Network Working Group   T. Clausen
Internet-Draft   U. Herberg
Intended status: Informational
Expires: May 9, 2016   J. Yi
                                                LIX, Ecole Polytechnique
                                                        November 6, 2015

Security Threats for the Optimized Link State Routing Protocol version 2 (OLSRv2)

draft-ietf-manet-olsrv2-sec-threats-01

Abstract

This document analyzes common security threats of the Optimized Link State Routing Protocol version 2 (OLSRv2) and describes their potential impacts on Mobile Ad Hoc Network (MANET) operations. It then analyzes which of these security vulnerabilities can be mitigated when using the mandatory-to-implement security mechanisms for OLSRv2, and how the vulnerabilities are mitigated.

Table of Contents

1. Introduction

The Optimized Link State Routing Protocol version 2 (OLSRv2) [RFC5148], [RFC5444], [RFC5497], [RFC6130], [RFC7181], [RFC7182], [RFC7183], [RFC7187], [RFC7188] is a successor to OLSR [RFC3626] as a routing protocol for MANETs (Mobile Ad hoc NETworks). OLSRv2 retains the same basic algorithms as its predecessor, however offers various improvements, e.g., a modular and flexible architecture allowing extensions, such as for security, to be developed as add-ons to the basic protocol.

The developments reflected in OLSRv2 have been motivated by increased real-world deployment experiences, e.g., from networks such as FunkFeuer [FUNKFEUER], and the requirements presented for continued successful operation of these networks. With participation in such networks increasing (the FunkFeuer community network has, e.g., roughly 400 individual participants), operating with the assumption, that participants can be "trusted" to behave in a non-destructive way, is utopia. Taking the Internet as an example, as participation in the network increases and becomes more diverse, more efforts are required to preserve the integrity and operation of the network. Most SMTP-servers were, e.g., initially available for use by everyone on the Internet - with an increased populace on the Internet, attacks and abuses caused the recommended practice is today to require authentication and accounting for users of such SMTP servers [RFC5068].

As OLSRv2 often is 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.

A first step towards hardening against attacks disrupting the connectivity of a network, is to understand the vulnerabilities of routing protocol, managing the connectivity. This document therefore analyzes OLSRv2, to understand its inherent vulnerabilities and resiliences. The authors do not claim completeness of the analysis, but hope that the identified attacks, as presented, form a meaningful starting-point for developing secured OLSRv2 networks.

This document first describes security vulnerabilities to OLSRv2 when it is used without the mandatory-to-implement security mechanisms specified in Section 23.5 of [RFC7181]. It then analyzes which of these security vulnerabilities can be mitigated when using the mandatory-to-implement security mechanisms for OLSRv2, and how the vulnerabilities are mitigated. This separation is important since

other security mechanisms than the mandatory-to-implement ones may be used in a deployment, as stated in [RFC7181]:

> "Any deployment of OLSRv2 SHOULD use the security mechanism specified in [RFC7183] but MAY use another mechanism if more appropriate in an OLSRv2 deployment. For example, for longer-term OLSRv2 deployments, alternative security mechanisms (e.g., rekeying) SHOULD be considered."

Moreover, this document is also based on the assumption that no additional security mechanism such as IPsec is used in the IP layer or other mechanisms on lower layers, as not all MANET deployments may be able to accommodate such common protection mechanisms (e.g., because of limited resources of MANET routers).

The threats related to NHDP (Neighborhood Discovery Protocol) have been discussed in [RFC7186]. As NHDP is a fundamental block of OLSRv2, the vulnerabilities of NHDP apply also to OLSRv2.

It should be noted that many OLSRv2 implementations are configurable, and so an attack on the configuration system (such as [RFC6779] and [RFC7184]) can be used to adversely affect the operation of an NHDP implementation.

1.1. OLSRv2 Overview

OLSRv2 contains three basic processes: Neighborhood Discovery, MPR Flooding and Link State Advertisements, described in the below with sufficient details for elaborating the analyses in this document.

1.1.1. Neighborhood Discovery

Neighborhood Discovery is the process, whereby each router discovers the routers which are in direct communication range of itself (1-hop neighbors), and detects with which of these it can establish bi-directional communication. Each router sends HELLO messages periodically, listing the identifiers of all the routers from which it has recently received a HELLO message, as well as the "status" of the link (heard or verified bi-directional). A router A receiving a HELLO message from a neighbor B, in which B indicates to have recently received a HELLO message from A, considers the link A-B to be bi-directional. As B lists identifiers of all its neighbors in its HELLO message, A learns the "neighbors of its neighbors" (2-hop neighbors) through this process. HELLO messages are sent periodically, however certain events may trigger non-periodic HELLOs. OLSRv2 [RFC7181] uses NHDP [RFC6130] as its neighborhood discovery mechanism. The vulnerabilities of NHDP are analyzed in [RFC7186].

1.1.2. MPR Flooding

Multi Point Relay (MPR) Flooding is the process whereby each router is able to efficiently conduct network-wide broadcasts. Each router designates, from among its bi-directional neighbors, a subset (MPR set) such that a multicast message transmitted by the router and relayed by the MPR set can received by all its 2-hop neighbors. MPR selection is encoded in outgoing HELLO messages.

Routers may express, in their HELLO messages, their "willingness" (integer between 1 "will never" and 7 "will always") to be selected as MPR, which is taken into consideration for the MPR calculation, and which is useful for example when an OLSRv2 network is "planned". The set of routers having selected a given router as MPR is the MPR-selector-set of that router. A study of the MPR flooding algorithm can be found in [MPR-FLOODING].

1.1.3. Link State Advertisement

Link State Advertisement is the process whereby routers are determining which link state information to advertise through the network. Each router must advertise, at least, all links between itself and its MPR selectors, in order to allow all routers to calculate shortest paths. Such link state advertisements are carried in Topology Control (TC) messages, broadcast through the network using the MPR flooding process described above. As a router selects MPRs only from among bi-directional neighbors, links advertised in TC are also bi-directional and routing paths calculated by OLSRv2 contain only bi-directional links. TCs are sent periodically, however certain events may trigger non-periodic TCs.

1.2. Link State Vulnerability Taxonomy

Proper functioning of OLSRv2 assumes that (i) each router signals its presence in the network and the topology information that it obtained honestly, (ii) each router can acquire and maintain a topology map, accurately reflecting the effective network topology; and (iii) that the network converges, i.e., that all routers in the network will have sufficiently identical topology maps.

An OLSRv2 network can be disrupted by breaking either of these assumptions, specifically (a) routers may be prevented from acquiring a topology map of the network; (b) routers may acquire a topology map that does not reflect the effective network topology; and (c) two or more routers may acquire inconsistent topology maps.

1.3. OLSRv2 Attack Vectors

Besides "radio jamming", attacks on OLSRv2 consist of a compromised OLSRv2 router injecting "correctly looking, but invalid, control traffic" (TCs, HELLOs) into the network. A compromised OLSRv2 router can either (a) lie about itself (its identification, its willingness to serve as MPR), henceforth Identity Spoofing, or (b) lie about its relationship to other routers (pretend existence of links to other routers), henceforth Link Spoofing. Such attacks may disrupt the the Link State Advertisement process, through targeting the MPR Flooding mechanism, or by causing incorrect link state information to be included in TCs, causing routers to have incomplete, inaccurate or inconsistent topology maps. In a different class of attacks, a compromised OLSRv2 router injects control traffic, designed so as to cause an in-router resource exhaustion, e.g., by causing the algorithms calculating routing tables or MPR sets to be invoked continuously, preventing the internal state of a router from converging.

2. Terminology

This document uses the terminology and notation defined in [RFC5444], [RFC6130] and [RFC7181]. Additionally, it defines the following terminology:

Compromised OLSRv2 router: - An attacker that is present in the network and generates syntactically correct OLSRv2 control messages. Control messages emitted by a compromised OLSRv2 router may contain additional information, or omit information, as compared to a control message generated by a non-compromised OLSRv2 router located in the same topological position in the network.

Legitimate OLSRv2 router: - An OLSRv2 router that is not a compromised OLSRv2 router.

3. Topology Map Acquisition

Topology Map Acquisition relates to the ability for any given router in the network to acquire a representation of the network connectivity. A router, unable to acquire a topology map, is incapable of calculating routing paths and participating in forwarding data. Topology map acquisition can be hindered by (i) TCs to not being delivered to (all) routers in the network, such as what happens in case of Flooding Disruption, or (ii) in case of "jamming" of the communication channel.

The jamming and flooding disruption due to identity spoofing and link spoofing have been discussed in [RFC7186].

3.1. Attack on Jittering

OLSRv2 incorporates a jittering: a random, but bounded, delay on outgoing control traffic [RFC5148]. This may be necessary when link layers (such as 802.11 [IEEE802.11]) are used that do not guarantee collision-free delivery of frames, and where jitter can reduce the probability of collisions of frames on lower layers.

In OLSRv2, TC forwarding is jittered by a value between 0 and MAX_JITTER. In order to reduce the number of transmissions, when a control message is due for transmission, OLSRv2 piggybacks all queued messages into a single transmission. Thus, if a compromised OLSRv2 router sends many TCs within a very short time interval, the jitter time of the attacked router tends to 0. This renders jittering ineffective and can lead to collisions on the link layer.

In addition to causing more collisions, forwarding a TC with little or no jittering can make sure that the TC message forwarded by a compromised router arrives before the message forwarded by legitimate routers. The compromised router can thus inject malicious content in the TC, and the legitimate message will be discarded as duplicate message. This preemptive action is important for some of the attacks introduced in the following sections.

3.2. Hop-count and Hop-limit Attacks

The hop-count and hop-limit fields are the only parts of a TC that are modified when forwarding. A compromised OLSRv2 router can modify either of these when forwarding TCs.

3.2.1. Modifying the Hop Limit

A compromised OLSRv2 router can decrease the hop limit when forwarding a TC. This will reduce the scope of forwarding the message, and may lead to some routers in the network not receiving that TC. Note that this is not necessarily the same as not relaying the message (i.e., setting the hop limit to 0), as illustrated in Figure 1.

```
                          .---.
                          | X |
                        --'---' __
                       /          \
                      /            \
                  .---.              .---.
   TC ----->      | A |              | C |
                  '---'              '---'
                      \    .---.   /
                       \-- | B |__/
                           '---'
```

Figure 1: Hop Limit Attack.

A TC arrives at and is forwarded by router A, such that it is received by both B and the malicious X. X can forward the TC without any delay (including without jitter) such that its transmissions arrives before that of B at C. Before forwarding, it significantly reduces the hop limit of the message. Router C receives the TC, processes (and forwards) it, and marks it as already received - causing it to discard further copies received from B. Thus, if the TC is forwarded by C, it has a very low hop limit and will not reach the whole network.

3.2.2. Modifying the Hop Count

A compromised OLSRv2 router can modify the hop count when forwarding a TC. This may have two consequences: (i) if the hop count is set to the maximum value, then the TC will be forwarded no further by, or (ii) artificially manipulating the hop count may affect the validity time as calculated by recipients, when using distance-dependent validity times as defined in [RFC5497] (e.g., as part of a fish-eye extension to OLSR2 [OLSR-FSR]).

```
        v_time(1hop)=2s  v_time(2hops)=4s   v_time(3hops)=6s
.---.          .---.          .---.           .---.
| A |-------> | B | -------> | X |---------->| C |
`---'          `---'          `---'           `---'
```

Figure 2: Different validity times based on the distance in hops.

In Figure 2, router A sends a TC with a validity time of two seconds for neighbors that are one hop away, four seconds for routers in a two-hop distance and six seconds in a three-hop distance. If X is a compromised OLSRv2 router and modifies the hop count (say, by decreasing it to 0), then C will calculate the validity time of received information to two seconds - after which it expires unless

refreshed. If TCs from A are sent less frequently than that up to 3 hops, this causes links advertised in such TCs to be only intermittently available to C.

4. Effective Topology

Link-state protocols assume that each router can acquire an accurate topology map, reflecting the effective network topology. This implies that the routing protocol, through its message exchange, identifies a path from a source to a destination, and this path is valid for forwarding data traffic. If an attacker disturbs the correct protocol behavior, the perceived topology map of a router can permanently differ from the effective topology.

Considering the example in Figure 3(a), which illustrates the topology map as acquired by router S. This topology map indicates that the routing protocol has identified that for S, a path exists to D via B, which it therefore assumes can be used for transmitting data. If, effectively, B does not forward data traffic from S, then the topology map in S does not accurately reflect the effective network topology. Rather, the effective network topology from the point of view of S would be as indicated in Figure 3(b): D is not part of the network reachable from router S.

```
  .---.    .---.    .---.          .---.    .---.
  | S |----| B |----| D |          | S |----| B |
  `---'    `---'    `---'          `---'    `---'

         (a)                              (b)
```

Figure 3: Incorrect Data Traffic Forwarding.

Some of the attacks related to NHDP, such as message timing attack, indirect channel overloading have been discussed in [RFC7186]. Other threats specific to OLSRv2 are further detailed in this section.

4.1. Incorrect Forwarding

OLSRv2 routers exchange information using link-local transmissions (link-local multicast or limited broadcast) for their control messages, with the routing process in each router retransmitting received messages destined for network-wide diffusion. Thus, if the operating system in a router is not configured to enable forwarding, this will not affect the operating of the routing protocol, or the topology map acquired by the routing protocol. It will, however,

cause a discrepancy between the effective topology and the topology map, as indicated in Figure 3(a) and Figure 3(b).

This situation is not hypothetical. A common error seen when deploying OLSRv2-based networks using Linux-based computers as router is to neglect enabling IP forwarding, which effectively becomes an accidental attack of this type.

4.2. Wormholes

A wormhole, depicted in the example in Figure 4, may be established between two collaborating devices, connected by an out-of-band channel. These devices send traffic through the "tunnel" to their alter-ego, which "replays" the traffic. Thus, routers D and S appear as if direct neighbors and reachable from each other in 1 hop through the tunnel, with the path through the MANET being 100 hops long.

```
.---.                                     .---.
| S |----   ....100-hop long path  ... ---| D |
`---.                                   / `---'
    \                                  /
     \                                /
      \X============================X

             1-hop path via wormhole
```

Figure 4: Wormholing between two collaborating devices not participating in the routing protocol.

The consequences of such a wormhole in the network depends on the detailed behavior of the wormhole. If the wormhole relays only control traffic, but not data traffic, the same considerations as in Section 4.1 applies. If, however, the wormhole relays all traffic, control and data alike, it is connectivity-wise identical to a usable link - and the routing protocol will correctly generate a topology map reflecting the effective network topology. The efficiency of the topology so obtained depends on (i) the wormhole characteristics, (ii) how the wormhole presents itself, and (iii) how paths are calculated.

Assuming that paths are calculated with unit-cost for all links, including the "link" presented by the wormhole: if the real characteristics of the wormhole are as-if it was a path of more than 100 hops (e.g., with respect to delay, bandwidth, etc.), then the

presence of the wormhole results in a degradation in performance as compared to using the non-wormhole path. Conversely, if the "link" presented by the wormhole has better characteristics, the wormhole results in improved performance.

If paths are calculated using non-unit-costs for all links, and if the cost of the "link" presented by the wormhole correctly represents the actual cost (e.g., if the cost is established through measurements across the wormhole), then the wormhole may in the worst case cause no degradation in performance, in the best case improve performance by offering a better path. If the cost of the "link" presented by the wormhole is misrepresented, then the same considerations as for unit-cost links apply.

An additional consideration with regards to wormholes is, that such may present topologically attractive paths for the network - however it may be undesirable to have data traffic transit such a path: an attacker could, by virtue of introducing a wormhole, acquire the ability to record and inspect transiting data traffic.

4.3. Sequence Number Attacks

OLSRv2 uses two different sequence numbers in TCs, to (i) avoid processing and forwarding the same message more than once (Message Sequence Number), and (ii) to ensure that old information, arriving late due to, e.g., long paths or other delays, is not allowed to overwrite fresher information (Advertised Neighbor Sequence Number - ANSN).

4.3.1. Message Sequence Number

An attack may consist of a compromised OLSRv2 router spoofing the identity of another router in the network, and transmitting a large number of TCs, each with different Message Sequence Numbers. Subsequent TCs with the same sequence numbers, originating from the router whose identity was spoofed, would hence be ignored, until eventually information concerning these "spoofed" TCs expires.

4.3.2. Advertised Neighbor Sequence Number (ANSN)

An attack may consist of a compromised OLSRv2 router spoofing the identity of another router in the network, and transmitting a single TC, with an ANSN significantly larger than that which was last used by the legitimate router. Routers will retain this larger ANSN as "the most fresh information" and discard subsequent TCs with lower sequence numbers as being "old".

4.4. Indirect Jamming

Indirect Jamming is an attack in which a compromised OLSRv2 router is, by its actions, causing legitimate routers to generate inordinate amounts of control traffic, thereby increasing both channel occupation and the overhead incurred in each router for processing this control traffic. This control traffic will be originated from legitimate routers, thus to the wider network, the malicious device may remain undetected.

The general mechanism whereby a malicious router can cause indirect jamming is for it to participate in the protocol by generating plausible control traffic, and to tune this control traffic to in turn trigger receiving routers to generate additional traffic. For OLSRv2, such an indirect attack can be directed at, respectively, the Neighborhood Discovery mechanism and the Link State Advertisement mechanism.

The most efficient indirect jamming attack in OLSRv2 is to target control traffic, destined for network-wide diffusion. This is illustrated in Figure 5.

The malicious router X selects router A as MPR at time t0 in a HELLO. This causes X to appear as MPR selector for A and, consequently, A sets X to be advertised in its "Neighbor Set" and increments the associated "Advertised Neighbor Sequence Number" (ANSN). Router A must, then, advertise the link between itself and X in subsequent outgoing TCs (t1), also including the ANSN in such TCs. Upon X having received this TC, it declares the link between itself and A as no longer valid (t2) in a HELLO (indicating the link to a as LOST). Since only symmetric links are advertised by OLSRv2 routers, A will upon receipt hereof remove X from the set of advertised neighbors and increment the ANSN. Router A will then in subsequent TCs advertise the remaining set of advertised neighbors (i.e., with X removed) and the corresponding ANSN (t3). Upon X having received this information in another TC from A, it may repeat this cycle, alternating advertising the link A-X as "LOST" and as "MPR".

```
             broadcast TC    ANS={}         TC:()
              (X-A) ANSN      ANSN++          ANSN
      .---.        .---.        .---.        .---.
      | A |        | A |        | A |        | A |
      '---'        '---'        '---'        '---'
        ^            |            ^            |
        |            |            |            |
        | select     |            |indicate    |
        | as MPR     |            |as LOST     |
      .---.        .---.        .---.        .---.
      | X |        | X |        | X |        | X |
      '---'        '---'        '---'        '---'

        t0           t1            t2           t3
```

Figure 5: Indirect Jamming in Link State Advertisement: the malicious X flips between link status MPR and LOST.

Routers receiving a TC will parse and process this message, specifically updating their topology map as a consequence of successful receipt. If the ANSN between two successive TCs from the same router has incremented, then the topology has changed and routing sets are to be recalculated. This is a potentially computationally costly operation.

A compromised OLSRv2 router may chose to conduct this attack against all its neighbors, thus attaining maximum disruptive impact on the network with relatively little overhead of its own: other than participating in the Neighborhood Discovery procedure, the compromised OLSRv2 router will monitor TCs generated by its neighbors and alternate the advertised status for each such neighbor, between "MPR" and "LOST". The compromised OLSRv2 router will indicate its willingness to be zero (thus, avoid being selected as MPR) and may ignore all other protocol operations, while still remaining effective as an attacker.

The basic operation of OLSRv2 employs periodic message emissions, and by this attack it can be ensured that each such periodic message will entail routing table recalculation in all routers in the network.

If the routers in the network have "triggered TCs" enabled, this attack may also cause an increased TC frequency. Triggered TCs are intended to allow a (stable) network to have relatively low TC emission frequencies, yet still allow link breakage or link emergence to be advertised through the network rapidly. A minimum message interval (typically much smaller than the regular periodic message interval) is imposed, to rate-limit worst-case message emissions. This attack can cause the TC interval to, permanently, become equal

to the minimum message interval. [RFC7181] proposes as default that the minimum TC interval be 0.25 x TC interval.

Indirect Jamming by a compromised OLSRv2 router can thus have two effects: it may cause increased frequency of TC generation and transmission, and it will cause additional routing table recalculation in all routers in the network.

5. Inconsistent Topology

Inconsistent topology maps can occur by a compromised OLSRv2 router employing either of identity spoofing or link spoofing for conducting an attack against an OLSRv2 network. The threats related to NHDP, such as identity spoofing in NHDP, link spoofing in NHDP and creating loops have been illustrated in [RFC7186]. This section mainly addresses the vulnerabilities in [RFC7181].

5.1. Identity Spoofing

Identity spoofing can be employed by a compromised OLSRv2 router via the Neighborhood Discovery process and via the Link State Advertisement process. Either of them causes inconsistent topology maps in routers in the network. The inconsistent topology maps due to neighborhood discovery has been discussed in [RFC7186]. For OLSRv2, the attack on link state advertisements can also cause inconsistent topology maps.

An inconsistent topology map may occur when the compromised OLSRv2 router takes part in the Link State Advertisement (LSA) procedure, by selecting a neighbor as MPR, which in turn advertises the spoofed identities of the compromised OLSRv2 router. This attack will alter the topology maps of all routers of the network.

```
A -- B -- C -- D -- E -- F -- X

                            (X spoofs A)
```

Figure 6: Identity Spoofing: compromised OLSRv2 router X spoofs the identity of A, leading to a wrongly perceived topology.

In Figure 6, router X spoofs the address of router A. If X selects F as MPR, all routers in the network will be informed about the link F-A by the TCs originating from F. Assuming that (the real) A selects B as MPR, the link B-A will also be advertised in the network.

When calculating paths, B and C will calculate paths to A via B, as illustrated in Figure 7(a); for these routers, the shortest path to A is via B. E and F will calculate paths to A via F, as illustrated in Figure 7(b); for these routers, the shortest path to A is via the compromised OLSRv2 router X, and these are thus disconnected from the real A. D will have a choice: the path calculated to A via B is of the same length as the path via the compromised OLSRv2 router X, as illustrated in Figure 7(b).

In general, the following observations can be made:

o The network will be split in two, with those routers closer to B than to X reaching A, whereas those routers closer to X than to B will be unable to reach A.

o Routers beyond B, i.e., routers beyond one hop away from A will be unable to detect this identity spoofing.

The identity spoofing attack via the Link State Advertisement procedure has a higher impact than the attack on the neighborhood discovery procedure, since it alters the topology maps of all routers in the network, and not only in the 2-hop neighborhood. However, the attack is easier to detect by other routers in the network. Since the compromised OLSRv2 router is advertised in the whole network, routers whose identities are spoofed by the compromised OLSRv2 router can detect the attack. For example, when a receives a TC from F advertising the link F-A, it can deduce that some entity is injecting incorrect Link State information as it does not have F as one of its direct neighbors.

```
                                               (X spoofs A)

   A < ---- B < ---- C           E ----> F ----> X

   (a) Routers B and C           (b) Routers E and F


      A < --- B < --- C < --- D ---> E ---> F ----> X

                                                  (X spoofs A)
```

Figure 7: Routing paths towards A, as calculated by the different routers in the network in presence of a compromised OLSRv2 router X, spoofing the address of A.

As the compromised OLSRv2 router X does not itself send the TCs, but rather, by virtue of MPR selection, ensures that the addresses it

spoofs are advertised in TCs from its MPR selector F, the attack may be difficult to counter: simply ignoring TCs that originate from F may also suppress the link state information for other, legitimate, MPR selectors of F.

Identity spoofing by a compromised OLSRv2 router, participating in the Link State Advertisement process by selecting MPRs only, thus, creates a situation wherein two or more routers have substantially inconsistent topology maps: traffic for an identified destination is, depending on where in the network it appears, delivered to different routers.

5.2. Link Spoofing

Link Spoofing is a situation in which a router advertises non-existing links to another router (possibly not present in the network). Essentially, TCs and HELLOs both advertise links to direct neighbor routers, with the difference being the scope of the advertisement. Thus, link spoofing consists of a compromised OLSRv2 router, reporting that it has neighbors routers which are, either, not present in the network, or which are effectively not neighbors of the compromised OLSRv2 router.

It can be noted that a situation similar to link spoofing may occur temporarily in an OLSR or OLSRv2 network without compromised OLSRv2 routers: if A was, but is no more, a neighbor of B, then A may still be advertising a link to B for the duration of the time it takes for the the Neighborhood Discovery process to determine this changed neighborhood.

In the context of this document, link spoofing refers to a persistent situation where a compromised OLSRv2 router intentionally advertises links to other routers, for which it is not a direct neighbor.

5.2.1. Inconsistent Topology Maps due to Link State Advertisements

Figure 8 illustrates a network, in which the compromised OLSRv2 router X spoofs links to a existing router A by participating in the Link State Advertisement process and including this non-existing link in its advertisements.

```
A --- B --- C --- D --- E --- F --- G --- H --- X

                          (X spoofs the link to A)
```

Figure 8: Link Spoofing: The compromised OLSRv2 router X advertises a

spoofed link to A in its TCs, thus all routers will record both of the links X-A and B-A.

As TCs are flooded through the network, all routers will receive and record information describing a link X-A in this link state information. If A has selected router B as MPR, B will likewise flood this link state information through the network, thus all routers will receive and record information describing a link B-A.

When calculating routing paths, B, C and D will calculate paths to A via B, as illustrated in Figure 9(a); for these routers, the shortest path to A is via B. F and G will calculate paths to A via X, as illustrated in Figure 9(b); for these routers, the shortest path to A is via X, and these are thus disconnected from the real router A. E will have a choice: the path calculated to A via B is of the same length as the path via X, as illustrated in Figure 9(b).

```
A < --- B < --- C < --- D           F ---> G ---> X ---> A

    (a) Routers B, C, and D           (b) Routers F and G


A < --- B < --- C < --- D < --- E ---> F ---> G ---> X ---> A

                       (c) Router E
```

Figure 9: Routing paths towards router A, as calculated by the different routers in the network in presence of a compromised OLSRv2 router X, spoofing a link to router A.

In general, the following observations can be made:

- The network will be separated in two, with those routers closer to B than to X reaching A, whereas those routers closer to X than to B unable to reach A.

- Routers beyond B, i.e., routers beyond one hop away from A will be unable to detect this link spoofing.

The impact of this attack is similar to that presented in Section 5.2.1, however, is easier to detect as the compromised OLSRv2 router is generating control traffic reaching the entire network.

6. Mitigation of Security Vulnerabilities for OLSRv2

As described in Section 1, [RFC7183] specifies a security mechanism for OLSRv2 that is mandatory to implement. However, deployments may choose to use different security mechanisms if more appropriate. Therefore, it is important to understand both the inherent resilience of OLSRv2 against security vulnerabilities when not using the mechanisms specified in [RFC7183], as well as the protection that [RFC7183] provides when used in a deployment.

6.1. Inherent OLSRv2 Resilience

OLSRv2 (without the mandatory-to-implement security mechanisms in [RFC7183]) provides some inherent resilience against part of the attacks described in this document. In particular, it provides the following resilience:

- Sequence numbers: OLSRv2 employs message sequence numbers, specific per router identity and message type. Routers keep an "information freshness" number (ANSN), incremented each time the content of a Link State Advertisement from a router changes. This allows rejecting "old" information and duplicate messages, and provides some protection against "message replay". This, however, also presents an attack vector (Section 4.3).

- Ignoring uni-directional links: The Neighborhood Discovery process detects and admits only bi-directional links for use in MPR selection and Link State Advertisement. Jamming attacks may affect only reception of control traffic, however OLSRv2 will correctly recognize, and ignore, such a link as not bi-directional.

- Message interval bounds: The frequency of control messages, with minimum intervals imposed for HELLO and TCs. This may limit the impact from an indirect jamming attack (Section 4.4).

- Additional reasons for rejecting control messages: The OLSRv2 specification includes a list of reasons, for which an incoming control message should be rejected as malformed - and allows that a protocol extension may recognize additional reasons for OLSRv2 to consider a message malformed. This allows - together with the flexible message format [RFC5444] - addition of security mechanisms, such as digital signatures, while remaining compliant with the OLSRv2 standard specification.

6.2. Resilience by using RFC7183 with OLSRv2

[RFC7183] specifies mechanisms for integrity and replay protection for NHDP and OLSRv2, using the generalized packet/message format described in [RFC5444] and the TLV definitions in [RFC7182]. The specification describes how to add an Integrity Check Value (ICV) in a TLV to each control message, providing a digital signature of the content of the message using HMAC/SHA-256. In addition, a timestamp TLV is added to the message prior to creating the ICV, enabling replay protection of messages. The document specifies how to sign outgoing messages and how to verify incoming messages, as well as under which circumstances a non-valid message is rejected. Because of the HMAC/SHA-256 ICV, a shared key between all routers in the MANET is assumed. A router without valid credentials is not able to create an ICV that can be correctly verified by other routers in the MANET; therefore, such an incorrectly signed message will be rejected by other MANET routers, and the router cannot participate in the OLSRv2 routing process (i.e., the malicious router will be ignored by other, legitimate routers). [RFC7183] does not address the case where a router with valid credentials has been compromised. Such a compromised router will not be excluded from the routing process, and other means of detecting such a router are necessary if required in a deployment (in addition to using asymmetric keys, allowing to revoke access to one particular router instead of revoking the shared key used by all routers in the MANET).

In the following sections, each of the vulnerabilities described earlier in this document will be evaluated in terms of whether OLSRv2 with the mechanisms in [RFC7183] provides sufficient protection against the attack. It is implicitly assumed in each of the following sections that [RFC7183] is used with OLSRv2.

6.2.1. Topology Map Acquisition

Attack on Jittering - As only OLSRv2 routers with valid credentials can participate in the routing process, a malicious router cannot reduce the jitter time of an attacked router to 0 by sending many TC messages in a short time. The attacked router would reject all the incoming messages as "invalid" and not forward them. The same applies for the case where a malicious router wants to assure that by forcing a zero jitter interval, the message arrives before the same message forwarded by legitimate routers.

Modifying the Hop Limit - As the hop limit is not protected by [RFC7183] (since it is a mutual field, changing at every hop), this attack is still feasible.

Modifying the Hop Count - Similarly to the hop limit, as the hop count is not protected by [RFC7183] (since it is a mutual field, changing at every hop), this attack is still feasible.

6.2.2. Effective Topology

Incorrect Forwarding - As only OLSRv2 routers with valid credentials can participate in the routing process, a malicious router will not be part of the topology of other legitimate OLSRv2 routers. Therefore, no data traffic will be sent to the malicious router for forwarding.

Wormholes - Since a wormhole consists of at least two devices forwarding (unmodified) traffic, this attack is still feasible and undetectable by the OLSRv2 routing process since the attack does not involve the OLSRv2 protocol itself (but rather lower layers). By using [RFC7183], it can at least be assured that the content of the control messages is not modified while being forwarded via the wormhole. Moreover, the timestamp TLV assures that the forwarding can only be done in a short time window after the actual TC message has been sent.

Message Sequence Number - As the message sequence number is included in the ICV calculation, OLSRv2 is protected against this attack.

Advertised Neighbor Sequence Number (ANSN) - As the ANSN is included in the ICV calculation, OLSRv2 is protected against this attack.

Indirect Jamming - Since the control messages of a malicious router will be rejected by other legitimate OLSRv2 routers in the MANET, this attack is mitigated.

6.2.3. Inconsistent Topology

Identity Spoofing - Since the control messages of a malicious router will be rejected by other legitimate OLSRv2 routers in the MANET, a router without valid credentials may spoof its identity (e.g., IP source address or message originator address), but the messages will be ignored by other routers. As the mandatory mechanism in [RFC7183] uses shared keys amongst all MANET routers, a single compromised router may spoof its identify and cause harm to the network stability. Removing this one malicious router once detected implies rekeying all other routers in the MANET. Asymmetric keys, in particular when using identity based signatures, such as specified in [IBS] may further allow to revoke single routers and to verify their identity based on the ICV itself.

Link Spoofing - Similar to identity spoofing, a malicious router without valid credential may spoof links, but its control messages will be rejected by other routers, thereby mitigating the attack.

Inconsistent Topology Maps due to Link State Advertisements - The same considerations as for link spoofing apply.

7. Security Considerations

This document does not specify a protocol or a procedure. The document, however, reflects on security considerations for OLSRv2, and its constituent parts, including NHDP.

8. IANA Considerations

This document has no actions for IANA.

9. References

9.1. Normative References

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

[RFC7186] Yi, J., Herberg, U., and T. Clausen, "Security Threats for the Neighborhood Discovery Protocol (NHDP)", RFC 7186, April 2014.

9.2. Informative References

[FUNKFEUER] "http://www.funkfeuer.at/".

[IBS] Dearlove, C., "Identity-Based Signatures for MANET Routing Protocols", work in progress draft-ietf-manet-ibs-02, July 2014.

[IEEE802.11] "IEEE 802.11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Spec.", 2007.

[MPR-FLOODING] Qayyum, A., Viennot, L., and A. Laouiti, "Multipoint relaying: An efficient technique for flooding in mobile

wireless networks.", 2001.

[OLSR-FSR]
Adjih, C., Baccelli, E., Clausen, T., Jacquet, P., and G. Rodolakis, "Fish eye OLSR scaling properties, IEEE Journal of Communication and Networks (JCN), Special Issue on Mobile Ad Hoc Wireless Networks", 2004.

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

[RFC5068] Hutzler, C., Crocker, D., Resnick, P., Allman, E., and T. Finch, "Email Submission Operations: Access and Accountability Requirements", RFC 5068, BCP 134, October 2007.

[RFC5148] Clausen, T., Dearlove, C., and B. Adamson, "Jitter Considerations in Mobile Ad Hoc Networks (MANETs)", RFC 5148, February 2008.

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

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

[RFC7182] Herberg, U., Clausen, T., and C. Dearlove, "Integrity Check Value and Timestamp TLV Definitions for Mobile Ad Hoc Networks (MANETs)", RFC 7182, April 2014.

[RFC7183] 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 7183, April 2014.

[RFC7184] Herberg, U., Cole, R., and T. Clausen, "Definition of Managed Objects for the Optimized Link State Routing Protocol Version 2", RFC 7184, April 2014.

[RFC7187] Dearlove, C. and T. Clausen, "Routing Multipoint Relay Optimization for the Optimized Link State Routing Protocol Version 2 (OLSRv2)", RFC 7187, April 2014.

[RFC7188] Dearlove, C. and T. Clausen, "Optimized Link State Routing Protocol Version 2 (OLSRv2) and MANET Neighborhood Discovery Protocol (NHDP) Extension TLVs", RFC 7188, April 2014.

Authors' Addresses

Thomas Clausen

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

Ulrich Herberg

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

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/