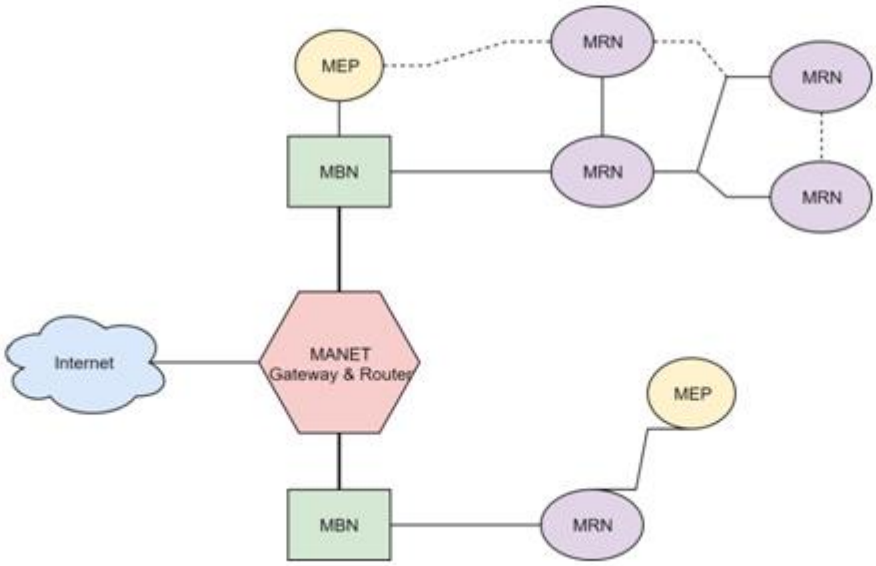

Figure 4. The MANET has two MBN connected to the MANET router over a wired interface (the thick line) as well as one or more MRN or MEP. The radio IP/radio protocol links are shown as thin lines and the links which only support radio protocol are shown as dotted lines.

When a MANET wishes to auto-configure to an IP network, the MANET gateway and MBN will receive their IP address first from the DHCP server [17]. Next, the MRN and MEP that have a direct radio link to a MBN will receive their IP address from the DHCP server (with the DHCP request/grant messages being routed through the MBN and MANET gateway). Then, successive MRN/MEP will then be granted IP addresses as soon as one of their direct radio link neighbors are granted an IP address and join the IP network tree [16].

Every MRN will keep track of the next hop's MAC address to the MBN and the number of hops between it and the MBN. Then when it routes a message on the IP network it will route it to the next hop towards the MBN. If the next hop MRN is no longer available it will then flood a routing request message looking for a radio link neighbor who is the closest to the MBN and then adjust its own hope number (the number of hops between it and the MBN) accordingly. This should preserve the tree structure of the IP network that is overlaid over the radio routing protocol network, making it robust to changes in topology and to dynamic time varying performance of the radio link.

Multi-cast messages received by the MBN over the radio interface will be forwarded to other MBN in the MANET over its wired interface. Radio protocol multi-cast messages received by a MBN over its wired interface will only be forwarded out the radio interface of that MBN.

6. CONCLUSION AND FUTURE WORK

The auto-configuration method described in this paper offers a method to auto-configure of MANET and to route IPv4 traffic using existing MANET routing protocols. One of the reasons why there are multiple MANET routing protocols is that different MANET topologies and operational profiles will require different routing protocols to have the best characteristics in protocol overhead, robustness, convergence time, and scalability. This auto-configuration method depends on the characteristics of the MANET routing protocol for these characteristics. In fact, the optimal MANET routing protocol can be chosen which best meets these criteria for the given topology and operational profile.

Future work could evaluate the efficiency of the auto- configuration method described in this work. It will also compare this auto-configuration method with versus methods described in [5]. Characteristics which should be evaluated include protocol overhead, robustness, convergence time, scalability, and address space utilization.

ACKNOWLEDGEMENTS

The author would like to thank University of Tabuk for supporting.

REFERENCES

[1] L. J. Garc´ıa Villalba, J. Garc´ıa Matesanz, A. L. Sandoval Orozco, and J. D. Ma´rquez D´ıaz, “Auto-configuration protocols in mobile ad hoc networks,” Sensors, vol. 11, no. 4, pp. 3652– 3666, 2011.

[2] L. M. S. Committee et al., “Ansi/ieee std 802.11, 1999 edition, part 11: Wireless lan medium access control (mac) and physical layer (phy) specifications,” IEEE standard, 1999.

[3] A. Sandoval Orozco, J. Garcia Matesanz, L. J. Garc´ıa Villalba, J. Mar- quez Diaz, and T.-H. Kim, “Security issues in mobile ad hoc networks,” International Journal of Distributed Sensor Networks, vol. 8, no. 11, p. 818054, 2012.

[4] J. Macker, I. Chakeres, and T. Clausen, “Mobile ad hoc network architecture,” IETF Autoconf Working Group, Internet Draft, 2007.

[5] C. Bernardos, M. Caldero´n, and H. Moustafa, “Survey of ip address autoconfiguration mechanisms for manets,” IETF, draft- bernardosmanetautoconf-survey-05. txt (work-in- progress).(June 2010), 2005.

[6] T. Narten, E. Nordmark, W. Simpson, and H. Soliman, “Neighbor discovery for ip version 6 (ipv6),” Tech. Rep., 2007.

[7] C. Perkins, E. Belding-Royer, and S. Das, “Ad hoc on-demand distance vector (aodv) routing,” Tech. Rep., 2003.

[8] D. Johnson, Y.-c. Hu, and D. Maltz, “The dynamic source routing protocol (dsr) for mobile ad hoc networks for ipv4,” Tech. Rep., 2007.

[9] T. Clausen and P. Jacquet, “Rfc 3626: Optimized link state routing protocol (olsr),” IETF, October, vol. 4, 2003.

[10] R. Ogier, F. Templin, and M. Lewis, “Topology dissemination based on reverse-path forwarding (tbrpf),” Tech. Rep., 2004.

[11] R. Pries, A. Ma¨der, D. Staehle, and M. Wiesen, “On the performance of mobile ip in wireless lan environments,” in International Workshop of the EuroNGI Network of Excellence. Springer, 2006, pp. 155–170.

[12] L. Yang, P. Zerfos, and E. Sadot, “Architecture taxonomy for control and provisioning of wireless access points (capwap),” Tech. Rep., 2005.

[13] B. O’Hara, P. Calhoun, and J. Kempf, “Configuration and provisioning for wireless access points (capwap) problem statement,” Tech. Rep., 2005.

[14] S. Khalid, A. Mahboob, F. Azim, and A.-u. Rehman, “Idhocnet-a novel protocol stack and architecture for ad hoc networks,” International Journal of Communication Networks and Information Security, vol. 7, no. 1, p. 20, 2015.

[15] C. Bernardos, M. Caldero´n, and H. Moustafa, “Survey of ip address autoconfiguration mechanisms for manets,” IETF, draft- bernardosmanetautoconf-survey-05. txt (work-in- progress).(June 2010), 2005.

[16] J. Macker, “Mobile ad hoc networking (manet): Routing protocol performance issues and evaluation considerations,” 1999.

[17] L. J. Garc´ıa Villalba, J. G. Matesanz, A. L. Sandoval Orozco, and J. D. Ma´rquez D´ıaz, “Distributed dynamic host configuration protocol (d2hcp),” Sensors, vol. 11, no. 4, pp. 4438– 4461, 2011.

AUTHORS

Adel R. Alharbi, Ph.D received the Bachelor of Science degree in Computer Science from Qassim University, Saudi Arabia in 2008, and two Masters of Science degrees in Security Engineering and Computer Engineering from Southern Methodist University, The United States of America, Texas, Dallas in 2013 and 2015 respectively. He also had the degree of Doctor of Philosophy in Computer Engineering from Southern Methodist University, The United States of America, Texas, Dallas in 2017. Adel has been a faculty staff member at College of Computer Science and Information Technology in University of Tabuk, Saudi Arabia since 2009. He acquired several academic certificates and published many scientific papers.