SMF-06 Update

draft-ietf-manet-smf-06

Joe Macker

IETF 70

Vancouver, BC, CA

Background Refresh

- Submission Intent is EXP initially
- Reason: Encourage more experimentation of use cases and modes of operation
- Present prototype implementations are running in simulation, emulation, and working networks

SMF-05 -> 06

- More extensive changes than anticipated at last meeting
  - Editor and others felt that was necessary
  - Many comments integrated from list discussions
  - Other issues raised during redesign
  - Added significant new material
  - Removed a lot of non-specification information
  - Actual overall page growth was about +1
- Major change areas
  - DPD Details
  - CDS Detailed added
  - TLVs added

Duplicate Packet Detection Changes

- Two fundamental DPD modes remain H-DPD and I-DPD
  - Hash-based H-DPD
  - Explicit identifier I-DPD

- Overall Changes
  - S-DPD renamed to I-DPD: identification based
    - Mitigate sequence-based security vulnerabilities
    - Support native methods (IPv4 ID randomization scenarios,etc)
  - Added support for IPv4 and IPv6 fragmentation and revised IPSEC discussions
  - Added identification type tables and processing rules for implementation guidance
  - Modified writeup but optional hash mode remains largely as described in -05

- IPv4
  - Removed IP header id field mucking
  - Also I-DPD does not assume sequence-based progression of id space

- Added recommended solutions to deal with certain security threats

IPv6 Processing Rules

IPv6 I-DPD Processing Rules

IPv6 Fragment Header	IPv6 IPSEC Header	IPv6 I-DPD Header	SMF IPv6 I-DPD Mode Action
Present	*	*	Use Fragment Header I-DPD Check and Process for Forwarding
Not Present	Present	*	Use IPSEC Header I-DPD Check and Process for Forwarding
Present	*	Present	Invalid, do not Forward
Not Present	Present	Present	Invalid, do not Forward
Not Present	Not Present	Not Present	Add I-DPD Header,and Process for Forwarding
Not Present	Not Present	Present	Use I-DPD Header Check and Process for Forwarding

IPv4 Processing Rules

IPv4 I-DPD Processing Rules

df	mf	fragment offset	IPSEC	IPv4 I-DPD Action
1	1	*	*	Invalid, Do Not Forward
1	0	nonzero	*	Invalid, Do Not Forward
*	0	zero	not Present	Tuple I-DPD Check and Process for Forwarding
*	0	zero	Present	IPSEC enhanced Tuple I-DPD Check and Process for Forwarding
0	0	nonzero	*	Extended Fragment Offset Tuple I-DPD Check and Process for Forwarding
0	1	zero or nonzero	*	Extended Fragment Offset Tuple I-DPD Check and Process for Forwarding

Relay Set Updates

- Added section in document to specify TLVs related to CDS operation in an NHDP mode

- Revised Appendices describing candidate CDS algorithms

TLV Definitions

- SMF Relay Algorithm ID TLV
  - Identifier for Relay Algorithm type in use

Value	Algorithm
0	S-MPR
1	E-CDS
2	MPR-CDS
3-127	Reserved for Future Assignment
128-255	Experimental Space

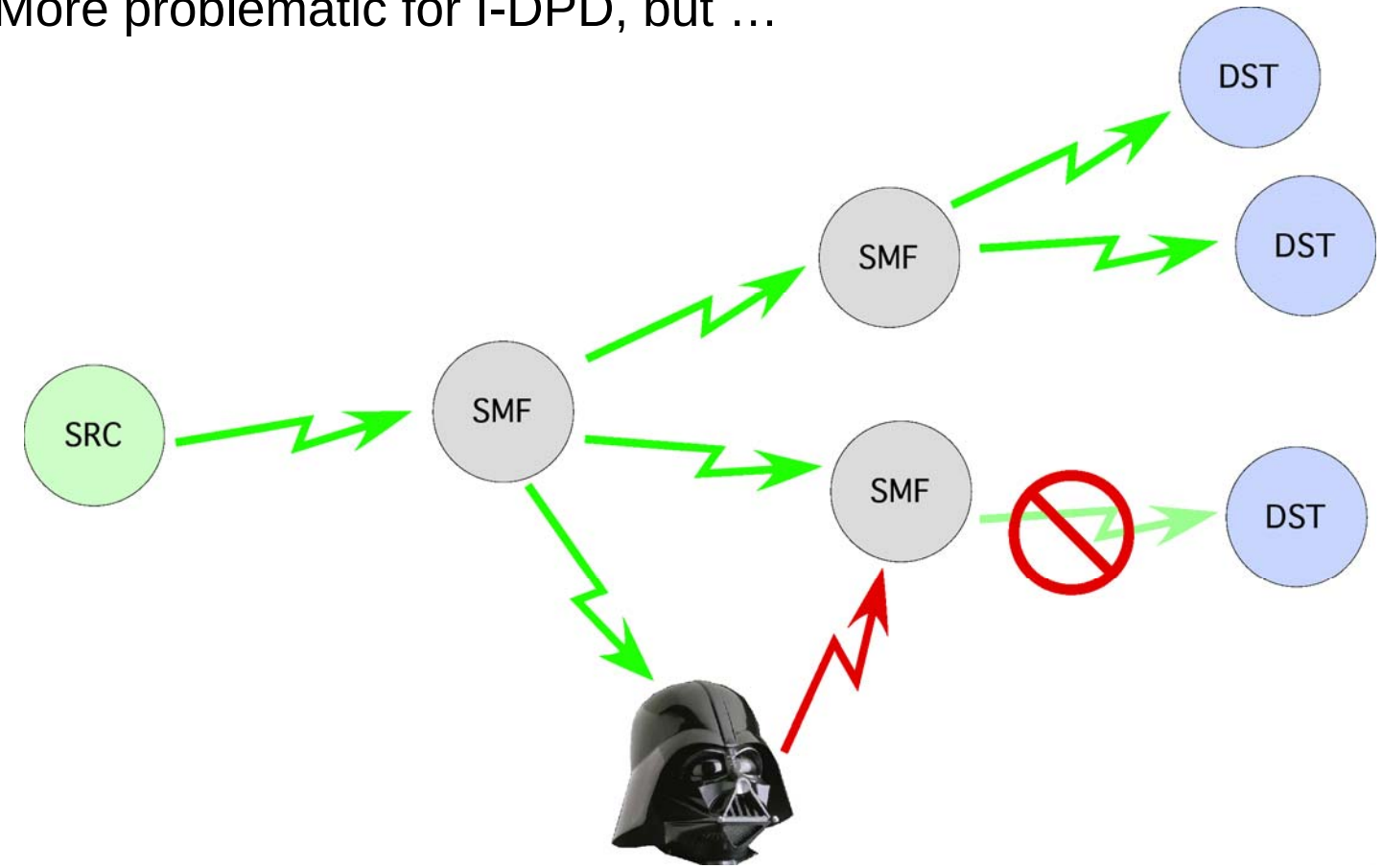
- Router Priority TLV
  - Priority values what can be used in CDS election process
  - 1-hop and 2-hop variant defined

SMF Security Issues

- SMF reliance on Duplicate Packet Detection can make it subject to some denial-of-service attacks
- The concern is low-cost, high-payoff attacks that deny forwarding of valid packet flows
- Note this does not address the issue of malicious packet “spamming” or spoofing

Evil Pre-Play Attack

- Malicious user monitors a packet flow and “pre-plays” or spoofs packets with predictable DPD identifier that results in valid packets being considered “duplicate”.
  - More problematic for I-DPD, but …

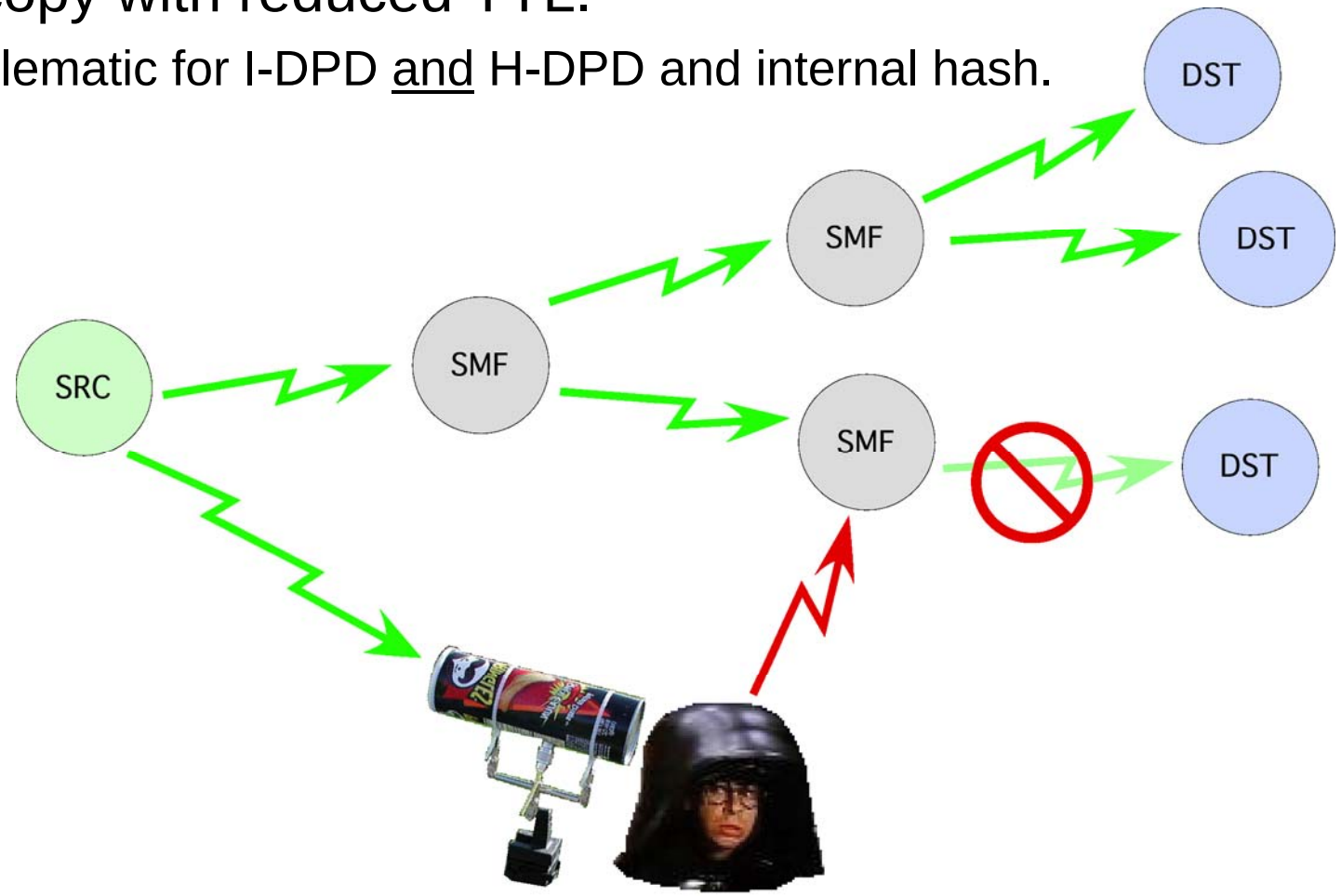


Possible Solutions to DPD Pre-play Attack

- Cryptographically-strong hash algorithm for H-DPD
  - May be computationally complex
  - No HAV possible for IPv4 or IPSEC flows anyway
- “Internal Hash” used in conjunction with I-DPD
  - Lower complexity hash algorithm may suffice.
  - May also “strengthen” IPv4 ID field use for I-DPD

More Evil Pre-play Attack using a “Wormhole”

- Malicious user previews incoming packets, and pre-plays copy with reduced TTL.
  - Problematic for I-DPD and H-DPD and internal hash.



Candidate Solution to “Wormhole” Pre-play Attack

- Keep TTL/ Hop Limit of forwarded packets with DPD table state
- If a duplicate packet arrives with a larger TTL than the previously forwarded version, forward the duplicate and update TTL in DPD table
- There may some topology cases when this “solution” may temporarily cause unnecessary duplicates, but this is expected to be exceptional.