On Using 'Symbiotic' Relationship to Repel Network Flooding Defense

draft-haddad-mipshop-netflood-defense-00

What is a 'Symbiotic' Relationship (SR)?

- An SR is a unidirectional cryptographic relation between two nodes or between one node and a set of nodes.
- Computing a CGA address requires generating first a 128-bit random parameter (R0) then using it with other parameters to derive the 64-bit IID.
- When establishing an SR with node (B), (A) has to generate a new 128-bit random parameter (R1) from hashing B's public key together with (R0).

What is a 'Symbiotic' Relationship? (2)

- After auto-configuring its CGA address, (A) sends (R0) to (B).
- In the right context, SR enables (B) to provide a "proof of relationship" with node (A) to a third party, by "at least" disclosing R0 and signing with its private key.
- In all subsequent exchanges, (A) does not need to disclose (R0) to any other node, i.e., it discloses (R1) only.

Using SR to Repel Network Flooding Attack

- SR can be used to protect the network from flooding attack launched by mobile and/or multi-homed node (Nomadicity).
- Our proposal consists on requesting the MN to establish an SR with the dedicated node and to confidentially send (RO) to that node. Let's assume that such node is the AR.
- When an attack is launched by a malicious MN, the AR sends a signed "Flushing Request" message to (each) CN, in which it discloses the "proof of relationship" with the MN.

Using SR to Authenticate Fast BU Messages (FMIPv6)

- When moving between different ARs, the SR becomes also a bidirectional SA between the MN and the AR. Hence, it allows the MN to authenticate the Fast BU message without any additional signaling.

Questions?
Thank You!