Mobile Ad hoc Networking (MANET)
Internet-Draft
Intended status: Informational
Expires: May 16, 2010

U. Herberg
T. Clausen
LIX, Ecole Polytechnique

November 12, 2009

Security Threats for NHDP
draft-herberg-manet-nhdp-sec-threats-00

Abstract

This document analyses common security threats of the Neighborhood Discovery Protocol (NHDP) and describes impacts for MANET routing protocols using NHDP.

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on May 16, 2010.

Copyright Notice

Table of Contents

1. Introduction

The Neighborhood Discovery Protocol (NHDP) [NHDP] allows routers to exchange information about their one-hop and two-hop neighbors by means of HELLO messages. It is a common base protocol for several protocols in the MANET working group, such as OLSRv2 [OLSRv2] and SMF [SMF]. The neighborhood information, exchanged between routers using NHDP, serves these routing protocols as a baseline for calculating paths to all destinations in the MANET, relay set selection for network-wide transmissions etc.

Due to the fact that NHDP is typically used in wireless environments, it is potentially exposed to different kinds of security threats, some of which are of particular significance as compared to wired networks. As wireless radio waves can be captured as well as transmitted by any wireless device within radio range, there is commonly no physical protection as for wired networks. The NHDP specification does not define any security means for protecting the integrity of the information it acquires, however suggests that this be addressed in a fashion appropriate to the deployment of the network.

This document will describe these security attacks which NHDP is vulnerable to. In addition, the document outlines the consequences of such security attacks to NHDP for routing protocols using NHDP for neighborhood discovery. It is out of scope of this document to provide solutions to counteract security attacks to NHDP.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

Additionally, this document uses the terminology of [RFC5444] and [NHDP].

3. NHDP Threat Overview

NHDP [NHDP] defines a message exchange protocol based on HELLO messages in order for each router to acquire topological information about 1-hop and 2-hop neighbors. It specifies information bases that store the information and the necessary message exchange. These information bases can be accesses by routing protocols such as OLSRv2 [OLSRv2] to construct routes to destinations in the MANET.

Every router periodically transmits HELLO messages on each of its interfaces with a hop-limit of 1 (i.e. HELLOs are never forwarded by a router). In these HELLO messages, a router announces the IP addresses of heard, symmetric and lost neighbor interface addresses.

An adversary has several ways of harming the neighbor discovery process: It can announce "wrong" information about its identity, postulate non-existent links, and replay HELLO messages. These attacks are presented in detail in Section 4.

The different ways of attacking an NHDP deployment will eventually lead to inconsistent information bases, not reflecting the correct topology of the MANET any more. This means that routers may be unable to detect links to their neighbors correctly (for NHDP), and thus corrupt the routing process of a routing protocol using the neighbor information of NHDP. These implications to protocols using the state of NHDP are in detail described in Section 5.

4. Detailed Description of Security Threats to NHDP

In this section, the different kind of threats to NHDP are detailed.

For every attack, a description of the mechanism of the attack is followed by the implications for the NHDP instance. Implications on routing protocols using NHDP are presented in Section 5.

For simplicity, in all examples contained in the following sections, it is assumed that routers only have a single interface with a single IP address configured. All the attacks apply as well for routers with multiple interfaces and multiple addresses.

4.1. Jamming

One vulnerability, common for all protocols operating a wireless ad hoc network, is that of "jamming" - i.e. that a router generates massive amounts of interfering radio transmissions, which will prevent legitimate traffic (e.g. control traffic as well as data traffic) on part of a network. This vulnerability cannot be dealt with at L3 (if at all), leaving the network without the ability to maintain connectivity. Jamming is somewhat similar to that of network overload and subsequent denial of service: a sufficiently significant amount of control traffic is lost, preventing HELLO messages to be correctly received.

If a considerable amount of HELLO messages are lost or corrupted due to collisions, neighbor routers are able not any more to establish links between them. This effectively renders NHDP unusable for upper layer protocols, since no stable links can be used for sending out

control packets, or for calculating routing information.

4.2. Incorrect HELLO Message Generation

Every router running NHDP performs mainly two tasks: Periodically generating HELLO messages and processing incoming HELLO messages from neighbor routers. This section describes two security attacks involving the HELLO generation.

4.2.1. Identity Spoofing

The so-called identity spoofing implies that a router sends HELLO messages pretending to have the identity of another router. An attacker can accomplish this by using another router's IP address in an address block of a HELLO, and associating this address with a

LOCAL_IF Address Block TLV. In addition, it may need to set the source address of the IP header that contains the control message.

If a router receives such a forged HELLO message from a neighbor, it will assume that this HELLO comes from a router with the claimed interface address. As a consequence, it will add a Link Tuple to that neighbor with the spoofed address, and include it in its next HELLO messages as a heard neighbor (and possibly as symmetric neighbor after another HELLO exchange).

Identity spoofing is particular harmful if a router spoofs the identity of another router that exists in the same routing domain. With respect to NHDP, such a duplicated, spoofed address can lead to an inconsistent state up to two hops from a router. Figure 1) depicts a simple example. In that example, router A is in radio range of C, but not of X. If X spoofs the address of A, that can lead to conflicts for upper-layer routing protocols, and therefore for wrong path calculations as well as incorrect data traffic forwarding.

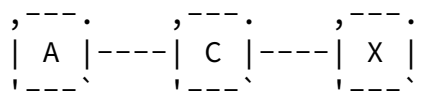

Figure 1

Figure 2) depicts another example. In this example, A is two hops away from router C, reachable through router B. If the attacker X spoofs the address of A, C may think that A is indeed reachable through router D.

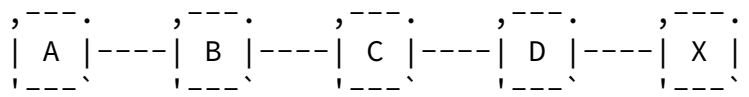

Figure 2

4.2.2. Link Spoofing

Similarly, link spoofing implies that a router sends HELLO messages, signaling an incorrect set of neighbors. This may take either of two forms: An attacker can postulate addresses of non-present neighbor routers in an address block of a HELLO, associated with LINK_STATUS TLVs. Alternatively, a compromised router can "ignore" existing neighbors by not advertizing them in its HELLO messages.

The effect of link spoofing with respect to NHDP are twofold, depending on the two cases mentioned above: If the compromised router ignores existing neighbors, there may not be any connectivity to or from these routers to others routers in the MANET. If, on the other hand, the router advertizing non-existing links, this can lead wrong topological information in the information base, which may be used by routing protocols.

4.3. Replay attack

A replay attack is, simply, where control traffic from one region of the network is recorded and replayed in a different region (this type of attack is also known as the Wormhole attack). This may, for example, happen when two routers collaborate on an attack, one recording traffic in its proximity and tunneling it to the other router, which replays the traffic. In a protocol where links are discovered by testing reception, this will result in extraneous link creation (basically, a link between the two ``attacking'' routers). While this may result from an attack, we note that it may also be intentional: if data-traffic too is relayed over the virtual link over the ``tunnel'', the link being detected is, indeed valid. This is, for instance, used in wireless repeaters. If data traffic is not carried over the virtual link, an imaginary, compromised, link has been created. Replay attacks can be especially damaging if coupled with spoofing and playing with sequence numbers in the replayed messages, potentially destroying some important topology information in routers all over the network.

5. Impact of inconsisent Information Bases for Routing Protocols using NHDP

The different security attacks on NHDP have been presented in

Section 4 which lead to an inconsistent state of the topology on the

routers. This section describes the impact for routing protocols that use NHDP as underlying neighbor discovery protocol, in particular OLSRv2 [OLSRv2], and SMF.

5.1. MPR Calculation

TBD

5.2. Routing Loops

TBD

5.3. Invalid or non-existing Paths to Destinations

TBD

5.4. Data Sinkhole

TBD

6. IANA Considerations

This document contains no actions for IANA.

7. Security Considerations

This document does not specify a protocol or a procedure. The document, however, reflects on security considerations for NHDP and MANET routing protocols using NHDP for neighborhood discovery.

8. Normative References

[NHDP] Clausen, T., Dean, J., and C. Dearlove, "MANET Neighborhood Discovery Protocol (NHDP)", work in progress draft-ietf-manet-nhdp-11.txt, October 2009.

[OLSRv2] Clausen, T., Dearlove, C., and P. Philippe, "The Optimized Link State Routing Protocol version 2", work in progress draft-ietf-manet-olsrv2-10.txt, September 2009.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC5444] Clausen, T., Dearlove, C., Dean, J., and C. Adjih,

"Generalized MANET Packet/Message Format", RFC 5444, February 2009.

[SMF] Macker, J., "Simplified Multicast Forwarding", work in progress draft-ietf-manet-smf-09.txt, July 2009.

Authors' Addresses

Ulrich Herberg
LIX, Ecole Polytechnique
91128 Palaiseau Cedex,
France

Phone: +33-1-6933-4126
Email: ulrich@herberg.name
URI: http://www.herberg.name/

Thomas Heide Clausen
LIX, Ecole Polytechnique
91128 Palaiseau Cedex,
France

Phone: +33 6 6058 9349
Email: T.Clausen@computer.org
URI: http://www.thomasclausen.org/