DENYING THE DENIAL - SECURING 6LOWPAN AGAINST DOS

Mitigation strategies to minimize vulnerabilities in IoT 802.15.4 protocol stack

# Objective

To come up with a secure protocol suite enabling mitigation strategies against

1. Layer 2, 3, 4 Denial of service vulnerabilities
2. Identity spoofing attacks

**How shall we do it?**

Allow the master device to validate/invalidate a packet in just 16 bytes, no need of deep packet inspection. Proposed packet structure for this scheme:

16 bytes hash || AES encrypted packet (follows IPv6 packaging)

**How are these hash bytes useful?**

This 16 bytes hash is

1. Unique to each device and provides context to communication between the master and slave devices.
2. This provided context helps against identity spoofing, denial of service through flooding and packet replay attacks.
3. Changes every time master and slave devices talk (One-time pad's provable security).
4. Even on capturing packets, no critical information can be revealed.

This 16 bytes hash FH is

FH (RFD (slave) information, Sequence of packet, 16 bit right shifted unique identifier)

*Sequence of packet* and shifting of *unique identifier* are two variables which change every time.

# Costs - Long term and short term

**Short Term**

1. This system is implementable in hardware as well as software and hence can be adopted easily.
2. Computation requirements are added for every packet validation (*Creation of hash for every transmission on RFDs (slave) and Creation of hash + Comparison of hash for every device on master device*).
3. These added computation requirements mean the master device needs to be a capable device whereas slave devices are relatively free of these.

**Long Term**

1. Once adopted this system will remove the bottleneck in IoT industry as a billion dollar business can't be built over an insecure model.
2. In critical systems where network layer vulnerability kills IoT implementation, this implementation is much cheaper as it allows sustainability in the long run.

# State-of-the-Art advancements which exist

1. IEEE 802.15.4 doesn't propose any solution for denial of service, identity spoofing and other network layer vulnerabilities.
2. Key exchange is a challenge as no official protocols have been declared for it.
3. Identity verification can be bypassed easily in the current existing recommendations.

# Limitations

1. So far only intra-PAN systems can be made secure with this proposed scheme.
2. In a global model of IoT, i.e where you need every device to be connected to every other device, it is not applicable. As it allows the slave devices to only talk to the master device.
3. Identity flexible inter-PAN models such as Vehicular IoT do not benefit from this scheme.