

nrlsmf Update

IETF 70
5 December 2007

Brian Adamson
Naval Research Laboratory

nrlsmf Overview

- User-space IP multicast forwarding (IPv4 and IPv6) supporting SMF experimentation.
- Requires *nrlolsrd* (or other) external process for neighborhood discovery and relay-set selection.
 - Has been used with Quagga OSPF-MANET
 - Future version to include built-in NHDP support.
- Supports multiple interface operation for gateway or multi-homed MANET.
- Considerable use in DARPA and ONR/NRL experiments by multiple parties for a variety of scenarios.

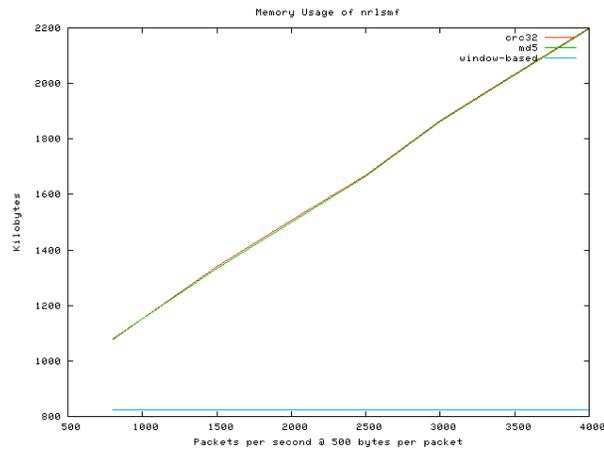
New *nrlsmf* Features

- Table-based I-DPD now default (window-based approach still available)
- Added support for H-DPD operation (see “hash” command-line option)
- Added support for “Internal Hash” in conjunction with I-DPD.
- Support for fragmented packets and IPSec per current SMF draft.
- Currently conducting some performance testing and simulations.
 - CPU/ memory usage trade-offs
 - Further testing, studies, etc planned

New *nrlsmf* Commands

- Commands added to support H-DPD and “internal hash” computation including the following algorithms:
 - CRC32, MD5, SHA1
- New *nrlsmf* commands added:
 - Specify H-DPD operation with a given <algorithm>:
`nrlsmf hash <algorithm>`
 - I-DPD plus optional “internal hash”:
`nrlsmf ihash <algorithm>`
 - Window-based I-DPD instead of H-DPD:
`nrlsmf window on`
- Table-based I-DPD is default operation.
- Table entries are timed-out after 10 seconds by default.
- Other:
 - “ttl” command available to rescope outbound, locally-generated multicast packets.

nrlsmf Memory Usage



nrlsmf CPU Usage

- Some initial tests have been conducted to assess I-DPD vs. H-DPD CPU demands.
- Further work to be conducted to look at trade-off of security vs. complexity for “Internal Hash” computation.
- It is expected that I-DPD + “Internal Hash” can be implemented with considerably lower complexity than H-DPD.
 - Table-based I-DPD and H-DPD have similar “lookup” and memory costs.
 - A much simpler internal hash algorithm may be used.

nrlsmf Next Steps

- Investigate light-weight algorithms for “internal hash” computation.
 - Security vs. complexity trade-off.
- Implement suggested TTL-based solution to “wormhole” attack as an option.
- Per-interface control of DPD timeouts.
- Built-in support for NHDP and relay set selection.