Lecture 7

maandag 6 maart 2023 13:21

need to know :

about IEEE802.15.4 5 components of security

security levels

MAC low MAC high

key management

---

today : routing & RPL

↓

routing protocol for low-power and lossy network

In 6LoWPAN, the 'network layer' is split into an adaptation layer and a network layer

↓

6LoWPAN

↓

IPv6 over low power and lossy networks

header compression

fragmentation + reassembly of IPv6 packets usual max payload : 65536 bytes

routing protocols aim to find the best path from source to destination node

in RPL, some nodes may hold the routing table, while others may not.

routing tables contain gateways for destinations

traditional routing protocols are too inefficient for the IoT domain

RPL is based on a DODAG destination-oriented directed acyclic graph

→ has a single root and path to root

? RPL instance

the objective function defines essential configuration parameters

routing metrics speed, energy, storage

optimization objectives

rank calculation strategies

→ rank = relative position to DODAG root

i.e. rank 0 = border router

lowest rank is always preferred, value strictly increases when moving away from root node

rank may be defined in terms of number of hops, throughput / packet delivery rate, use of a battery, etc.
vs. USB-powered

DODAGID IPv6 address of root node

DODAG version specific iteration version of DODAGID
counter
managed (incremented) only by the root node of the DODAG
needed to take topology changes into account

RPL header format

		always present
type	0x155 (ICMPv6) ↳ fixed!	✓
code	identifies type of message	✓
checksum		✓
security		
base format	content depend on type of message being sent	
options	optional fields	

RPL has five control messages

DIO DODAG information update: delivered by each node when
joining network
creating a DODAG
maintaining a node

root node immediately transmits

DIS DODAG information solitication used when wants to join a DODAG or when no DIO messages are received for a long time

can be unicast or multicast
↓ cause unicast DIO (for DIS sender only)
→ cause multiple broadcast DIO
every node starts sending DIO messages
can lead to DDOS 'attack'

DAO Destination Advertisement Object
used to find downward routes; contains path information for route from reachable nodes to sender

DAO-ACK used to confirm route is now known

non-storing mode: only root node has routing table → messages go to root node, then to destination

storing mode: each node maintains routing table

root node decides which mode is active

trickle timer

used to send DIO messages at regular interval

new DIO sent when timer expires or DIO received which changes configuration

self-healing mechanism

global repair mechanism
affects all nodes
runs when inconsistencies are found
new DODAG versions
discard previous DODAG instances

? local repair mechanism

CC (consistency check) messages

used only in secure mode

used to verify consistency of e.g. DODAG ID, counters, timestamps

roughly challenge-response-protocol

nonce requested value → nonce correct value

RPL security features are optional
might be delegated to MAC layer instead e.g. in Contiki-ng

modes:
0 unsecured

1 pre-installed pre-shared keys (PSK)

2 authenticated use PSK to obtain key from authentication authority
implementation left open

RPL security header

T (counter is time) if true, counter field is a timestamp

(encryption) algorithm CCM with AES-128

KIM key identifier mode implicit / explicit

security level LVL

key identifier (key source and key index)

need to know existing level values

replay protection based on consistency check messages ?!

WSN-inherited threats

wireless sensor networks, independent of protocol

blackhole node which discards all packets

selective forward forwards only selected packets, drops the rest

difficult to distinguish from e.g. moving node

mitigation: use disjoint paths but success depends on number of devices under control of adversary

use encryption so that adversary cannot select what to forward

request ACK

intrusion detection system (IDS)

sinkhole advertise manipulated low rank to attract traffic, powerful wh. combined with other attacks

trust-based mechanisms

IDS

specification-/metric-based approaches

tough problem: rank cannot be verified / is set locally

wormhole out of band 'fast link' through which all traffic passes

sybil attacks clone identity of a node; can create (routing loops due to) duplicate hosts in network

recomputing topologies may cause energy depletion

hello/DIO flood send HELLO messages with strong routing metrics / strong signal ⇒ rank will be incorrect

legitimate packets discarded

exhaustion of resources / energy depletion

congestion

RPL specific attacks

similar to WSN attacks, but use specific properties of RPL

rank attacks can be used to carry out sinkhole attacks

RPL version attack → send incorrect version → create new DODAG → energy depletion

local repair attack → similar, but in sub-DODAG

RPL DIS attack → waste energy by ?

neighbor attack → create illusion that device is close by, while it is not

route table poisoning → send bogus DAO packets

delay, packet loss

route table overload → crash node

DIO/DIS/DAO replay attack

outdated / false routing information