Internet Engineering Task Force (IETF)
Request for Comments: 7186
Category: Informational
ISSN: 2070-1721

J. Yi
LIX, Ecole Polytechnique
U. Herberg
Fujitsu Laboratories of America
T. Clausen
LIX, Ecole Polytechnique

April 2014

Security Threats for the Neighborhood Discovery Protocol (NHDP)

Abstract

This document analyzes common security threats of the Neighborhood Discovery Protocol (NHDP) and describes their potential impacts on Mobile Ad Hoc Network (MANET) routing protocols using NHDP. This document is not intended to propose solutions to the threats described.

Status of This Memo

This document is not an Internet Standards Track specification; it is published for informational purposes.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Not all documents approved by the IESG are a candidate for any level of Internet Standard; see Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc7186.

Table of Contents

1. Introduction 3
2. Terminology 4
3. NHDP Threat Overview 4
4. Detailed Threat Description 5
4.1. Jamming 5
4.2. Denial-of-Service Attack 5
4.3. Eavesdropping and Traffic Analysis 6
4.4. Incorrect HELLO Message Generation 7
4.4.1. Identity Spoofing 7
4.4.2. Link Spoofing 8
4.5. Replay Attack 9
4.6. Message Timing Attacks 9
4.6.1. Interval Time Attack 10
4.6.2. Validity Time Attack 10
4.7. Indirect Channel Overloading 10
4.8. Attack on Link Quality Update 11
5. Impact of Inconsistent Information Bases on Protocols using NHDP 12
5.1. MPR Calculation 12
5.1.1. Flooding Disruption due to Identity Spoofing 12
5.1.2. Flooding Disruption due to Link Spoofing 13
5.1.3. Broadcast Storm 14
5.2. Routing Loops 15
5.3. Invalid or Nonexistent Paths to Destinations 16
5.4. Data Sinkhole 16
6. Future Work 16
7. Security Considerations 17
8. Acknowledgments 18
9. References 18
9.1. Normative References 18
9.2. Informative References 18

1. Introduction

The Neighborhood Discovery Protocol (NHDP) [RFC6130] allows routers to acquire topological information up to two hops away from themselves, by way of periodic HELLO message exchanges. The information acquired by NHDP is used by other protocols, such as the Optimized Link State Routing Protocol version 2 (OLSRv2) [RFC7181] and Simplified Multicast Forwarding (SMF) [RFC6621]. The topology information, acquired by way of NHDP, serves these routing protocols by detecting and maintaining local 1-hop and 2-hop neighborhood information.

As 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 radio signals can be received as well as transmitted by any compatible wireless device within radio range, there is commonly no physical protection as otherwise known for wired networks. NHDP does not define any explicit security measures for protecting the integrity of the information it acquires; however, it suggests that the integrity protection be addressed in a fashion appropriate to the deployment of the network.

This document is based on the assumption that no additional security mechanism such as IPsec is used in the IP layer, as not all MANET deployments may be able to accommodate such common IP protection mechanisms (e.g., because of limited resources of MANET routers). The document analyzes possible attacks on and misconfigurations of NHDP and outlines the consequences of such attacks/misconfigurations to the state maintained by NHDP in each router (and, thus, made available to protocols using this state).

This document is not intended to propose solutions to the threats described. [RFC7185] provides further information on how to enable integrity protection to NHDP, which can help mitigating the threats described related to identity spoofing.

It should be noted that many NHDP implementations are configurable, and so an attack on the configuration system (such as [RFC6779]) can be used to adversely affect the operation of an NHDP implementation.

The NHDP MIB module [RFC6779] might help monitoring some of the security attacks mentioned in this document. [MGMT-SNAP] provides a snapshot of OLSRv2-routed MANET management as currently deployed, while [MANET-MGMT] is intended to provide specific guidelines on MANET network management considering the various MIB modules that have been written.

2. Terminology

This document uses the terminology and notation defined in "Generalized Mobile Ad Hoc Network (MANET) Packet/Message Format" [RFC5444], "Mobile Ad Hoc Network (MANET) Neighborhood Discovery Protocol (NHDP)" [RFC6130], and "Internet Security Glossary, Version 2" [RFC4949].

Additionally, this document introduces the following terminology:

NHDP router: A MANET router, running NHDP as specified in [RFC6130].

Attacker: A device that is present in the network and intentionally seeks to compromise the information bases in NHDP routers.

Compromised NHDP router: An attacker that is present in the network and generates syntactically correct NHDP control messages. Control messages emitted by a compromised NHDP router may contain additional information, or omit information, as compared to a control message generated by a non-compromised NHDP router located in the same topological position in the network.

Legitimate NHDP router: An NHDP router that is not a compromised NHDP router.

3. NHDP Threat Overview

NHDP defines a HELLO messages exchange, enabling each NHDP router to acquire topological information describing its 1-hop and 2-hop neighbors, and specifies information bases for recording this information.

An NHDP router periodically transmits HELLO messages using a link-local multicast on each of its interfaces with a hop-limit of 1 (i.e., HELLOs are never forwarded). In these HELLO messages, an NHDP router announces the IP addresses as heard, symmetric, or lost neighbor interface addresses.

An Attacker has several ways of harming this neighbor discovery process: it can announce "wrong" information about its identity, postulate nonexistent links, and replay HELLO messages. These attacks are presented in detail in Section 4.

The different ways of attacking an NHDP deployment may eventually lead to inconsistent information bases, not accurately reflecting the correct topology of the MANET. The consequence is that protocols using NHDP will base their operation on incorrect information, causing routing protocols to not be able to calculate correct (or

any) paths, degrade the performance of flooding operations based on reduced relay sets, etc. These consequences to protocols using NHDP are described in detail in Section 5.

4. Detailed Threat Description

For each threat, a description of the mechanism of the corresponding attack is given, followed by a description of how the attack affects NHDP. The impacts from each attack on protocols using NHDP are given in Section 5.

For simplicity in the description, the examples given assume that NHDP routers have a single interface with a single IP address configured. All the attacks apply, however, for NHDP routers with multiple interfaces and multiple addresses as well.

4.1. Jamming

One vulnerability, common for all protocols operating a wireless ad hoc network, is that of "jamming", i.e., that a device 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. Jamming is a form of interference and overload with the threat consequence of disruption [RFC4593].

Depending on lower layers, this may not affect transmissions: HELLO messages from an NHDP router with "jammed" interfaces may be received by other NHDP routers. As NHDP identifies whether a link to a neighbor is unidirectional or bidirectional, a routing protocol that uses NHDP for neighborhood discovery may ignore a link from a jammed NHDP router to a non-jammed NHDP router. The jammed router (a router with jammed carrier) would appear simply as "disconnected" for the unjammed part of the network, which is able to maintain accurate topology maps.

If a considerable amount of HELLO messages are lost or corrupted due to collisions caused by a jamming attack, neighbor NHDP routers are not able to establish links between themselves any more. Thus, NHDP will present empty information bases to the protocols using it.

4.2. Denial-of-Service Attack

A denial-of-service (DoS) attack can be a result of misconfiguration of legitimate NHDP routers (e.g., very short HELLO transmission interval) or malicious behavior of compromised NHDP routers [ACCT2012], so-called Byzantine routers [RFC4593]. DoS is a form of interference and overload with the threat consequence of disruption [RFC4593].

By transmitting a huge amount of HELLO messages in a short period of time, NHDP routers can increase channel occupation as described in Section 4.1. Furthermore, a compromised NHDP router can spoof a large amount of different IP addresses and send HELLOs to its neighbors to fill their Link/Neighbor Sets. This may result in memory overflow, and it makes the processing of legitimate HELLO messages impossible. A compromised NHDP router can also use link spoofing in its HELLO messages, generating huge 2-hop Sets in adjacent NHDP routers and therefore potentially a memory overflow. Moreover, protocols such as SMF and OLSRv2, using the 2-hop information for multipoint relay (MPR) calculation, may exhaust the available computational resources of the router if the Neighbor Set and 2-hop Sets have too many entries.

By exhausting the memory, CPU, and/or channel resources of a router in a DoS attack or a misconfiguration, NHDP routers may not be able to accomplish their specified tasks of exchanging 1-hop and 2-hop neighborhood information, and thereby disturbing the operation of routing protocols using NHDP.

In some MANETs, the routers are powered by battery. Another consequence of a DoS attack in such networks is that the power will be drained quickly by unnecessary processing, transmitting, and receiving of messages.

4.3. Eavesdropping and Traffic Analysis

Eavesdropping, sometimes referred to as sniffing, is a common and easy passive attack in a wireless environment. Once a packet is transmitted, any adjacent NHDP router can potentially obtain a copy, for immediate or later processing. Neither the source nor the intended destination can detect this. A malicious NHDP router can eavesdrop on the NHDP message exchange and thus learn the local topology. It may also eavesdrop on data traffic to learn source and destination addresses of data packets, or other header information, as well as the packet payload.

Eavesdropping does not pose a direct threat to the network or to NHDP, in as much as that it does not alter the information recorded by NHDP in its information bases and presented to other protocols. However, eavesdropping can provide network information required for enabling other attacks, such as the identity of communicating NHDP routers, detection of link characteristics, and NHDP router configuration. The compromised NHDP routers may use the obtained information to launch subsequent attacks, and they may also share NHDP routing information with other NHDP or non-NHDP entities. [RFC4593] would categorize the threat consequence as disclosure.

Traffic analysis normally follows eavesdropping, which is the process of intercepting messages in order to deduce information from communication patterns. It can be performed even when HELLO messages are encrypted (encryption is not a part of NHDP), for example:

- Triggered HELLO messages: an attacker could figure out that messages are triggered and determine that there was a change of symmetric neighbors of an NHDP router sending the HELLO (as well get the frequency).

- Message size: the message grows exactly by x bytes per neighbor. Depending on which cipher is used for the encryption, some information about the size could be inferred, and thus the number of neighbors could be guessed.

[RFC4593] would categorize the threat consequence as disclosure.

4.4. Incorrect HELLO Message Generation

An NHDP router performs two distinct tasks: it periodically generates HELLO messages, and it processes incoming HELLO messages from neighbor NHDP routers. This section describes security attacks involving the HELLO generation.

4.4.1. Identity Spoofing

Identity spoofing implies that a compromised NHDP router sends HELLO messages, pretending to have the identity of another NHDP router, or even a router that does not exist in the networks. A compromised NHDP router can accomplish this by using an IP address, which is not its own, in an address block of a HELLO message, and associating this address with a LOCAL_IF Address Block TLV [IJNSIA2010].

An NHDP router receiving that HELLO message from a neighbor will assume that it originated from the NHDP router with the spoofed 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 a symmetric neighbor after another HELLO exchange).

Identity spoofing is particularly harmful if a compromised NHDP router spoofs the identity of another NHDP 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 an NHDP router. [RFC4593] would categorize the threat consequences as disclosure and deception.

Figure 1 depicts a simple example. In that example, NHDP router A is in radio range of NHDP router C, but not of the compromised NHDP router X. If X spoofs the address of A, that can lead to conflicts for a routing protocol that uses NHDP, and therefore for wrong path calculations as well as incorrect data traffic forwarding.

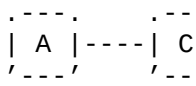

Figure 1

Figure 2 depicts another example. In this example, NHDP router A is two hops away from NHDP router C, reachable through NHDP router B. If the compromised NHDP router X spoofs the address of A, NHDP router D will take A as its 1-hop neighbor, and C may think that A is indeed reachable through D.

Figure 2

4.4.2. Link Spoofing

Similar to identity spoofing, link spoofing implies that a compromised NHDP router sends HELLO messages, signaling an incorrect set of neighbors. This is sometimes referred to as falsification [RFC4593], and in NHDP it may take either of two forms:

- A compromised NHDP router can postulate addresses of non-present neighbor NHDP routers in an address block of a HELLO, associated with LINK_STATUS TLVs.

- A compromised NHDP router can "ignore" otherwise existing neighbors by not advertising 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 NHDP router ignores existing neighbors in its advertisements, links will be missing in the information bases maintained by other routers, and there may not be any connectivity for these NHDP routers to or from other NHDP routers in the MANET.

- On the other hand, if the compromised NHDP router advertises nonexistent links, this will lead to inclusion of topological information in the information base, describing nonexistent links in the network (which, then, may be used by other protocols using NHDP in place of other, existing, links).

[RFC4593] would categorize the threat consequences as usurpation, deception, and disruption.

4.5. Replay Attack

A replay attack implies that control traffic from one region of the network is recorded and replayed in a different region at (almost) the same time, or in the same region at a different time. This may, for example, happen when two compromised NHDP routers collaborate on an attack, one recording traffic in its proximity and tunneling it to the other compromised NHDP router, which replays the traffic. In a protocol where links are discovered by testing reception, this will result in extraneous link creation (basically, a "virtual" link between the two compromised NHDP routers will appear in the information bases of neighboring NHDP routers). [RFC4593] would categorize this as a falsification and interference threat with threat consequences of usurpation, deception, and disruption.

While this situation may result from an attack, it may also be intentional: if data traffic is also relayed over the "virtual" link, the link being detected is indeed valid for use. This is, for instance, used in wireless repeaters. If data traffic is not carried over the virtual link, an imaginary, useless link between the two compromised NHDP routers has been advertised and is being recorded in the information bases of their neighboring NHDP routers.

Compared to incorrect HELLO message attacks described in Section 4.4, the messages used in replay attacks are legitimate messages sent out by (non-malicious) NHDP routers and replayed at a later time or different locality by malicious routers. This makes this kind of attack harder to be detect and to counteract; integrity checks cannot help in this case, as the original message's Integrity Check Value (ICV) was correctly calculated.

4.6. Message Timing Attacks

In NHDP, each HELLO message contains a "validity time" (the amount of time that information in that control message should be considered valid before being discarded) and may contain an "interval time" field (the amount of time until the next control message of the same type should be expected) [RFC5497].

4.6.1. Interval Time Attack

A use of the expected interval between two successive HELLO messages is for determining the link quality in NHDP: if messages are not received within the expected intervals (e.g., a certain fraction of messages are missing), then this may be used to exclude a link from being considered as useful, even if (some) bidirectional communication has been verified. If a compromised NHDP router X spoofs the identity of an existing NHDP router A and sends HELLOs indicating a low interval time, an NHDP router B receiving this HELLO will expect the following HELLO to arrive within the interval time indicated. If that expectation is not met, the link quality for the link A-B will be decreased. Thus, X may cause NHDP router B's estimate of the link quality for the link A-B to fall below the minimum considered useful, so the link would not be used [CPSCOM2011]. [RFC4593] would categorize the threat consequence as usurpation.

4.6.2. Validity Time Attack

A compromised NHDP router X can spoof the identity of an NHDP router A and send a HELLO using a low validity time (e.g., 1 ms). A receiving NHDP router B will discard the information upon expiration of that interval, i.e., a link between NHDP router A and B will be "torn down" by X. The sending of a low validity time can be caused by intended malicious behaviors or simply misconfiguration in the NHDP routers. [RFC4593] would categorize the threat consequence as usurpation.

4.7. Indirect Channel Overloading

Indirect Channel Overloading is when a compromised NHDP router X by its actions causes other legitimate NHDP routers to generate inordinate amounts of control traffic. This increases channel occupation and the overhead in each receiving NHDP router that processes this control traffic. With this traffic originating from legitimate NHDP routers, the malicious device may remain undetected in the wider network. It is a form of interference and overload with the threat consequence of disruption [RFC4593].

Figure 3 illustrates Indirect Channel Overloading with NHDP. A compromised NHDP router X advertises a symmetric spoofed link to the nonexistent NHDP router B (at time t0). Router A selects X as MPR upon reception of the HELLO then triggers a HELLO at t1. Overhearing this triggered HELLO, the attacker sends another HELLO at t2, advertising the link to B as lost; this causes NHDP router A to

deselect the attacker as MPR, and to send another triggered message at t3. The cycle may be repeated, where the link X-B is advertised alternately as LOST and SYM.

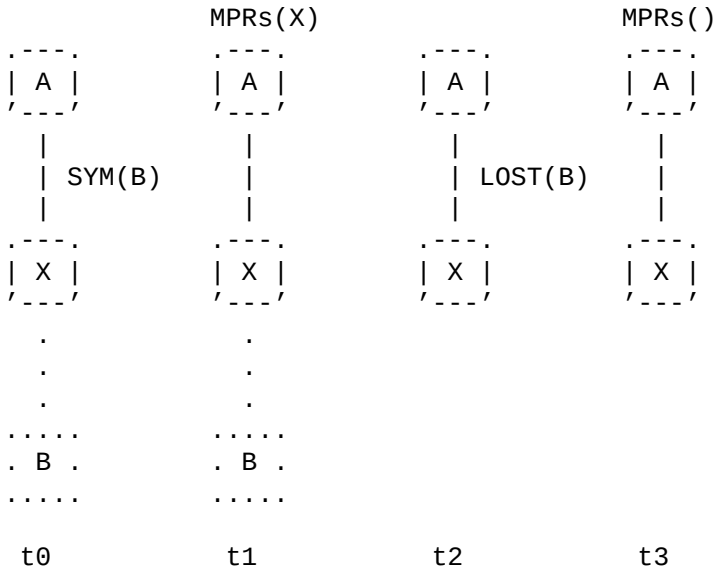

Figure 3

4.8. Attack on Link Quality Update

According to NHDP [RFC6130]:

> Link quality is a mechanism whereby a router MAY take considerations other than message exchange into account for determining when a link is and is not a candidate for being considered as HEARD or SYMMETRIC. As such, it is a "link admission" mechanism.

Section 14.4 of NHDP [RFC6130] then lists several examples of which information can be used to update link quality. One of the listed examples uses packet exchanges between neighbor routers (as described in [RFC5444]), e.g., an NHDP router may update the link quality of a neighbor based on receipt or loss of packets if they include a sequential packet sequence number.

NHDP does not specify how to acquire link quality updates normatively; however, attack vectors may be introduced if an implementation chooses to calculate link quality based on packet sequence numbers. The consequences of such threats would depend on specific implementations. For example, if the link quality update is based on a sequential packet sequence number from neighbor routers, a

compromised NHDP router can spoof packets appearing to be from another legitimate NHDP router that skips some packet sequence numbers. The NHDP router receiving the spoofed packets may degrade the link quality as it appears that several packets have been dropped. Eventually, the router may remove the neighbor when the link quality drops below HYST_REJECT.

5. Impact of Inconsistent Information Bases on Protocols using NHDP

This section describes the impact on protocols that use NHDP when NHDP fails to obtain and represent accurate information, possibly as a consequence of the attacks described in Section 4. This description emphasizes the impacts on the MANET protocols OLSRv2 [RFC7181] and SMF [RFC6621].

5.1. MPR Calculation

MPR selection (as used in [RFC7181] and [RFC6621], for example) uses information about a router's 1-hop and 2-hop neighborhood, assuming that (i) this information is accurate, and (ii) each 1-hop neighbor is apt to act as MPR, depending on the willingness it reports. Thus, a compromised NHDP router may seek to manipulate the 1-hop and 2-hop neighborhood information in a router so as to cause the MPR selection to fail, leading to a flooding disruption of traffic control messages. This can result in incomplete topology advertisement or can degrade the optimized flooding to classical flooding.

5.1.1. Flooding Disruption due to Identity Spoofing

A compromised NHDP router can spoof the identify of other routers in order to disrupt the MPR selection, so as to prevent certain parts of the network from receiving flooded traffic [IJNSIA2010].

In Figure 4, a compromised NHDP router X spoofs the identity of B. The link between X and C is correctly detected and listed in X's HELLOs. Router A will receive HELLOs indicating links from B:{B-E}, X:{X-C, X-E}, and D:{D-E, D-C}, respectively. For router A, X and D are equal candidates for MPR selection. To make sure the X can be selected as MPR for router A, X can set its willingness to the maximum value.

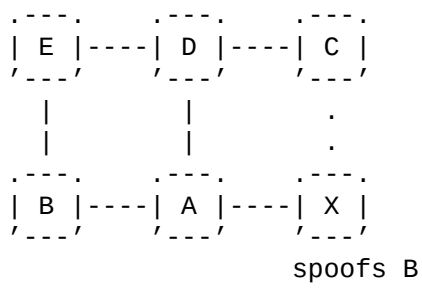

Figure 4

If B and X (i) accept MPR selection and (ii) forward flooded traffic as if they were both B, identity spoofing by X is harmless. However, if X does not forward flooded traffic (i.e., does not accept MPR selection), its presence entails flooding disruption: selecting B over D renders C unreachable by flooded traffic.

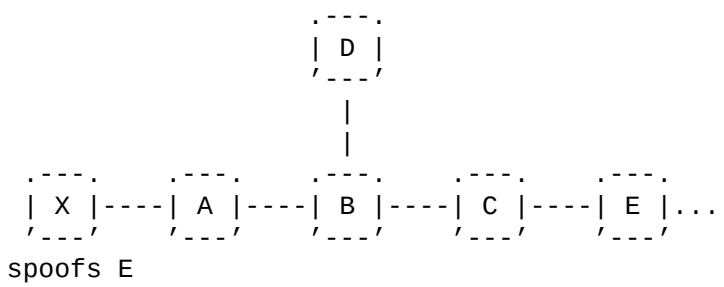

Figure 5

In Figure 5, the compromised NHDP router X spoofs the identity of E, i.e., routers A and C both receive HELLOs from a router identifying itself as E. For router B, routers A and C present the same neighbor sets and are equal candidates for MPR selection. If router B selects only router A as MPR, C will not relay flooded traffic from B or transiting via B, and router X (and routers to the "right" of it) will not receive flooded traffic.

5.1.2. Flooding Disruption due to Link Spoofing

A compromised NHDP router can also spoof links to other NHDP routers, thereby making itself appear as the most appealing candidate to be MPR for its neighbors, possibly to the exclusion of other NHDP routers in the neighborhood. (In particular, this can occur if the compromised NHDP router spoofs links to all other NHDP routers in the neighborhood, plus to one NHDP router outside the neighborhood.) By thus excluding other legitimate NHDP routers from being selected as MPR, the compromised NHDP router will receive and be expected to

relay all flooded traffic (e.g., traffic control messages in OLSRv2 or data traffic in SMF) that it can then drop or otherwise manipulate.

In the network in Figure 6, the compromised NHDP router X spoofs links to the existing router C, as well as to a fictitious W. Router A receives HELLOs from X and B, reporting X: {X-C, X-W}, B: {B-C}. All else being equal, X appears a better choice for MPR than B, as X appears to cover all neighbors of B, plus W.

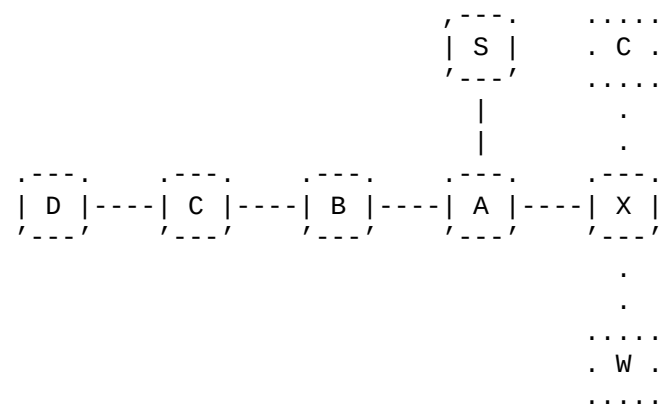

Figure 6

As router A will not select B as MPR, B will not relay flooded messages received from router A. The NHDP routers on the left of B (starting with C) will, thus, not receive any flooded messages from router A or transiting router A (e.g., a message originating from S).

5.1.3. Broadcast Storm

A compromised NHDP router may attack the network by attempting to degrade the performance of optimized flooding algorithms so as to be equivalent to classic flooding. This can be achieved by forcing an NHDP router into choosing all its 1-hop neighbors as MPRs. In MANETs, a broadcast storm caused by classic flooding is a serious problem that can result in redundancy, contention, and collisions [MOBICOM99].

As shown in Figure 7, the compromised NHDP router X spoofs the identity of NHDP router B and, spoofs a link to router Y {B-Y} (Y does not have to exist). By doing so, the legitimate NHDP router A has to select the legitimate NHDP router B as its MPR in order for it to reach all its 2-hop neighbors. The compromised NHDP router Y can

perform this identity-and-link spoofing for all of NHDP router A's 1-hop neighbors, thereby forcing NHDP router A to select all its neighbors as MPR and disabling the optimization sought by the MPR mechanism.

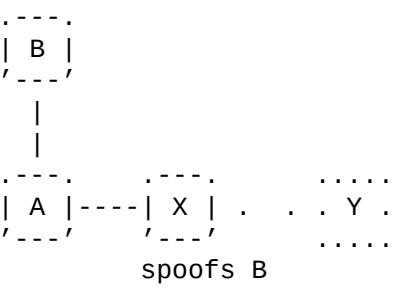

Figure 7

5.2. Routing Loops

Inconsistent information bases, provided by NHDP to other protocols, can also cause routing loops. In Figure 8, the compromised NHDP router X spoofs the identity of NHDP router E. NHDP router D has data traffic to send to NHDP router A. The topology recorded in the information base of router D indicates that the shortest path to router A is {D->E->A}, because of the link {A-E} reported by X. Therefore, the data traffic will be routed to NHDP router E. As the link {A-E} does not exist in NHDP router E's information bases, it will identify the next hop for data traffic to NHDP router A as being NHDP router D. A loop between the NHDP routers D and E is thus created.

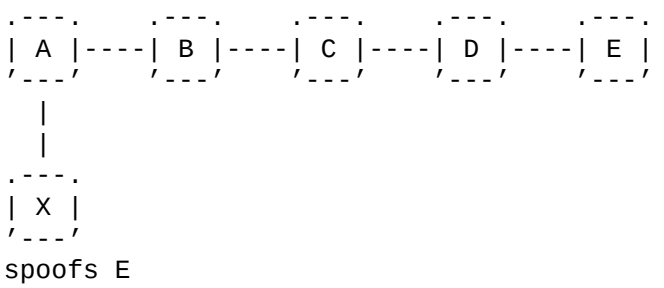

Figure 8

5.3. Invalid or Nonexistent Paths to Destinations

By reporting inconsistent topology information in NHDP, the invalid links and routers can be propagated as link state information with traffic control messages and results in route failure. As illustrated in Figure 8, if NHDP router B tries to send data packets to NHDP router E, it will choose router A as its next hop, based on the information about the nonexistent link {A-E} reported by the compromised NHDP router X.

5.4. Data Sinkhole

With the ability to spoof multiple identities of legitimate NHDP routers (by eavesdropping, for example), the compromised NHDP router can represent a "data sinkhole" for its 1-hop and 2-hop neighbors. Data packets that come across its neighbors may be forwarded to the compromised NHDP router instead of to the real destination. The packet can then be dropped, manipulated, duplicated, etc., by the compromised NHDP router. As shown in Figure 8, if the compromised NHDP router X spoofs the identity of NHDP router E, all the data packets to E that cross NHDP routers A and B will be sent to NHDP router X, instead of to E.

6. Future Work

This document does not propose solutions to mitigate the security threats described in Section 4. However, this section aims at driving new work by suggesting which threats discussed in Section 4 could be addressed by deployments or applications.

- Section 4.1: Jamming - If a single router or a small area of the MANET is jammed, protocols could be specified that increase link metrics in NHDP for the jammed links. When a routing protocol such as OLSRv2 uses NHDP for neighborhood discovery, other paths leading "around" the jammed area would be preferred, and therefore would mitigate the threat to some extent.

- Section 4.2: DoS - A DoS attack using a massive amount of HELLO messages can be mitigated by admitting only trusted routers to the network. [RFC7185] specifies a mechanism for adding Integrity Check Values (ICVs) to HELLO messages and therefore providing an admittance mechanism for NHDP routers to a MANET. (Note that adding ICVs creates a new DoS attack vector, as ICV verification requires CPU and memory resources.) However, using ICVs does not address the problem of compromised routers. Detecting compromised routers could be addressed in new work. [RFC7185] mandates implementation of a security mechanism that is based on shared keys and makes excluding single compromised routers difficult;

work could be done to facilitate revocation mechanisms in certain MANET use cases where routers have sufficient capabilities to support asymmetric keys.

- Section 4.3: Eavesdropping - [RFC7185] adds ICVs to HELLO messages but does not encrypt them. Therefore, eavesdropping of control traffic is not mitigated. Future work could provide encryption of control traffic for sensitive MANET topologies. Note that, other than using a single shared secret key, providing encryption of traffic among a set of neighbors (when that set is potentially undetermined) is nontrivial, especially without multiplying overheads. With traffic analysis, attackers could still deduce the network information like HELLO message triggering and HELLO message size, even though the HELLO messages are encrypted.

- Section 4.4.2: Link spoofing - [RFC7185] provides certain protection against link spoofing, but an NHDP router has to "trust" the originator of a HELLO that the advertised links are correct. For example, if a router A reports a link to B, routers receiving HELLOs from A have to trust that B is actually a (symmetric) neighbor of A. New protocol work could address protection of links without overly increasing the space and time overheads. An immediate suggestion for deployments is to protect routers against being compromised and to distribute keys only to trusted routers.

- Section 4.5: Replay Attacks - [RFC7185] uses ICVs and timestamps to provide some protection against replay attacks. It is still feasible to replay control messages within a limited time. A suggestion for deployments is to provide time synchronization between routers. New work could provide time synchronization mechanisms for certain MANET use cases or specify a mechanism using nonces instead of timestamps in HELLO messages.

- Section 4.4.1: Identity spoofing; Section 4.6: Message timing attacks; Section 4.7: Indirect channel overloading; and Section 4.8: Attack on link quality update - [RFC7185] provides protection against these attacks, assuming the routers are not compromised.

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. Acknowledgments

The authors would like to gratefully acknowledge the following people for valuable comments and technical discussions: Teco Boot, Henning Rogge, Christopher Dearlove, John Dowdell, Joseph Macker, and all the other participants of the IETF MANET working group.

9. References

9.1. Normative References

[RFC5444] Clausen, T., Dearlove, C., Dean, J., and C. Adjih, "Generalized Mobile Ad Hoc Network (MANET) Packet/Message Format", RFC 5444, February 2009.

[RFC5497] Clausen, T. and C. Dearlove, "Representing Multi-Value Time in Mobile Ad Hoc Networks (MANETs)", RFC 5497, March 2009.

[RFC6130] Clausen, T., Dearlove, C., and J. Dean, "Mobile Ad Hoc Network (MANET) Neighborhood Discovery Protocol (NHDP)", RFC 6130, April 2011.

9.2. Informative References

[ACCT2012] Jhaveri, R. and S. Patel, "DoS Attacks in Mobile Ad Hoc Networks: A Survey", Second International Conference on Advanced Computing & Communication Technologies (ACCT), January 2012.

[CPSCOM2011] Yi, J., Clausen, T., and U. Herberg, "Vulnerability Analysis of the Simple Multicast Forwarding (SMF) Protocol for Mobile Ad Hoc Networks", Proceedings of the IEEE International Conference on Cyber, Physical, and Social Computing (CPSCom), October 2011.

[IJNSIA2010] Herberg, U. and T. Clausen, "Security Issues in the Optimized Link State Routing Protocol version 2", International Journal of Network Security & Its Applications, April 2010.

[MANET-MGMT] Nguyen, J., Cole, R., Herberg, U., Yi, J., and J. Dean, "Network Management of Mobile Ad hoc Networks (MANET): Architecture, Use Cases, and Applicability", Work in Progress, February 2013.

[MGMT-SNAP]
Clausen, T. and U. Herberg, "Snapshot of OLSRv2-Routed MANET Management", Work in Progress, February 2014.

[MOBICOM99]
Ni, S., Tseng, Y., Chen, Y., and J. Sheu, "The Broadcast Storm Problem in a Mobile Ad Hoc Network", Proceedings of the 5th annual ACM/IEEE international conference on Mobile computing and networking, 1999.

[RFC4593] Barbir, A., Murphy, S., and Y. Yang, "Generic Threats to Routing Protocols", RFC 4593, October 2006.

[RFC4949] Shirey, R., "Internet Security Glossary, Version 2", RFC 4949, August 2007.

[RFC6621] Macker, J., "Simplified Multicast Forwarding", RFC 6621, May 2012.

[RFC6779] Herberg, U., Cole, R., and I. Chakeres, "Definition of Managed Objects for the Neighborhood Discovery Protocol", RFC 6779, October 2012.

[RFC7181] Clausen, T., Dearlove, C., Jacquet, P., and U. Herberg, "The Optimized Link State Routing Protocol Version 2", RFC 7181, April 2014.

[RFC7185] Herberg, U., Dearlove, C., and T. Clausen, "Integrity Protection for the Neighborhood Discovery Protocol (NHDP) and Optimized Link State Routing Protocol Version 2 (OLSRv2)", RFC 7185, April 2014.

Authors' Addresses

Jiazi Yi
LIX, Ecole Polytechnique
91128 Palaiseau Cedex
France

Phone: +33 1 77 57 80 85
EMail: jiazi@jiaziyi.com
URI: http://www.jiaziyi.com/

Ulrich Herberg
Fujitsu Laboratories of America
1240 E Arques Ave
Sunnyvale, CA 94085
USA

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/