Mobile Ad-hoc Networks (MANET)
Internet-Draft
Intended status: Informational
Expires: January 12, 2014
E. Baccelli
INRIA
C. Perkins
Futurewei
July 11, 2013

Multi-hop Ad Hoc Wireless Communication
draft-baccelli-manet-multihop-communication-02

Abstract

This document describes characteristics of communication between nodes in a multi-hop ad hoc wireless network, that protocol engineers and system analysts should be aware of when designing solutions for ad hoc networks at the IP layer.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

Experience gathered with ad hoc routing protocol development, deployment and operation, shows that wireless communication presents specific challenges [RFC2501] [DoD01], which Internet protocol designers should be aware of, when designing solutions for ad hoc networks at the IP layer. This document briefly describes these challenges.

2. Multi-hop Ad Hoc Wireless Networks

For the purposes of this document, a multi-hop ad hoc wireless network will be considered to be a collection of devices that each have a radio transceiver, that are using the same physical and medium access protocols, that are moreover configured to self-organize and provide store-and-forward functionality on top of these protocols as needed to enable communications. The devices providing network connectivity are considered to be routers. Other non-routing wireless devices, if present in the ad hoc network, are considered to be "end-hosts". The considerations in this document apply equally to routers or end-hosts; we use the term "node" to refer to any such network device in the ad hoc network.

Examples of multi-hop ad hoc wireless network deployment and operation include wireless community networks such as Funkfeuer[FUNKFEUER] and Freifunk[FREIFUNK]; these use routers running OLSR (Optimized Link State Routing [RFC3626]) on IEEE 802.11 in ad hoc mode with the same ESSID (Extended Service Set Identification) at the link layer. Multi-hop ad hoc wireless networks may also run on link layers other than 802.11, and may use routing protocols other than OLSR (for instance, AODV[RFC3561], TBRPF[RFC3684], DSR[RFC4728], or OSPF-MPR[RFC5449]).

In contrast, simple hosts communicating through an 802.11 access point in infrastructure mode do not form a multi-hop ad hoc wireless network, since the central role of the access point is predetermined, and since nodes other than the access point do not generally provide store-and-forward functionality.

3. Common Packet Transmission Characteristics in Multi-hop Ad Hoc Wireless Networks

Let A and B be two nodes in a multi-hop ad hoc wireless network N. Suppose that, when node A transmits a packet through its interface on network N, that packet is correctly received by node B without requiring storage and/or forwarding by any other device. We will then say that B can "detect" packets transmitted by A, or more simply that B detects A. Note that therefore, when B detects an IP packet transmitted by A, the TTL of the IP packet detected by B will be precisely the same as it was when A transmitted that packet.

Let S be the set of nodes that can detect packets transmitted by node A through its interface on network N. The following section gathers common characteristics concerning packet transmission over such networks, which were observed through experience with MANET routing protocol development (OLSR[RFC3626], AODV[RFC3561], TBRPF[RFC3684], DSR[RFC4728], or OSPF-MPR[RFC5449]), as well as deployment and operation (Freifunk[FREIFUNK], Funkfeuer[FUNKFEUER]).

3.1. Asymmetry, Time-Variation, and Non-Transitivity

First, even though a node C in set S can (by definition) detect packets transmitted by node A, there is no guarantee that node C can, conversely, send IP packets directly to node A. In other words, even though C can detect packets transmitted by A (since it is a member of set S), there is no guarantee that A can detect packets transmitted by C. Thus, multi-hop ad hoc wireless communications may be "asymmetric". Such cases are common.

Second, there is no guarantee that, as a set, S is at all stable, i.e. the membership of set S may in fact change at any rate, at any time. Thus, multi-hop ad hoc wireless communications may be "time-variant". Time variation is often observed in multi-hop ad hoc wireless networks due to variability of the wireless medium, and to node mobility.

Now, conversely, let V be the set of nodes which A detects -- in other words, IP packets transmitted by any node in set V are received directly by A, without TTL decrement. Suppose that node A is communicating at time t0 through its interface on network N. As a consequence of time variation and asymmetry, we observe that A:

1. cannot assume that S = V,

2. cannot assume that S and/or V are unchanged at time t1 later than t0.

Furthermore, transitivity is not guaranteed over multi-hop ad hoc wireless networks. Indeed, let's assume that, through their respective interfaces within network N:

1. node B and node A can detect one another (i.e. node B is a member of sets S and V), and,

2. node A and node C can also detect one another (i.e. node C is a also a member of sets S and V).

These assumptions do not imply that node B can detect node C, nor that node C can detect node B (through their interface on network N). Such "non-transitivity" is common on multi-hop ad hoc wireless networks.

In a nutshell: multi-hop ad hoc wireless communications can be asymmetric, non-transitive, and time-varying.

3.2. Radio Range and Wireless Irregularities

Section 3.1 presents an abstract description of some common characteristics concerning packet transmission over multi-hop ad hoc wireless networks. This section describes practical examples, which illustrate the characteristics listed in Section 3.1 as well as other common effects.

Wireless communication links are subject to limitations to the distance across which they may be established. The range-limitation factor creates specific problems on multi-hop ad hoc wireless networks. In this context, the radio ranges of several nodes often partially overlap. Such partial overlap causes communication to be non-transitive and/or asymmetric, as described in Section 3.1. Moreover, the range varies from one node to another, depending on location and environmental factors. This is in addition to the time variation of range and signal strength caused by variability in the local environment.

For example, as depicted in Figure 1, it may happen that a node B detects a node A which transmits at high power, whereas B transmits at lower power. In such cases, B detects A, but A cannot detect B. This examplifies the asymmetry in multi-hop ad hoc wireless communications as defined in Section 3.1.

```
                 Radio Ranges for Nodes A and B

              <~~~~~~~~~~~~~+~~~~~~~~~~~~~>
                            |      <~~~~~~+~~~~~~>
                         +--|--+       +--|--+
                         |  A  |======>|  B  |
                         +-----+       +-----+
```

Figure 1: Asymmetric Link example. Node A can communicate with node B, but B cannot communicate with A.

Another example, depicted in Figure 2, is known as the "hidden node" problem. Even though the nodes all have equal power for their radio transmissions, they cannot all detect one another. In the figure, nodes A and B can detect one another, and A and C can also detect one another. On the other hand, nodes B and C cannot detect one another. When nodes B and C try to communicate with node A simultaneously, their radio signals collide. Node A will only be able to detect noise, and may even be unable to determine the source of the noise. The hidden terminal problem illustrates the property of non-transitivity in multi-hop ad hoc wireless communications as described in Section 3.1.

```
                    Radio Ranges for Nodes A, B, C

      <~~~~~~~~~~~~~+~~~~~~~~~~~~~> <~~~~~~~~~~~~~+~~~~~~~~~~~~~>
                    |<~~~~~~~~~~~~~+~~~~~~~~~~~~~>|
                 +--|--+        +--|--+        +--|--+
                 |  B  |=======>|  A  |<=======|  C  |
                 +-----+        +-----+        +-----+
```

Figure 2: The hidden node problem. Nodes C and B try to communicate with node A at the same time, and their radio signals collide.

Another situation, shown in Figure 3, is known as the "exposed node" problem. In the figure, node A is transmitting (to node B). As

shown, node C cannot reliably communicate with node D, because of the on-going transmission of node A, presenting interference within C's radio-range. Node C cannot detect D, but node D can detect C because D is outside A's radio range. Node C is then called an "exposed node", because it is exposed to co-channel interference from node A and thereby prevented from exchanging protocol messages to enable data transmission to node D -- even though the transmission would be successful and would not interfere with the reception of data sent from node A to node B.

```
                   Radio Ranges for Nodes A, B, C, D

  <~~~~~~~~~~~~+~~~~~~~~~~~~> <~~~~~~~~~~~~+~~~~~~~~~~~>
               |<~~~~~~~~~~~~+~~~~~~~~~~~~>|<~~~~~~~~~~~~+~~~~~~~~~>
            +--|--+       +--|--+       +--|--+       +--|--+
            |  B  |<======|  A  |       |  C  |======>|  D  |
            +-----+       +-----+       +-----+       +-----+
```

Figure 3: The exposed node problem. When node A is communicating with node B, node C is an "exposed node".

Hidden and exposed node situations are often observed in multi-hop ad hoc wireless networks. Problems with asymmetric links may also arise for reasons other than power inequality (e.g., multipath interference). Such problems are often resolved by specific mechanisms below the IP layer. However, depending on the link layer technology in use and the position of the nodes, such problems due to range-limitation and partial overlap may affect the IP layer.

Besides radio range limitations, wireless communications are affected by irregularities in the shape of the geographical area over which nodes may effectively communicate (see for instance [MC03], [MI03]). For example, even omnidirectional wireless transmission is typically non-isotropic (i.e. non-circular). Signal strength often suffers frequent and significant variations, which are not a simple function of distance. Instead, it is a complex function of the environment including obstacles, weather conditions, interference, and other factors that change over time. Because each individual link has to encounter different terrain, path, obstructions, atmospheric conditions and other phenomena, analytical formulation of signal strength is considered intractable [VTC99], and the radio engineering community has thus developed numerous radio propagation models, relying on median values observed in specific environments [SAR03].

The above irregularities also cause communications on multi-hop ad hoc wireless networks to be non-transitive, asymmetric, or time-varying, as described in Section 3.1, and may impact protocols at the

IP layer and above. There may be no indication to IP when a previously established communication channel becomes unusable; "link down" triggers are generally absent in multi-hop ad hoc wireless networks, since the absence of detectable radio energy (e.g., in carrier waves) may simply indicate that neighboring nodes are not currently transmitting. Such an absence of detectable radio energy does not therefore indicate whether or not transmissions have failed to reach the intended destination.

4. Alternative Terminology

Many terms have been used in the past to describe the relationship of nodes in a multi-hop ad hoc wireless network based on their ability to send or receive packets to/from each other. The terms used in this document have been selected because the authors believe they are unambiguous, with respect to the goal of this document (see Section 1).

Nevertheless, here are a few other terms that describe the same relationship between nodes in multi-hop ad hoc wireless networks. In the following, let network N be, again, a multi-hop ad hoc wireless network. Let the set S be, as before, the set of nodes that can directly receive packets transmitted by node A through its interface on network N. In other words, any node B belonging to S can detect packets transmitted by A. Then, due to the asymmetry characteristic of wireless links:

- We may say that node B hears node A. In this terminology, there is no guarantee that node A is hears node B, even if node B hears node A.

- We may say that node B is reachable from node A. In this terminology, there is no guarantee that node A is reachable from node B, even if node B is reachable from node A.

- We may say that node A has a link to node B. In this terminology, there is no guarantee that node B has a link to node A, even if node A has a link to node B.

- We may say that node B is adjacent to node A. In this terminology, there is no guarantee that node A is adjacent to node B, even if node B is adjacent to node A.

- We may say that node B is downstream from node A. In this terminology, there is no guarantee that node A is downstream from node B, even if node B is downstream from node A.

- We may say that node B is a neighbor of node A. In this terminology, there is no guarantee that node A is a neighbor of node B, even if node B a neighbor of node A. As it happens, the terminology for "neighborhood" is quite confusing for asymmetric links. When B can detect signals from A, but A cannot detect B, it is not clear whether B should be considered a neighbor of A at all, since A would not necessarily be aware that B was a neighbor. Perhaps it is best to avoid the "neighbor" terminology except for symmetric links.

This list of alternative terminologies is given here for illustrative purposes only, and is not suggested to be complete or even representative of the breadth of terminologies that have been used in various ways to explain the properties mentioned in Section 3.

5. IP over Multi-hop Ad Hoc Wireless

The characteristics of packet transmission over multi-hop ad hoc wireless networks, described in previous sections, are not the typical characteristics expected by IP [RFC6250]. Nevertheless, it is possible and desirable to run IP over such networks, through the use of:

IP interface configuration, such as described in RFC 5889 [RFC5889], or

routing protocols designed for operation over wireless interfaces, for example OLSR[RFC3626], AODV[RFC3561], or OSPF-MPR[RFC5449].

Thus, even though the physical effects described in this document require robust protocol designs for routing and topology management, the experience in the projects described in the cited references shows that useful networks can be designed and operated using well-understood techniques. Protocols running above the IP layer can be shielded somewhat from the unusual characteristics experienced over multi-hop ad hoc wireless networks. Note however that some protocols are nevertheless more appropriate than others when interfaces to multi-hop ad hoc wireless networks are involved in the communication. For instance, for applications written to run over both UDP and TCP, the latter choice may be preferred in situations with relatively high packet loss rates. But such choices must be based on application requirements.

6. Security Considerations

This document does not have any security considerations.

7. IANA Considerations

This document does not have any IANA actions.

8. Informative References

[RFC2501] Corson, M. and J. Macker, "Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations", RFC 2501, January 1999.

[RFC3561] Perkins, C., Belding-Royer, E., and S. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing", RFC 3561, July 2003.

[RFC3626] Clausen, T. and P. Jacquet, "Optimized Link State Routing Protocol (OLSR)", RFC 3626, October 2003.

[RFC3684] Ogier, R., Templin, F., and M. Lewis, "Topology Dissemination Based on Reverse-Path Forwarding (TBRPF)", RFC 3684, February 2004.

[RFC4728] Johnson, D., Hu, Y., and D. Maltz, "The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4", RFC 4728, February 2007.

[RFC4903] Thaler, D., "Multi-Link Subnet Issues", RFC 4903, June 2007.

[RFC5449] Baccelli, E., Jacquet, P., Nguyen, D., and T. Clausen, "OSPF Multipoint Relay (MPR) Extension for Ad Hoc Networks", RFC 5449, February 2009.

[RFC5889] Baccelli, E. and M. Townsley, "IP Addressing Model in Ad Hoc Networks", RFC 5889, September 2010.

[RFC6250] Thaler, D., "Evolution of the IP Model", RFC 6250, May 2011.

[DoD01] Freebersyser, J. and B. Leiner, "A DoD perspective on mobile ad hoc networks", Addison Wesley C. E. Perkins, Ed., 2001, pp. 29--51, 2001.

[FUNKFEUER]

, "Austria Wireless Community Network, http://www.funkfeuer.at", 2013.

[MC03] Corson, S. and J. Macker, "Mobile Ad hoc Networking: Routing Technology for Dynamic, Wireless Networks", IEEE Press Mobile Ad hoc Networking, Chapter 9, 2003.

[SAR03] Sarkar, T., Ji, Z., Kim, K., Medour, A., and M. Salazar-Palma, "A Survey of Various Propagation Models for Mobile Communication", IEEE Press Antennas and Propagation Magazine, Vol. 45, No. 3, 2003.

[VTC99] Kim, D., Chang, Y., and J. Lee, "Pilot power control and service coverage support in CDMA mobile systems", IEEE Press Proceedings of the IEEE Vehicular Technology Conference (VTC), pp.1464-1468, 1999.

[MI03] Kotz, D., Newport, C., and C. Elliott, "The Mistaken Axioms of Wireless-Network Research", Dartmouth College Computer Science Technical Report TR2003-467, 2003.

[FREIFUNK] , "Freifunk Wireless Community Networks, http://www.freifunk.net", 2013.

Appendix A. Acknowledgements

This document stems from discussions with the following people, in alphabetical order: Jari Arkko, Teco Boot, Carlos Jesus Bernardos Cano, Ian Chakeres, Thomas Clausen, Christopher Dearlove, Ralph Droms, Brian Haberman, Ulrich Herberg, Paul Lambert, Kenichi Mase, Thomas Narten, Erik Nordmark, Alexandru Petrescu, Stan Ratliff, Zach Shelby, Shubhranshu Singh, Fred Templin, Dave Thaler, Mark Townsley, Ronald Velt in't, and Seung Yi.

Authors' Addresses

Emmanuel Baccelli
INRIA

Phone: +33-169-335-511
EMail: Emmanuel.Baccelli@inria.fr
URI: http://www.emmanuelbaccelli.org/

Charles E. Perkins
Futurewei

Phone: +1-408-330-5305
EMail: charlie.perkins@huawei.com