Vulnerability Analysis of Relay Set Selection Algorithms for the Simplified Multicast Forwarding (SMF) Protocol for Mobile Ad Hoc Networks

Jiazi Yi, Thomas Clausen
Laboratoire d'Informatique - LIX, Ecole Polytechnique, France
jiazi@jiaziyi.com, thomas@thomasclausen.org

***Abstract*—After more than a decade of research and standardization, Mobile Ad Hoc NETworks (MANET) are finding their place in real-world deployments, such as in community, tactical and vehicular networks. Becoming so present in "*the real world*" also means that MANETs, and the protocols operating them, are affronted with a more hostile environment, where misconfiguration, eavesdropping, and attacks must be addressed. A first step in addressing MANET security is understanding the vulnerabilities of MANET protocols, and how an attacker can exploit these.**

This paper studies the Relay Set Selection (RSS) algorithms that are commonly used in multicast routing protocol for MANETs, and which are undergoing standardization as part of the Simplified Multicast Forwarding (SMF) protocol, developed within the Internet Engineering Task Force (IETF). Attack vectors for these different RSS algorithms are described, with the purpose of enabling future development of security solutions.

I. Introduction

Network security is as old as networking, and as vast as authentication, non-repudiation, integrity, etc. In traditional wired networks, security is largely based on maintaining physical control of access to the communication channel (fiber, coaxial cable, etc.). In a wireless MANET environment, routers and hosts are more vulnerable to different threats since:

- Physical access to the wireless medium is not delimited by wired cables, but available to anyone within transmission range. Furthermore, compared to a wired media, a wireless medium is more unreliable and unpredictable, rendering behavioral observation more difficult;
- Resources in mobile devices are often constrained, both in terms of CPU power, memory space, battery life, etc. Such limited resource render the network more vulnerable to attacks, especially Denial-of-Service (DoS) attack by maliciously consuming the transmission channel, CPU time, or resulting in memory overflow;
- The topology of a MANET is dynamic due to both mobility of routers and variations in the wireless channel. This implies that the use of traditional mechanisms such as checkpoints, firewalls on ingress filtering based on a-priory knowledge is less obvious.

Given the above, if for MANETs to stand a chance outside the protected confines of research laboratories, security issues have to be addressed. MANET deployments must consider that misconfiguration and malicious routers are present, and that neither physical media control nor a-priori topology knowledge are viable security approaches.

A. Background and History

The "Simple Multicast Forwarding" (SMF) protocol [1] is a multicast routing protocol for MANET-wide efficient broadcasting. The protocol employs reduced relay sets for reducing the number of redundant retransmissions of a data packet in the network. Reduced relay sets so used were introduced in and standardized for IP networks by way of the Optimized Link State Routing Protocol (OLSR [2]) in 2003, where they were used for substantially reducing the protocol overhead incurred by diffusion of link state advertisements, in [2] denoted "TC messages". The reduced relay set mechanism in OLSR is based on Multi-Point Relays (MPRs) [3]. This concept was retained and used in an extension of OSPF for MANET areas [4]. Other experimental routing protocols, including [5] and [6], have used different reduced relay set mechanisms, and the Internet Engineering Task Force (IETF) is standardizing the next-generation MANET routing protocol OLSRv2 [7], retaining the MPR concept. The experimental reactive MANET routing protocol AODV [8] also uses MANET-wide broadcast of its route requests – for which [9] showed that using MPRs for flooding route requests resulted not just in reduced channel load, but also in shorter unicast paths.

The success of reduced relay sets for diffusion of routing protocol control traffic lead to work on using the same mechanisms also for user data traffic, including [10] and [11], ultimately leading to the IETF development of SMF [1], as an experimental protocol. SMF provides basic IP multicast routing for MANETs. It consists of two main components: multicast "Duplicate Packet Detection" (DPD) and "Relay Set Selection" (RSS).

- DPD is used in the forwarding process to identify if an incoming packet has been previously received (and forwarded) – and thus should be dropped – or not. DPD is achieved by a router maintaining a record of recently processed multicast packets, and comparing received multicast packets herewith. A duplicate packet detected is silently dropped, and not inserted into the forwarding path of that router – nor delivered to an application.

978-0-7695-4779-4/12 $26.00 © 2012 IEEE
DOI 10.1109/NBiS.2012.48

- RSS yields a reduced relay set for relaying data packets across a MANET. SMF supports several RSS algorithms: E-CDS (Essential Connected Dominating Set), S-MPR (Source-based Multi-Point Relay), and MPR-CDS, based on localized election and derived from those explored for topology diffusion in MANET routing protocols.

B. Statement of Purpose

RSS algorithms for efficient flooding have been well studied for performance and convergence properties. However it is generally assumes that all routers in the networks can be trusted to perform their part in the RSS algorithm properly. In the "Real World", where a wireless channel is accessible to anyone within radio-range, this can not be assumed be that due to router misconfiguration or malice.

This paper analyses the vulnerabilities of the different RSS algorithms, proposed by SMF [1]. It is worth noting that SMF, as an experimental protocol, does not prescribe a preferred RSS algorithm, but rather serves to document the different options and encourage experiments and evaluation in order to determine – by way of testing against "the real world" – which eventually becomes preferred. Part of this "testing against the real world" – and the ambition of this paper – is testing how an RSS algorithm stands up against different security threats.

While the paper has the ambition of being through, in matters of security it is prudent to be explicit to not claim completeness of analysis.

C. Paper Outline

The remainder of this paper is organized as follows: section II, describes general threats, commonly applicable to all RSS algorithms; section III, section IV and section V, then specifically studies vulnerabilities to E-CDS, S-MPR and MPR-CDS, respectively. This paper is concluded in section VI.

II. General Threats to Relay Set Selection

A. Eavesdropping

Eavesdropping is a common and easy passive attack in a wireless environment. Once a packet is transmitted, any close receiver can obtain a copy without being detected, for immediate or later decoding. SMF uses a neighborhood discovery protocol, NHDP [12] for providing each router with 1-hop and 2-hop topological information, permitting RSS algorithms to operate. A malicious router can eavesdrop on the NHDP message exchange and thus learn this local topology information, as well as some source and destination addresses of data packets transmitted. Eavesdropping is not direct threat to the network integrity, nor to SMF, but it can provide crucial network information such as identity of communicating routers, link characteristic, router configuration, etc., enabling other attacks.

B. Message Timing Attack

As NHDP is used to provide local topology information for RSS algorithms, NHDP vulnerabilities thus affect SMF. NHDP HELLO messages define two types of timing information:

- Validity time, the time during which the information conveyed by the message should be considered valid.
- Interval time, the time after which the next control message from the same router should be expected.

For *validity time*, an attacker can simply eavesdrop on HELLOs, then instantly upon receipt replay the HELLO – but modified to have a low validity time, illustrated in figure 1. Router *b* broadcasts a HELLO with $valiTime = 6s$. Router *a* receives the HELLO and marks the link between itself and *b* is valid for 6 seconds. *X* eavesdrops on the messages, obtains the identity of router *b*, then transmits the HELLO with *valiTime=0.1s*. Receipt of this message by *a* causes *a* to replace previously received link information, and therefore consider the link between itself and *b* as *invalid* after very short time (0.1 second). For SMF, this means that *b* will not be selected as relay by *a* even it may provide good connectivity to other parts of the network.

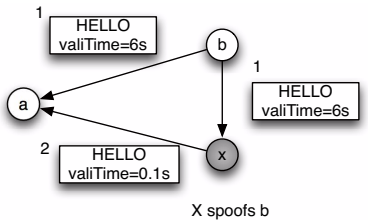

Figure 1. Validity time attack: The malicious router, *X*, spoofs *b* and declares a short validity time of the link.

A similar attack exists for *interval time*: a malicious router behaves as above, and also indicate a low interval time. A recipient of a HELLO with *interval time* so modified will expect a subsequent HELLO within this very short time – which will not arrive: the recipient decreases the link quality, or may discard this link. Further vulnerabilities to the NHDP exist [13].

C. Indirect Jamming

For NHDP, a malicious router can – intentionally and frequently – alter the neighborhood information, link state, etc. declared in HELLOs, and thereby cause generation of inordinate amounts of control traffic by legitimate routers and increase the resources required for message processing [13].

Used by all RSS algorithms, indirect jamming of NHDP is a threat to every SMF router: a malicious router can generate plausible control traffic to in turn trigger receiving routers to generate additional traffic, *e.g.,*a malicious router can keep changing its router priority to provoke recalculation of and signaling of relay sets.

D. RSSV Attack

SMF uses distributed RSS algorithms that dynamically calculate a topological Connected Dominating Set (CDS), generally assuming 1-hop and 2-hop neighborhood information as provided by NHDP. SMF supports different, and non-interoperable, RSS algorithms – and, hence, SMF routers

convey to their neighbors which algorithm(s) they respectively support. To this end, [1] defines a "Relay Set Selection Vector" (RSSV), by way of message and address block TLVs [14], to be included in the NHDP HELLOs such that an SMF router can declare which RSS algorithms it, and its immediate neighbors, support[1]. An SMF outer must therefore select relay sets according to compatibility of the algorithms operating in SMF routers in its 1-hop and 2-hop neighborhoods. A potential attack is, therefore, if a router – intentionally or otherwise – share false RSSV information for itself or for its neighbors.

For example, in figure 2, router *a* is about to select its relays. The following RSS algorithms are used in different routers:

- E-CDS: router *b, d, e*
- S-MPR: router *c, f, g*
- MPR-CDS: router *h*

All routers, faithfully, declare their RSSV. Based on the messages from routers *b, h* and *c*, router *a* learns what algorithms are supported by both its direct neighbors and its 2-hop neighbors. This allows router *a* to observe that while router *h* provides topological coverage to all of the 2-hop routers (*d, e, f, g*), router *h* runs an RSS algorithm different from all of *d, e, f, g*. Therefore, if *a* selects *h* as relay, *h* may not be able to select relays among *d, e, f, g* and thus packet forwarding beyond *d, e, f, g* would not happen. Router *a* also learns that router *b* runs the same RSS algorithm as the 2-hop neighbors *d, e*, reachable via *b* – and that router *c* runs the same RSS algorithm as the 2-hop neighbors *f, g*, reachable via *c*. Router *a* can therefore select *b* and *c* as relays, knowing that both of these will be able to not only provide coverage to all 2-hop neighbors, but also be able to select proper relays among these 2-hop neighbors.

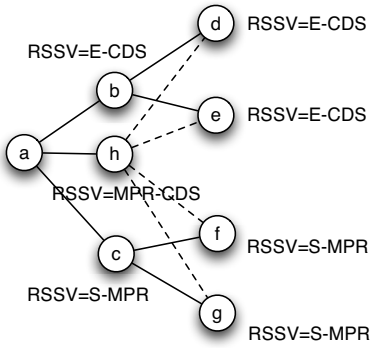

Figure 2. Relay set selection considering RSSV: Router *a* makes the decision based on the RSSV declared by TLVs.

A malicious router, spoofing the RSSV of its 2-hop neighbors, is shown in figure 3: *X* declares itself with *RSSV=MPR-CDS*, and further declares that *d, e, f, g* have *RSSV=MPR-CDS*. Thus, router *a* choses *X* as sole relay: from the information available to *a*, *X* provides optimal topological coverage of the 2-hop neighborhood – and by running the same RSS as (declared for) all 2-hop neighbors, should be able to also do proper relay set selection with these. As a consequence, *X* will "take control" of the multicast traffic in its neighborhood – in this case, be able to prohibit *b* and *c* from being selected as relays and, thus, if *X* isnot actually forwarding traffic or performing RSS, disrupt network connectivity.

[1]While several RSS are supported in the same *network*, it is not clearly specified in the current revision of SMF [1] whether a *router* can concurrently support several different RSS at the same time.

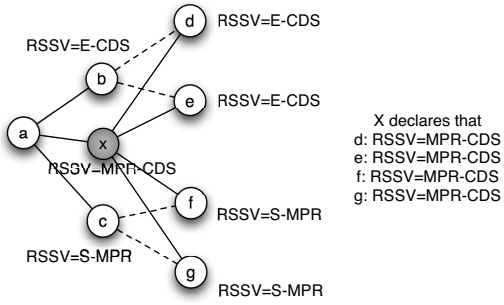

Figure 3. Attack on the RSSV to disrupt the relay set selection: The malicious router *X* spoofs the RSSV of *d, e, f, g*.

Furthermore, the indirect jamming attack mentioned in the previous subsection is also applicable to RSSV signaling by changing the RSSV type continuously.

III. E-CDS VULNERABILITIES

The Essential Connected Dominating Set (E-CDS) RSS algorithm produces a common set of relays for all routers in the network. Routers self-select as relays based on priority information and of the 1-hop and 2-hop neighborhood topology. The priority of a router can be *e.g.,*, a router metrics (such as power level) or simply a tie-breaker such as the router address. Using E-CDS, a router self-select as relay if and only if:

- the router's router priority is greater than the priority of all its two-hop neighbors, OR
- there is no path from the highest priority neighbor to all other one and two hop neighbors using only routers with greater priority as relays.

A malicious router can disrupt E-CDS selection, by way of *link spoofing* and *identity spoofing*, discussed separately.

A. Link Spoofing

Link spoofing implies that a router advertises non-existing links to another router (present in the network or not). Based on NHDP, a malicious router can perform link spoofing by modifying *HELLO*s.

In figure 4, where solid lines illustrate actual links whereas dotted lines "spoofed" links, router *a* tries to make E-CDS relay set selection based on the one-hop and two-hop neighborhood information from router *b*, *c*, *d* and *e* (The router priority is as indicated in figure 4). If the algorithm runs properly, *a* will choose itself as a relay, because it has the highest priority among its two-hop neighbors. Alas, present is also a malicious router, *X*, which (i) declares itself with the highest priority in the neighborhood ($RtrPri = 6$), and (ii) advertises links (real

or spoofed) to all of a's one-hop and two-hop neighbors. By thus presenting itself as a router with high priority and strong connection with other routers, *a* will not be able to select itself as relay: *X* appears as providing better coverage and higher priority.

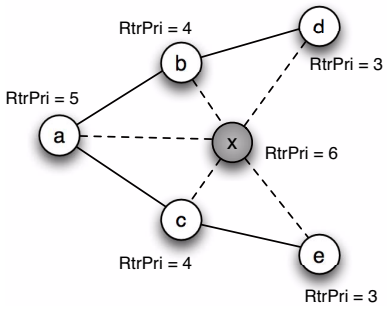

Figure 4. E-CDS algorithm disruption by link spoofing. Router *a* is trying to make relay set selection and malicious router *X* declares itself with high router priority and spoofs the link to the neighbors of *a*.

The effect of link spoofing depends on the local topology and the ability to eavesdrop: the biggest impact can be achieved when information describing all the 2-hop links of router *a* is available to *X*. If some of the 2-hop neighbors of *a* are 3-hop away from the malicious attacker *X*, shown in figure 5, *X* can not obtain the identity of router *c* directly through NHDP – limiting the effect of such an attack.

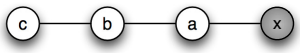

Figure 5. Limitation of link spoofing: malicious router *X* can not obtain the identity of router *c* directly through NHDP.

Thus, malicious routers disrupt the network by preventing legit routers from self-selecting as relays. Link-spoofing can also cause routers to (unnecessarily) self-select relays, with the goal of degrading the flooding operation to classic flooding. This is illustrated in figure 6, where solid lines illustrate actual links whereas dotted lines "spoofed" links: router *a* with low priority ($RtrPri = 2$) will not self-select since *b* both has the highest priority ($RtrPri = 5$)in the 2-hop neighborhood, and can provide links to all other neighbors of *a* by way of relays with higher priority than *a*. Alas, present is also a malicious router *X* which (i) declares itself with the lowest priority ($RtrPri = 1$), and (ii) spoofs a link to (fictive or present) router z. As a consequence, *a* has to self-select as relay no route to z, using only routers withs greater priority than *a*, exists. This will be the case for all the neighbors of *X*, therefore the E-CDS is by way of this link spoofing attack degraded locally to classical flooding locally (discussed further in section V-A).

B. Identity spoofing

Identity spoofing implies that a malicious router determines and makes use of the identity of other routers, without being authorized to do so. A malicious router can obtain the identity of a legitimate routers by overhearing HELLOs, or source/destination addresses from the data traffic. The malicious router can, then, generates (routing or data) traffic, pretending to be the legitimate router.

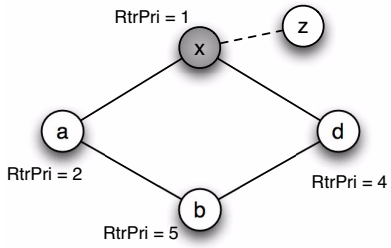

Figure 6. E-CDS link spoofing attack. Malicious router*X* mades router *a* have to choose itself as relay, which degrades the relay set selection to classical flooding.

As shown in figure 7, at time t_0, router *b* sends a HELLO , declaring its priority $RtrPri = 1$. Router *a* hears the HELLO and updates its information bases accordingly. The malicious router *X* also receives the same HELLO, records the address of *b*, and the sequence number of the HELLO, and then transmits a HELLO immediately at time t_1 (*e.g.,*100 ms after t_0), with the address of router *b*, with a higher sequence number (so as to make the message appear legitimate) and with a modified router priority ($RtrPri = 6$). On receiving this second HELLO, router *a* will see it as simply reporting updated information from *a*. As HELLO are sent periodically, *X* can time its transmissions such that *a* will operate with incorrect information for *b*. In this particular case, it will prevent *a* from self-selecting as relay.

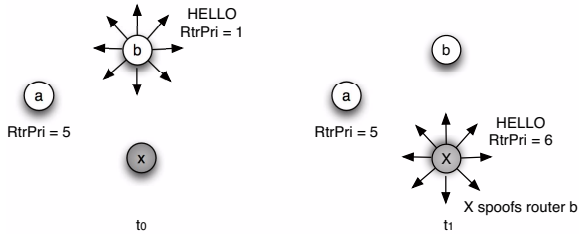

Figure 7. E-CDS identity spoofing attack. Malicious router *X* overhears the identity of *b* at t_0 and sends out a poisoned HELLLO message as *b* at t_1.

IV. S-MPR VULNERABILITIES

The Source-based Multipoint Relay (S-MPR) RSS algorithm is derived from [2] and [7], and enables routers to select a reduced relay set (called the routers MPR set) from among their one-hop neighbors such that a message generated by a router and relayed by its MPR Set will be received by all routers 2-hops away. Once a router has selected its MPR set, it signals this (embedded in a HELLO) to the neighbors it has selected as MPR. An S-MPR router forwards a multicast packet if and only if:

- the packet is never before received, AND
- the packet was received from a neighbor with which it has a bi-directional link, AND
- and the neighbor from which the packet was received has selected the router as an relay.

As with E-CDS, a malicious router can, by spoofing the link or the identity of specified routers, disrupt the proper functioning of the S-MPR RSS.

A. Link Spoofing

Routers that run S-MPR select relays from among their one-hop neighbors. To reduce redundant data transmissions, the routers with better connectivity are given priority when considered as relays. Thus, a malicious router can spoof the links to other routers to prevent that other, legitimate, routers be selected. This is illustrated in figure 8, where solid lines illustrate actual links whereas dotted lines "spoofed" links. Router *a* is selecting its relays from among *X* and *b*. If both *X* and *b* faithfully declare their neighborhoods, *b* has to be chosen so as to make sure that a message generated by *a* and relayed by the selected MPRs reach all routers 2-hops away from *a* (*i.e.,d, e*). Alas, *X* is malicious and spoofs links to *d* and *e* – in addition to a link to the fictitious router, *c*. As a consequence, when *a* is running S-MPR algorithm, it only choses *X* as its MPR as it believes that *X* can provide links to all the two-hop neighbors of *b*, in addition to the fictitious *c*. If *X* then ultimately does not relay multicast traffic *d* and *e* are rendered unreachable.

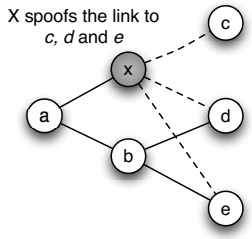

Figure 8. S-MPR link spoofing attack. Malicious router *X* spoofs links to *c*, *d* and *e*, to mask *b* from being chosen as relay by *a*.

B. Identity Spoofing

By overhearing HELLOs, the identity of other routers in the network may be available for a malicious router. In NHDP, HELLO messages are additive, thus a malicious router can inject vicious incorrect additional information by spoofing the identity of a detected legitimate router. This is illustrated in figure 9, where solid lines illustrate actual links whereas dotted lines "spoofed" links, and where router *a* is selecting relays from among its one-hop neighbors. Absent any malicious routers, *b* will be chosen as relay by *a*'s. Alas, present is also a malicious router *X*, which (i) spoofs the identity of router *c*, and (ii) declares links to *d* and (a fictitious or present) *f*. Consequently, *a* selects only *c* as its relay, rendering *d* ultimately unreachable for multicast traffic from *a*.

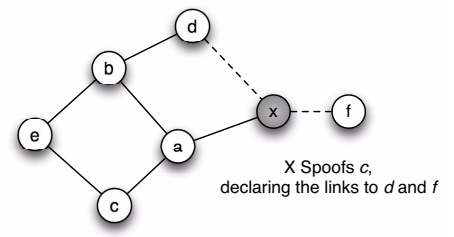

Figure 9. S-MPR identity spoofing attack. Router *a* is running S-MPR algorithm and malicious router *X* spoofs the identity of router *c*.

V. MPR-CDS Vulnerabilities

MPR-CDS [15] is a derivative from S-MPR which – as E-CDS – results in a common set of relays for all routers in the network. In MPR-CDS, the MPR selection and signaling from S-MPR is performed, but the forwarding rules are different, specifically forwarding does not depend on from which router a packet is received. An MPR-CDS router forwards a multicast packet if and only if:

- the packet is never before received, AND
  - the router's priority is higher than the priority of all its 1-hop neighborhood, OR
  - the router has been selected as an relay by the router that has the highest priority in its 1-hop neighborhood.

It is worth noting that the main difference between S-MPR and MPR-CDS is, that while MPR-CDS forms an unique broadcast tree for all sources in the network, S-MPR forms a different broadcast tree for each source in the network.

Nevertheless, as MPR-CDS combines E-CDS and S-MPR, the vulnerabilities of E-CDS and S-MPR, discussed in section III and section IV also apply to MPR-CDS. One additional vulnerability is introduced, though: a simple way of degrading the network into classic flooding.

A. Broadcast Storm

In wireless MANETs, a broadcast storm due to classic flooding causes serious performance degradation: two or more adjacent routers receiving a multicast packet at the same time are likely to also re-transmit at the same time - causing their transmissions to overlap, with as result channel contention and collisions [16]. Avoiding broadcast storms is one of the reasons why RSS algorithms are used – in SMF as well as in routing protocols such as [2].

MPR-CDS is vulnerable to being degraded into classical flooding, simply by way of a malicious router (i) declaring itself to have the the highest priority in its neighborhood, and (ii) selecting all its neighbors as MPR, shown in figure 10. Note that this attack works due to the "common set of relays for all routers in the network" philosophy. S-MPR is not vulnerable to this particular attack since the relays selected by the malicious router *X* are used only by traffic transiting *X* itself.

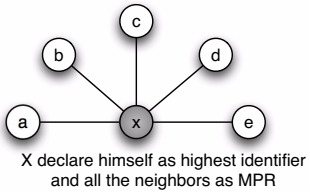

Figure 10. MPR-CDS

Figure 11 illustrated broadcast storm (dotted lines, classic flooding), compared to MPR-CDS (and S-MPR) intentional traffic (solid lines).

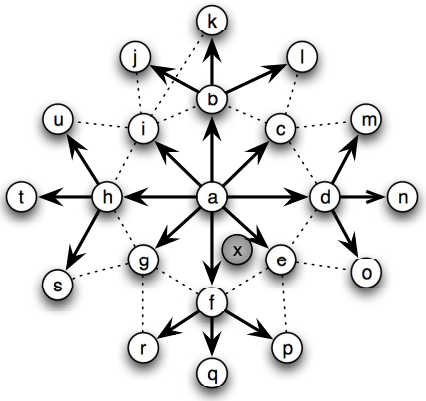

Figure 11. The broadcast storm attack: The bold line with arrow represents normal multicast traffic, and the dashed line the redundant traffic caused by having all the 1-hop neighbors of *a* be selected as relays.

VI. Conclusion

This paper has described a set of vulnerabilities of relay set selection algorithms as specified by the "Simple Multicast Forwarding" (SMF) protocol for Mobile Ad Hoc Networks. SMF provides a framework, supporting different RSS algorithms and, based on the neighborhood discovery protocols (NHDP) a set of RSS: E-CDS, S-MPR and MPR-CDS.

In addition to vulnerabilities inherited from the feature of wireless medium and its use of NHDP, SMF introduces vulnerabilities by way of those RSS algorithms. Mis-configured routers or malicious attackers can inject inconsistent topology information in the network by link spoofing or identity spoofing, thus result in network disruption or even degrading RSS algorithms to classical flooding. Furthermore, because SMF provides a signaling mechanism (RSSV) to identify various RSS algorithms, the malicious routers have the chance to present conflicting information to disturb the decision of relay set selection.

References

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

[2] T. Clausen and P. Jacquet, "Optimized Link State Routing Protocol (OLSR)," Experimental RFC 3626, October 2003.

[3] A. Qayyum, L. Viennot, and A. Laouiti, "Multipoint relaying: An efficient technique for flooding in mobile wireless networks," in *Proceedings of the 35th Annual Hawaii International Conference on System Sciences (HICSS)*, January 2001.

[4] T. Clausen, P. Jacquet, E. Baccelli, and D. Nguyen, "OSPF Multipoint Relay (MPR) Extension for Ad Hoc Networks," Experimental RFC 5449, February 2009.

[5] R. Ogier, F. Templin, and M. Lewis, "Topology Dissemination Based on Reverse-Path Forwarding (TBRPF)," Standards Track RFC 3686, 2004.

[6] R. Ogier and P. Spagnolo, "Mobile Ad Hoc Network (MANET) Extension of OSPF Using Connected Dominating Set (CDS) Flooding," Experimental RFC 5614, 2009.

[7] T. Clausen, C. Dearlove, and P. Jacquet, "The Optimized Link State Routing Protocol version 2," Internet Draft, draft-ietf-manet-olsrv2-14, work in progress, March 2012.

[8] C. Perkins, E. Belding-Royer, and S. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing," Experimental RFC 3561, July 2003.

[9] T. Clausen, L. Viennot, and P. Jacquet, "Optimizing Route Length in Reactive Protocols for Ad Hoc Networks," in *Proceedings of the IFIP MedHocNet*, September 2002.

[10] P. Jacquet and E. Baccelli, "Diffusion mechanisms for multimedia broadcasting in mobile ad hoc networks," in *Proceedings of the IASTED International Conference on Internet and Multimedia Systems and Applications (IMSA)*, August 2004.

[11] T. Clausen, T. Olesen, and L. N., "Investigating broadcast performance in mobile ad-hoc networks," in *Proceedings of the IEEE conference on Wireless Personal Multimedia Communications (WPMC)*, October 2002.

[12] T. Clausen, C. Dearlove, and J. Dean, "Mobile Ad Hoc Network (MANET) Neighborhood Discovery Protocol (NHDP)," Standards Track RFC 6130, April 2010.

[13] U. Herberg and T. Clausen, "Security Issues in the Optimized Link State Routing Protocol Version 2 (OLSRV2)," *International Journal of Network Security & Its Applications*, vol. 2, no. 2, pp. 162–181, 2010.

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

[15] C. Adjih, J. P, and L. Viennot, "Computing connected dominated sets with multipoint relays," *JOURNAL OF AD HOC AND SENSOR WIRELESS NETWORKS*, vol. 1, 2005.

[16] Y.-C. Tseng, S.-Y. Ni, Y.-S. Chen, and J.-P. Sheu, "The broadcast storm problem in a mobile ad hoc network," *Wireless Networks*, vol. 8, pp. 153–167, March 2002.