Multi-hop Ad Hoc Wireless Communication
draft-ietf-intarea-adhoc-wireless-com-02

Abstract

   This document describes characteristics of communication between
   interfaces 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 does not prescribe
   solutions, but instead briefly describes these challenges in hopes of
   increasing that awareness.

   As background, RFC 3819 [RFC3819] provides an excellent reference for
   higher-level considerations when designing protocols for shared
   media. From MTU to subnet design, from security to considerations
   about retransmissions, RFC 3819 provides guidance and design
   rationale to help with many aspects of higher-level protocol design.

   The present document focuses more specifically on challenges in
   multi-hop ad hoc wireless networking. For example, in that context,
   even though a wireless link may experience high variability as a
   communications channel, such variation does not mean that the link is
   "broken". Many layer-2 technologies serve to reduce error rates by
   various means. Nevertheless, such errors as noted in this document
   may still become visible above layer-2 and so become relevant to the
   operation of higher layer protocols.

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 at least one radio transceiver (i.e., wireless network
   interface), and that are moreover configured to self-organize and
   provide store-and-forward functionality as needed to enable

communications. This document focuses on the characteristics of
communications through such a network interface.

Although the characteristics of packet transmission over multi-hop ad
hoc wireless networks, described below, are not the typical
characteristics expected by IP [RFC6250], it is desirable and
possible to run IP over such networks, as demonstrated in certain
deployments currently in operation, such as Freifunk [FREIFUNK], and
Funkfeuer [FUNKFEUER]. These deployments use routers running IP
protocols e.g., OLSR (Optimized Link State Routing [RFC3626]) on top
of 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 IEEE 802.11, and may
use routing protocols other than OLSR. The following documents
provide a number of examples: AODV [RFC3561], OLSRv2 [RFC7181], TBRPF
[RFC3684], OSPF ([RFC5449], [RFC5820] and [RFC7137]), or DSR
[RFC4728].

Note that in contrast, devices communicating via an IEEE 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 devices 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**

In the following, we will consider several devices in a multi-hop ad
hoc wireless network N. Each device will be considered only through
its own wireless interface to network N. For conciseness and
readability, this document uses the expressions "device A" (or simply
"A") as a synonym for "the wireless interface of device A to network
N".

Let A and B be two devices in network N. Suppose that, when device A
transmits an IP packet through its interface on network N, that
packet is correctly and directly received by device B without
requiring storage and/or forwarding by any other device. We will
then say that B can "detect" A. Note that therefore, when B detects
A, an IP packet transmitted by A will be rigorously identical to the
corresponding IP packet received by B.

Let S be the set of devices that detect device A through its wireless
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 (for instance, OLSR[RFC3626], AODV[RFC3561],
TBRPF[RFC3684], DSR[RFC4728], and OSPF-MPR[RFC5449]), as well as

deployment and operation (e.g., Freifunk[FREIFUNK],
Funkfeuer[FUNKFEUER]).

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

First, even though a device C in set S can (by definition) detect
device A, there is no guarantee that C can, conversely, send IP
packets directly to A. In other words, even though C can detect A
(since it is a member of set S), there is no guarantee that A can
detect 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
device mobility.

Now, conversely, let V be the set of devices which A detects.
Suppose that 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, and

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. Suppose that, through their respective interfaces
within network N:

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

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

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

In summary: 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 communications are particularly subject to limitations on
   the distance across which they may be established. The range-
   limitation factor creates specific problems on multi-hop ad hoc
   wireless networks. Due to the lack of isolation between the
   transmitters, the radio ranges of several devices often partially
   overlap, causing communication to be non-transitive and/or asymmetric
   as described in Section 3.1. Moreover, the range of each device may
   depend on location and environmental factors. This is in addition to
   possible time variations of range and signal strength.

   For example it may happen that a device B detects a device A which
   transmits at high power, whereas B transmits at lower power. In such
   cases, as depicted in Figure 1, B can detect A, but A cannot detect
   B. This exemplifies asymmetry in wireless communications as defined
   in Section 3.1.

```
                   Radio Range for Device A
             <~~~~~~~~~~~~~+~~~~~~~~~~~~~~>
                          |        Range for Device B
                          |        <~~~~~~+~~~~~~>
                   +--|--+        +--|--+
                   |  A  |======>|  B  |
                   +-----+        +-----+
```
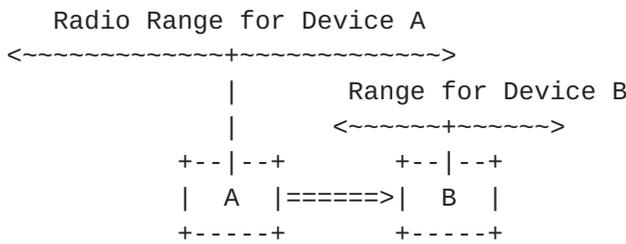
               Figure 1: Asymmetric Wireless Communication

   Another example, depicted in Figure 2, is known as the "Hidden
   Terminal" problem. Even though the devices all have equal power for
   their radio transmissions, they cannot all detect one another. In
   the figure, devices A and B can detect one another, and devices A and
   C can also detect one another. Nevertheless, B and C cannot detect
   one another. When B and C simultaneously try to communicate with A,
   their radio signals collide. Device A may then receive incoherent
   noise, and may even be unable to determine the source of the noise.
   The hidden terminal problem is a consequence of the property of non-
   transitivity in multi-hop ad hoc wireless communications as described
   in Section 3.1.

```
      Radio Range for Device B      Radio Range for Device C
   <~~~~~~~~~~~~+~~~~~~~~~~~~~> <~~~~~~~~~~~~~+~~~~~~~~~~~~~>
                |  Radio Range for Device A   |
                |<~~~~~~~~~~~~+~~~~~~~~~~~~~>|
        +--+--+          +--+--+          +--+--+
        |  B  |=======>|  A  |<=======|  C  |
        +-----+          +-----+          +-----+
```

              Figure 2: Hidden Terminal Problem

   Another situation, shown in Figure 3, is known as the "Exposed
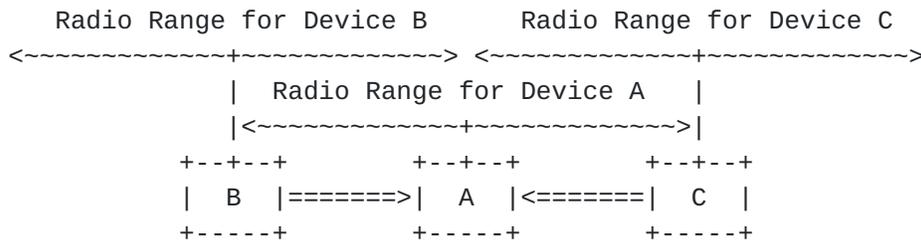   Terminal" problem. In the figure, device A and device B can detect
   each other, and A is transmitting packets to B, thus A cannot detect
   device C -- but C can detect A. As shown in Figure 3, during the on-
   going transmission of A, device C cannot reliably communicate with
   device D because of interference within C's radio range due to A's
   transmissions. Device C is then said to be "exposed", because it is
   exposed to co-channel interference from A and is thereby prevented
   from reliably exchanging protocol messages with D -- even though
   these transmissions would not interfere with the reception of data
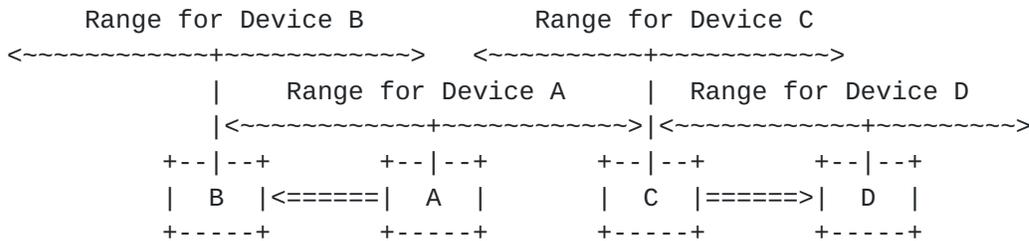   sent from A destined to B.

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

              Figure 3: Exposed Terminal Problem

   Hidden and exposed terminal situations are often observed in multi-
   hop ad hoc wireless networks. Asymmetry issues with wireless
   communication 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; CSMA/CA, for example,
   requires that the physical medium be unoccupied from the point of
   view of both devices before starting transmission. Nevertheless,
   depending on the link layer technology in use and the position of the
   devices, such problems may affect the IP layer due to range
   limitation and partial overlap.

   Besides radio range limitations, wireless communications are affected
   by irregularities in the shape of the geographical area over which
   devices 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 do not have a
simple dependence on distance. Instead, the dependence is a complex
function of the environment including obstacles, weather conditions,
interference, and other factors that change over time. Because
wireless communications often encounter different terrain, path,
obstructions, atmospheric conditions and other phenomena, analytical
formulation of signal strength is considered intractable [VTC99].
The radio engineering community has developed numerous radio
propagation approximations, relying on median values observed in
specific environments [SAR03].

These irregularities 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 the IP layer when a
previously established communication channel becomes unusable; "link
down" triggers are often 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 devices are not
currently transmitting.

4. Alternative Terminology

Many terms have been used in the past to describe the relationship of
devices 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
previous sections of this document have been selected because the
authors believe they are unambiguous, with respect to the goal of
this document as formulated in Section 1.

In this section, we exhibit some other terms that describe the same
relationship between devices 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 devices
that can directly receive packets transmitted by device A through its
interface on network N. In other words, any device B belonging to S
can detect packets transmitted by A. Then, due to the asymmetric
nature of wireless communications:

   - We may say that device A "reaches" device B. In this
   terminology, there is no guarantee that B reaches A, even if A
   reaches B.

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

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

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

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

   - We may say that device B "is a neighbor of" device A. In this
   terminology, there is no guarantee that A is a neighbor of B, even
   if B a neighbor of A. Terminology based on "neighborhood" is
   quite confusing for multi-hop wireless communications. For
   example, when B can detect A, but A cannot detect B, it is not
   clear whether or not B should be considered a neighbor of A; A
   would not necessarily be aware that B was a neighbor, as it cannot
   detect B. It is thus best to avoid the "neighbor" terminology,
   except when bidirectionality has been established.

   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. Note
   that bidirectionality is not synonymous with symmetry. For example,
   the error statistics in either direction are often different for a
   link that is otherwise considered bidirectional.

5. Security Considerations

   Section 18 of RFC 3819 [RFC3819] provides an excellent overview of
   security considerations at the subnetwork layer. Beyond the material
   there, multi-hop ad hoc wireless networking (i) is not limited to
   subnetwork layer operation, and (ii) makes use of wireless
   communications.

   On one hand, a detailed description of security implications of
   wireless communications in general is outside of the scope of this
   document. It is true that eavesdropping on a wireless link is much
   easier than for wired media (although significant progress has been
   made in the field of wireless monitoring of wired transmissions). As
   a result, traffic analysis attacks can be even more subtle and
   difficult to defeat in this context. Furthermore, such
   communications over a shared media are particularly prone to theft of
   service and denial of service (DoS) attacks.

On the other hand, the potential multi-hop aspect of the networks we consider in this document goes beyond traditional scope of subnetwork design. In practice, unplanned relaying of network traffic (both user traffic and control traffic) happens routinely. Due to the physical nature of wireless media, Man in the Middle (MITM) attacks are facilitated, which may significantly alter network performance. This highlights the importance of the "end-to-end principle": L3 security, end-to-end, becomes a primary goal, independently of securing layer-2 and layer-1 protocols (though L2 and L1 security often help to reach this goal).

6. IANA Considerations

This document does not have any IANA actions.

7. Informative References

[RFC2501] Corson, S. and J. Macker, "Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations", RFC 2501, DOI 10.17487/RFC2501, January 1999, <http://www.rfc-editor.org/info/rfc2501>.

[RFC3561] Perkins, C., Belding-Royer, E., and S. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing", RFC 3561, DOI 10.17487/RFC3561, July 2003, <http://www.rfc-editor.org/info/rfc3561>.

[RFC3626] Clausen, T., Ed. and P. Jacquet, Ed., "Optimized Link State Routing Protocol (OLSR)", RFC 3626, DOI 10.17487/RFC3626, October 2003, <http://www.rfc-editor.org/info/rfc3626>.

[RFC3684] Ogier, R., Templin, F., and M. Lewis, "Topology Dissemination Based on Reverse-Path Forwarding (TBRPF)", RFC 3684, DOI 10.17487/RFC3684, February 2004, <http://www.rfc-editor.org/info/rfc3684>.

[RFC3819] Karn, P., Ed., Bormann, C., Fairhurst, G., Grossman, D., Ludwig, R., Mahdavi, J., Montenegro, G., Touch, J., and L. Wood, "Advice for Internet Subnetwork Designers", BCP 89, RFC 3819, DOI 10.17487/RFC3819, July 2004, <http://www.rfc-editor.org/info/rfc3819>.

[RFC4728] Johnson, D., Hu, Y., and D. Maltz, "The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4", RFC 4728, DOI 10.17487/RFC4728, February 2007, <http://www.rfc-editor.org/info/rfc4728>.

   [RFC5449] Baccelli, E., Jacquet, P., Nguyen, D., and T. Clausen,
              "OSPF Multipoint Relay (MPR) Extension for Ad Hoc
              Networks", RFC 5449, DOI 10.17487/RFC5449, February 2009,
              <http://www.rfc-editor.org/info/rfc5449>.

   [RFC5820] Roy, A., Ed. and M. Chandra, Ed., "Extensions to OSPF to
              Support Mobile Ad Hoc Networking", RFC 5820,
              DOI 10.17487/RFC5820, March 2010,
              <http://www.rfc-editor.org/info/rfc5820>.

   [RFC6250] Thaler, D., "Evolution of the IP Model", RFC 6250,
              DOI 10.17487/RFC6250, May 2011,
              <http://www.rfc-editor.org/info/rfc6250>.

   [RFC7137] Retana, A. and S. Ratliff, "Use of the OSPF-MANET
              Interface in Single-Hop Broadcast Networks", RFC 7137,
              DOI 10.17487/RFC7137, February 2014,
              <http://www.rfc-editor.org/info/rfc7137>.

   [RFC7181] Clausen, T., Dearlove, C., Jacquet, P., and U. Herberg,
              "The Optimized Link State Routing Protocol Version 2",
              RFC 7181, DOI 10.17487/RFC7181, April 2014,
              <http://www.rfc-editor.org/info/rfc7181>.

   [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, Brian Carpenter, Carlos
   Jesus Bernardos Cano, Zhen Cao, Ian Chakeres, Thomas Clausen, Robert
   Cragie, 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

   EMail: Emmanuel.Baccelli@inria.fr
   URI: http://www.emmanuelbaccelli.org/

   Charles E. Perkins
   Futurewei

   Phone: +1-408-330-4586
   EMail: charlie.perkins@huawei.com