Mobile Ad hoc Networking (MANET)
Internet-Draft
Intended status: Informational
Expires: September 13, 2012

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

March 12, 2012

Security Threats for NHDP
draft-herberg-manet-nhdp-sec-threats-01

Abstract

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

Status of this Memo

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

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

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."

This Internet-Draft will expire on September 13, 2012.

Copyright Notice

Table of Contents

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 OLSRv2 [OLSRv2] and SMF [SMF]. The topology information, acquired by way of NHDP, serves these routing protocols for calculating paths to all destinations in the MANET, for relay set selection for network-wide transmissions, etc.

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 wireless radio waves can be captured as well as transmitted by any wireless device within radio range, there is commonly no physical protection as otherwise known for wired networks. [RFC6130] does not define any explicit security measures 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 analyses possible attacks on NHDP and outlines the consequences of such attacks to the state maintained by NHDP in each router (and, thus, made available to protocols using this state).

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 [RFC2119].

This document uses the terminology and notation defined in [RFC5444] and [RFC6130].

Additionally, this document introduces the following terminology:

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

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

Compromised NHDP Router: An attacker, present in the network and which 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-compromized NHDP router located

in the same topological position in the network.

Legitimate NHDP Router: An NHDP router, which is not a Compromised NHDP Router.

3. NHDP Threat Overview

[RFC6130] 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 running [RFC6130] 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 adversary has several ways of harming this 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 may eventually lead to inconsistent information bases, not accurately reflecting the correct topology of the MANET. The consequence hereof 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, described in the below, 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, 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.

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 [RFC6130] identifies and uses only bi-directional links, a link from a jammed NHDP router to a non-jammed NHDP router would not be considered, and the jammed NHDP router appear simply as "disconnected" for the un-jammed part of the network - which is able to maintain accurate topology maps.

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

4.2. Eavesdropping

Eavesdropping 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 nor 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 using it, but it can provide network information required for enabling other attacks, such as the identity of communicating NHDP routers, link characteristic, NHDP router configuration, etc.

4.3. Incorrect HELLO Message Generation

An NHDP router running [RFC6130] 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.

4.3.1. Identity Spoofing

Identity spoofing implies that a Compromised NHDP router sends HELLO messages, pretending to have the identity of another NHDP router. A Compromised NHDP router can accomplish this by using another NHDP router's IP address in an address block of a HELLO message, and associating this address with a LOCAL_IF Address Block TLV.

An NHDP router receiving the 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 symmetric neighbor after another HELLO exchange).

Identity spoofing is particular 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. Figure 1 depicts a simple example. In that example, NHDP router A is in radio range of C, but not of the Compromised NHDP router 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.

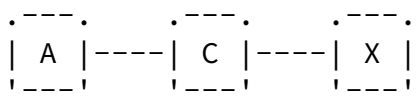

Figure 1

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

Figure 2

4.3.2. Link Spoofing

Similar to identity spoofing, link spoofing implies that a Compromised NHDP router sends HELLO messages, signaling an incorrect set of neighbors. This 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 to or from these NHDP routers to others NHDP routers in the MANET. If, on the other hand, the Compromised NHDP router advertises non-existing links, this will lead to inclusion of topological information in the information base, describing non-existing links in the network (which, then, may be used by other protocols using NHDP in place of other, existing, links).

4.4. Replay Attack

A replay attack implies that 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 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).

While this situation may result from an attack, it may also be intentional: if data-traffic also is 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.

Replay attacks can be especially damaging if coupled with spoofing and tampering with sequence numbers in the replayed messages, potentially destroying some important topology information in NHDP routers all over the network, as described in Section 4.5.

4.5. Sequence Number Attack

[RFC6130] uses message sequence numbers, to avoid processing and forwarding the same message more than once. An attack may consist of a Compromised NHDP router, spoofing the identity of another Legitimate NHDP router in the network and transmitting a large number of HELLO messages, each with different message sequence numbers. Subsequent HELLOs with the same sequence numbers, originating from theLegitimate NHDP router whose identity was spoofed, would hence be ignored, until eventually information concerning these "spoofed" HELLO messages expires.

As illustrated in Figure 1, if the Compromised NHDP router X spoofs the identify of NHDP router A, and broadcasts several HELLO messages, all the valid HELLO messages sent by A with the same sequence numbers will be discarded by C, until the information concerning these HELLOs expire.

4.6. Message Timing Attacks

In [RFC6130], each HELLO message contains a "validity time" and may contain an "interval time" field, identifying the time for which information in that control message should be considered valid until discarded, and the 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 [RFC6130]: 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) bi-directional 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 - or otherwise, decrease the link quality for the link A-B. Thus, X may cause NHDP router B's estimate of the link quality for the link A-B to fall below the limit, where it is no longer considered as useful and, thus, not used.

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.

4.7. Indirect Jamming

Indirect jamming 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 processing this control traffic. With this traffic originating from Legitimate NHDP routers, the malicious device may remain undetected to the wider network.

Figure 3 illustrates indirect jamming of [RFC6130]. A Compromised NHDP router X advertises a symmetric spoofed link to the non-existing NHDP router B (at time t0). Router A selects X as MPR upon reception of the HELLO, and will trigger a HELLO at t1. Overhearing this triggered HELLO, the attacker sends another HELLO at t2, advertising the link to B as lost, which leads to NHDP router A deselecting the attacker as MPR, and another triggered message at t3. The cycle may be repeated, alternating advertising the link X-B as LOST and SYM.

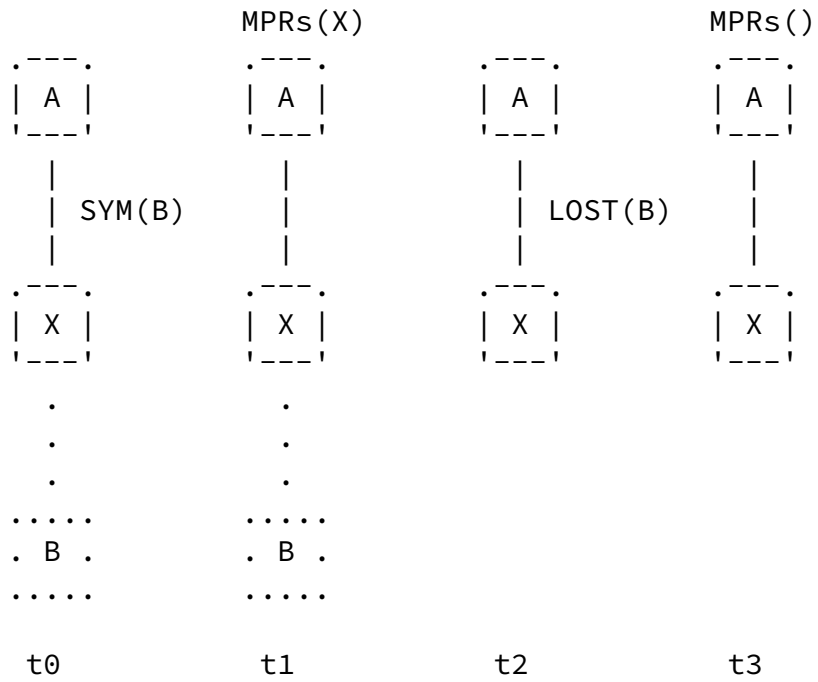

Figure 3

5. Impact of inconsistent Information Bases on Protocols using NHDP

This section describes the impact on protocols, using NHDP, of NHDP failing 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 [OLSRv2], and

SMF [SMF].

5.1. MPR Calculation

MPR selection (as used in e.g., [OLSRv2] and [SMF]) uses information about a router's 1-hop and 2-hop neighborhood, assuming that (i) this information is accurate, and (ii) all 1-hop neighbors are apt to act as as MPR, depending on the willingness they report. Thus, a Compromised NHDP router will seek to manipulate the 1-hop and 2-hop neighborhood information in a router such as to cause the MPR selection to fail, leading to a flooding disruption of TC messages.

5.1.1. Flooding Disruption due to Identity Spoofing

A Compromised NHDP router can spoof the identify of other routers, to disrupt the MPR selection, so as to cache certain parts of the network from the flooding traffic.

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, respectively B:{B-E}, X:{X-C, X-E}, and D:{D-E, D-C}. 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.

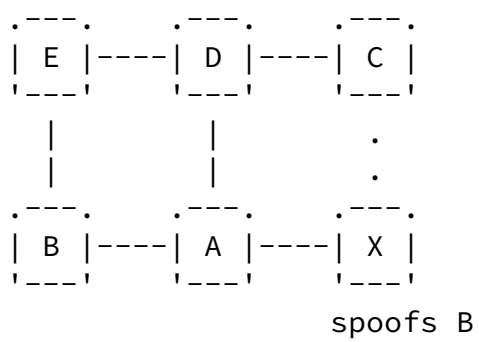

Figure 4

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.

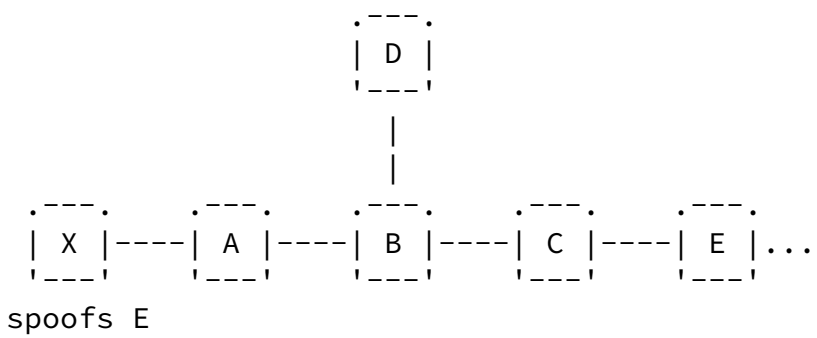

Figure 5

In Figure 5, the Compromised NHDP router X spoofs the identity of E, i.e.,router A and C both receive HELLOs from a router identifying as E. For router B, 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 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, and thereby makes itself appear as the most appealing candidate of MPR for its neighbors, possibly to the exclusion of other NHDP routers in the neighborhood (this, in particular, if the Compromised NHDP router spoof links to all other NHDP routers in the neighborhood, plus to one other NHDP router). 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., TC messages in OLSRv2 or data traffic in SMF) - which 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 as MPR than B, as X appears to cover all neighbors of B, plus W.

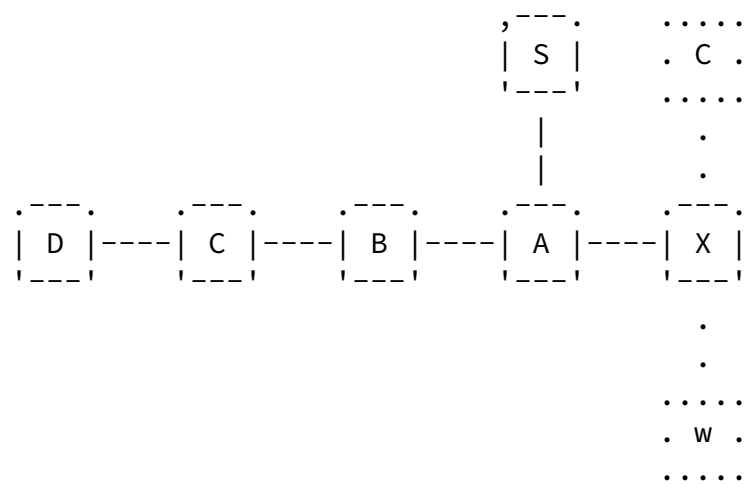

Figure 6

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 or transiting NHDP router A (e.g., a message originating from S).

5.1.3. Broadcast Storm

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 which can result in redundancy, contention and collisions [broadcast-storm].

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

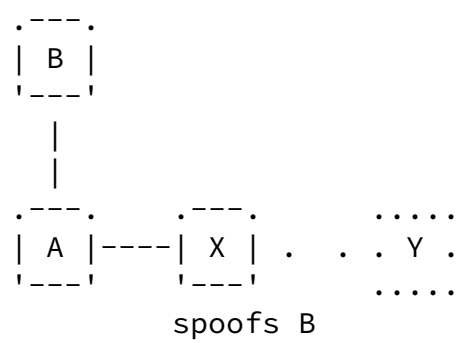

Figure 7

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 the 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.

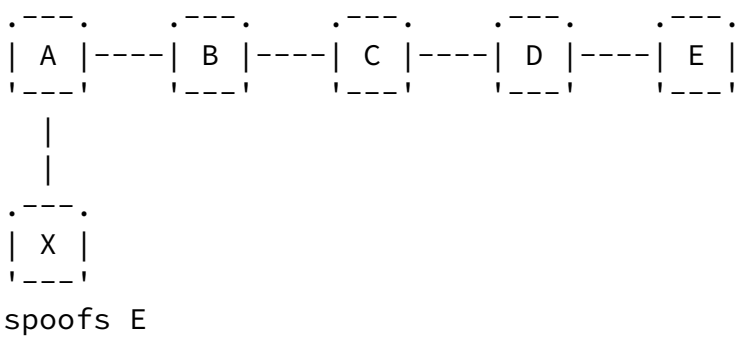

Figure 8

5.3. Invalid or Non-Existing Paths to Destinations

By reporting inconsistent topology information in NHDP, the invalid links/routers can be propagated as link state information with TC 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 of non-existing 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. 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.

7. IANA Considerations

This document contains no actions for IANA.

8. References

8.1. Normative References

[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.

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

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

8.2. Informative References

[OLSRv2] Clausen, T., Dearlove, C., Philippe, P., and U. Ulrich, "The Optimized Link State Routing Protocol version 2",

work in progress draft-ietf-manet-olsrv2-14.txt, March 2012.

[SMF] Macker, J., "Simplified Multicast Forwarding", work in progress draft-ietf-manet-smf-14.txt, March 2012.

[broadcast-storm] 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.

Authors' Addresses

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

Email: ulrich@herberg.name
URI: http://www.herberg.name/

Jiazi Yi
LIX, Ecole Polytechnique
91128 Palaiseau Cedex,
France

Phone: +33 1 69 33 40 31
Email: jiazi@jiaziyi@com
URI: http://www.jiaziyi.com/

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/