IoT Security and Privacy: Basic Knowledge

CPS and IoT Security

Alessandro Brighente

Master Degree in Cybersecurity

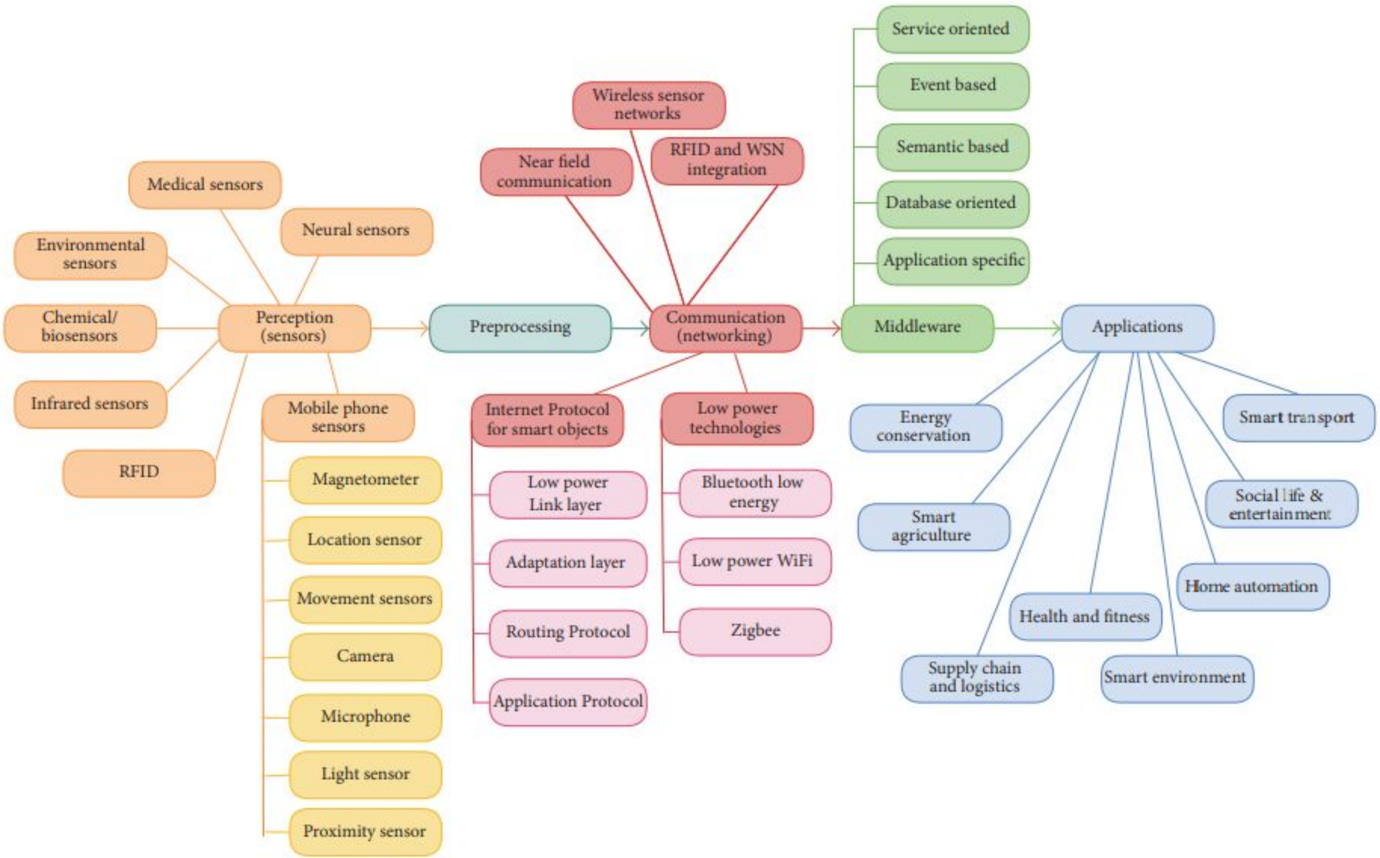
UNIVERSITÀ DEGLI STUDI DI PADOVA

SPRITZ SECURITY & PRIVACY RESEARCH GROUP

The Internet of Things

- An Internet of Things (IoT) describes a group of physical devices equipped with sensing, processing, and communication capabilities able to exchange information with each other over the Internet or other communication networks
- It is a result of development in different fields, including embedded devices, sensor networks, automation, and control systems
- We have already seen examples of internet of things

IoT Taxonomy



IoT Architecture

- An IoT system consist of three main layers: i) devices, ii) edge gateway, iii) cloud
- Devices are the *things*, i.e., those devices equipped with sensors and actuators that collect data and report it to the gateway
- Gateway is a data aggregation system to pre-process data, securing connectivity to cloud, the event hub, and sometimes fog computing
- Cloud contains the applications built using microservices, storage, event queuing, and messaging systems

Network Architecture

SPRITZ
Security & Privacy
Research Group

Università
degli Studi
di Padova

- We expect IoT networks to comprise a huge number of devices
- We use IETF IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN)
- Usually operates on top of IEEE 802.15.4 defined for low rate - PAN
- For industrial networks, we have IPv6 over TSCH model of IEEE 802.15.4e (6TiSCH)
- Data transport is provided by IETF Constrained Application Protocol (CoAP), ZeroMQ, and MQTT

IEEE 802.15.4

- Low Rate PAN standard specifying lower protocol layers (physical and MAC)
- Addressing uses a 64 bit node ID and 16 bit net ID
- Basic channel access mode is carrier-sense multiple access with collision avoidance (CSMA/CA)
- Check whether channel is occupied, if not send a RTS packet and wait for CTS
- If CTS received, send packet
- Uses data packets and ack packets

IEEE 802.15.4

Data Packet format

1 byte	2 bytes	1 byte	0/2/4/10 bytes	0/2/4/10 bytes	variable	2 bytes
Len.	Flags	Seq. No	Dest. Address	Source Address	Data payload	CRC

Also indicates whether security is enabled

ACK Packet format

1 byte	2 bytes	1 byte	2 bytes
Len.	Flags	Seq. No	CRC

IEEE 802.15.4 Security

SPRITZ
Security & Privacy
Research Group

Università
degli Studi
di Padova

- A link layer security protocol needs to provide four basic security services: access control, message integrity, message confidentiality, and replay protection
- In 802.15.4 security is handled at the media access control layer
- The application specifies the security stack and sets the appropriate control parameters
- Security is <u>not</u> enabled by default

IEEE 802.15.4 Security

- An application has a choice of *security suites* that controls the type of security protections provided for the transmitted data
- It defines eight different security suites
  - No security
  - Encryption only (AES-CTR)
  - Authentication only (AES-CBC-MAC)
  - Encryption and authentication (AES-CCM)
- Each category that supports authentication comes into three variants depending on the size of the MAC (4, 8, or 16 bytes)

AES-CTR

- confidentiality protection using AES block cypher with counter mode
- The sender breaks the cleartext packet into 16 byte blocks $p_1, \ldots, p_n$ and computes $c_i = p_i \oplus E_k(x_i)$ where each block uses its own counter x
- The receiver recovers the plaintext as $p_i = c_i \oplus E_k(x_i)$
- The counter, known as nonce or IV, is composed of a static flags filed, sender's address, and three separate counters

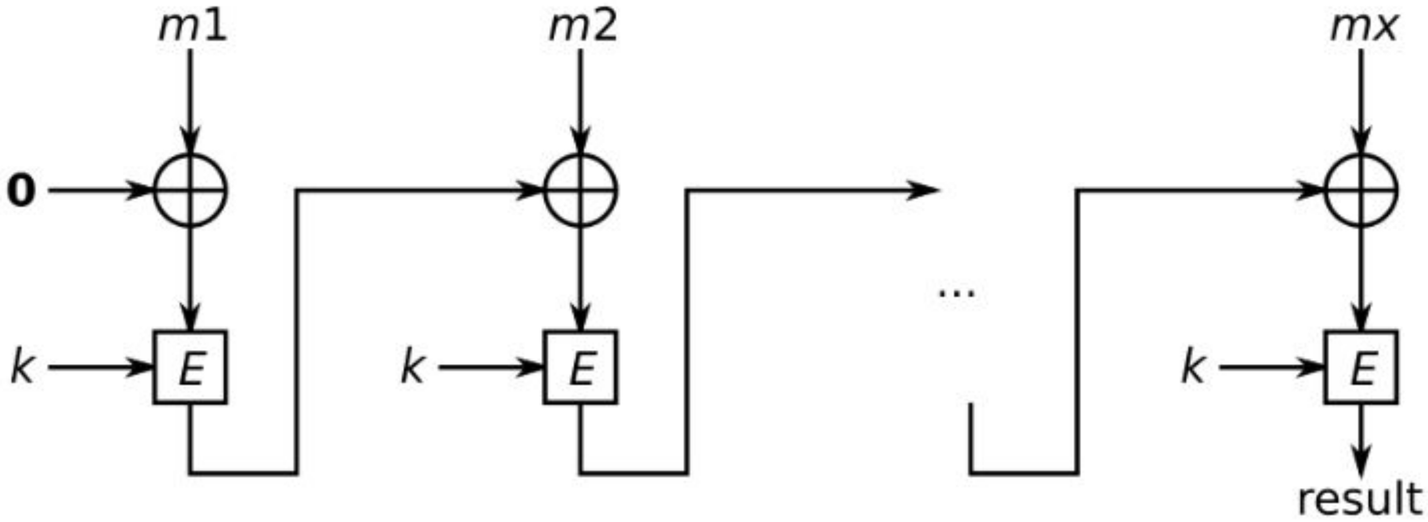
1 byte	8 bytes	4 bytes	1 byte	2 bytes
Flags	Source address	Frame Ctr	Key Ctr	Block Ctr

AES-CTR

- The frame counter is maintained by the hardware radio and the sender increments it after encrypting each packet
- The key counter is under application control
- Requirement: nonce must never repeat within the lifetime of any single key and frame and key counter should prevent nonce reuse
- The 2 bytes block counter ensures that each block will use a different nonce value

AES-CBC-MAC

- Provide integrity protection via CBC-MAC algorithm
- It can only be computed by parts having symmetric key
- MAC protects the packet headers and data payload



AES-CCM

- Provides both encryption and authentication
- It first applies integrity protection over header and data payload using CBC-MAC
- Encrypts data payload and MAC using AES-CTR mode

4 bytes	1 byte	variable	4/8/16 bytes
Frame Counter	Key Ctr	Encrypted Payload	Encrypted MAC

Keying models

SPRITZ
Security & Privacy
Research Group

Università
degli Studi
di Padova

- Govern what key a node uses to communicate with another node
- <u>Network shared keying:</u> single network-wide shared key. Key management becomes trivial and memory requirements are minimal
- However, vulnerable to insider attacks and single key compromise
- A single compromised node can undermine the security guarantees of the entire network
- If we expect nodes to be occasionally compromised or captured, not a good approach

Keying models

- Pairwise keying: limit the scope of every key
- Each pair of nodes shares a different key
- Thus, if a node is compromised, only the security of communication with its pair is undermined
- Comes with an increased overhead
- Each node must store a key for every other node it communicates to
- Select the proper key when communicating with a node
- IoT nodes have limited resources

Keying models

- Group keying: compromise between pairwise and network keying
- A single key is shared among a set of nodes and is used on all links between any two nodes in that group
- Groups can be created based on locations, network topology, or similarity of function
- Partial resistance to node compromise and partial improved management of resources

Secure Group Pairing

- IoT devices need a pairing mechanism which establishes shared cryptographic keys between devices
- Traditional pairing methods employ a centralized approach where a user pairs each device with a trusted IoT gateway through external helper device (e.g., type a pwd on the smartphone)
- However the central gateway is a single point of failure, sometimes preventing devices from communicating → move towards decentralized networking (e.g., OpenThread)

Context-Based Pairing

- In order to limit as much as possible the human intervention, there is an increasing interest in context-based pairing
- Co-located sensors establish shared keys based on the entropy extracted when they observe common events
- Although nice, it is limited to homogeneous devices which need to have the same sensing modalities
- Furthermore, if based on events, it might take some hours or days to have pairing

Zigbee

- Zigbee is a higher layer protocol based on IEEE 802.15.4 to create PAN networks
- It is usually leveraged for home automation, medical device data collection, and small scale projects
- It has a range of 10-100 m in line of sight
- Longer distances are achieved via multi-hop in a mesh network of intermediate devices

Zigbee Devices

Three type of devices in Zigbee:

- Zigbee Coordinator (ZC): root of the network tree and bridge with other networks. Only one ZC, since it is the originator of the network. Trusted node containing e.g., keys
- Zigbee Router (ZR): act as intermediate device to pass data to other devices. They are usually mains powered to always be available
- Zigbee End Device (ZED): minimal functionalities to talk to the parent node. Battery powered and wake up only when has something to say

Zigbee Security

- Zigbee security builds on top of IEEE 802.15.4 security
- Keys and modes we’ve seen for 802.15.4 are basic for Zigbee
- A momentary exception exists for the addition of a previously unpaired and unconfigured device
- We need to assume trust in the initial installation of keys
- Within the protocol stack, we need access policies to cope with the lack of cryptographic separation between different layers

Security Architecture

SPRITZ Security & Privacy Research Group

Università degli Studi di Padova

- Zigbee uses 128-bit keys to implement its security mechanism
- A key can be associated to a network or to a link, acquired via pre-installation, agreement, or transport
- There should be an initial master key obtained via a secure medium
- Establishment of link keys is based on a master key
- <u>Trust center:</u> special device in the network which other services trust for the distribution of secure keys
- Ideally, all devices will have the trust center address and initial master key

Security Architecture

- The security architecture is distributed to different layers

MAC layer

Layer	**Capabilities**
MAC	• Single hop reliable communications • Security level specified by upper layers
Network	• Outgoing frames use the appropriate link key according to routing
Application	• Key established and transport services to both ZDO and applications

Device Authentication

- After joining the network, an end-device needs to exchange security information with the trust center
- Needs to obtain the current network key from the trust center and establish a new end-to-end trust center link key
- It consists of four steps

Device Authentication

- Establish the Trust Center Link Key (TCLK): each device has a pre-installed TCLK typically obtained from the device installation code
- This key is provided to the TC through out-of-band means
- Establish the transport key: the TC and node can derive a transport key from the TCLK
- Distribute the network key: the TC can send to the new node the network key encrypted via transport key
- Establish new link key: as soon as the join procedure is completed, the TC updates the TCLK of the joining device

LoRAWAN

SPRITZ Security & Privacy Research Group

Università degli Studi di Padova

- Personal Area Networks sometimes are not sufficient for IoT purposes
- Long Range (LoRa) is a proprietary radio communication technique
- LoRa Wide Area Network (LoRaWAN) defines the communication protocols and system architecture to create a larger network than PAN
- Also in this case, we consider battery powered resource constrained devices
- It is a cloud based Medium Access Control (MAC) layer protocol
- Manages communications between LPWAN gateways and end-node devices

LoRAWAN Security

- The LoRa alliance designed security measures for LoRaWAN accounting for low power consumption, low complexity, low cost, and high scalability
- As part of the network join procedure, a LoRaWAN end-device establishes a mutual authentication with the LoRaWAN network
- MAC and application messaging are origin authenticated, integrity and replay protected, and encrypted
- End-to-end encryption for application payloads

LoRAWAN Security

- LoRaWAN uses AES, and each device has a unique 128 bit AES key and a globally unique identifier (EUI-64-based DevEUI)
- Allocation of EUI-64 identifiers require the assignor to have an Organizationally Unique Identifier from IEEE registration authority
- LoRaWAN networks are identified by a 24-bit globally unique identifier assigned by the LoRa Alliance

Mutual Authentication

- The Over-the-air activation (or join procedure) test whether both devices know the AppKey
- The proof is obtained by computing an AES-CMAC(AppKey) on the device's join request and by the backend receiver
- CMAC is a One-Key MAC that fixes security deficiencies of CBC-MAC, i.e., the fact that the latter is secure only for fixed-length messages
- Nevertheless, a variation of CBC-MAC

Mutual Authentication

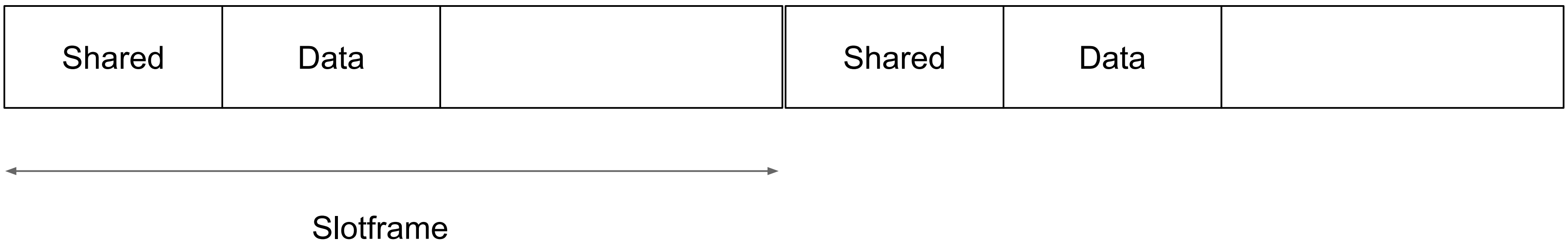
- Two keys are derived by LoRaWAN authentication:
    - Providing integrity protection and encryption of the LoRaWAN MAC commands (NwkSKey)
    - E2E encryption of application payloads (AppSKey)
- NwkSKey is distributed to the LoRaWAN network to prove and verify packet integrity and authenticity
- AppSKey is distributed to the application server to encrypt/decrypt the application payload

IoT Network Formation

- We consider the formation of a 6TiSCH network
- There exists a root node, called Joint Registrar/Coordinator (JRC) which periodically broadcasts Enhanced Beacon (EB) frames
- EBs contain basic network information such as the JRC ID, duration of a timeslot, number of time slots in a slot frame, channel hopping sequence, location of the shared cell
- Pledges are new nodes willing to join a 6TiSCH network

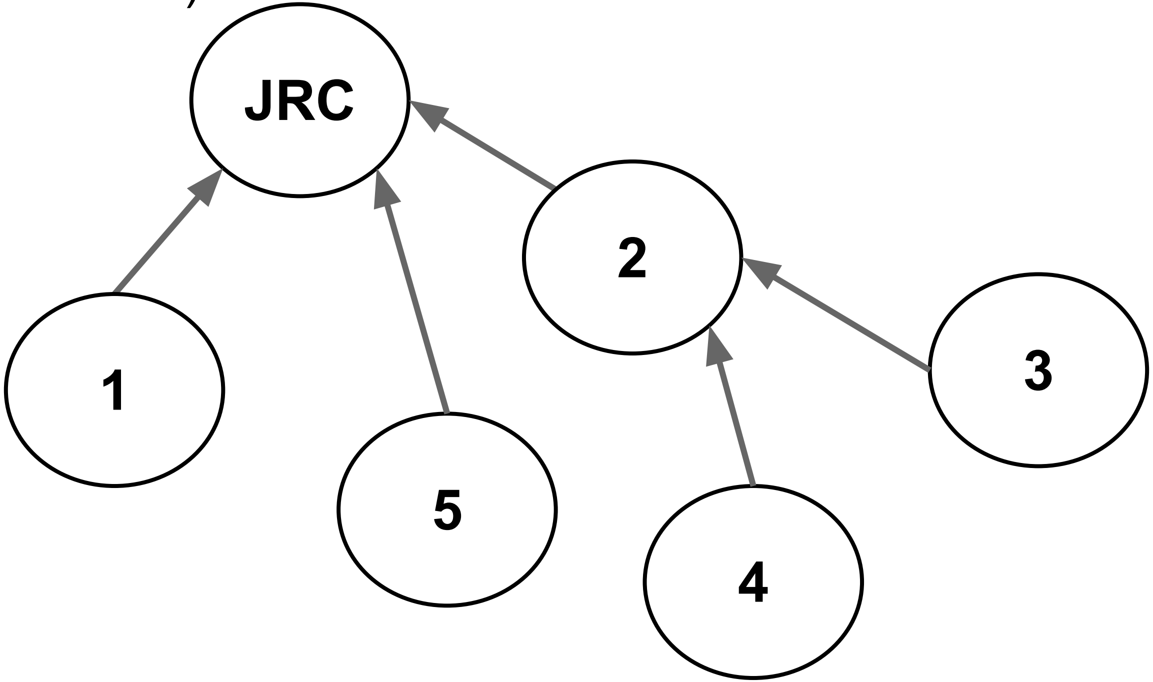
IoT Network Formation

- When pledges want to join the network, they start scanning until they receive a valid EB
- When it receives an EB from an already joined node, it becomes a TSCH synchronized node
- The channel is slotted, and is divided into control slots and shared slots

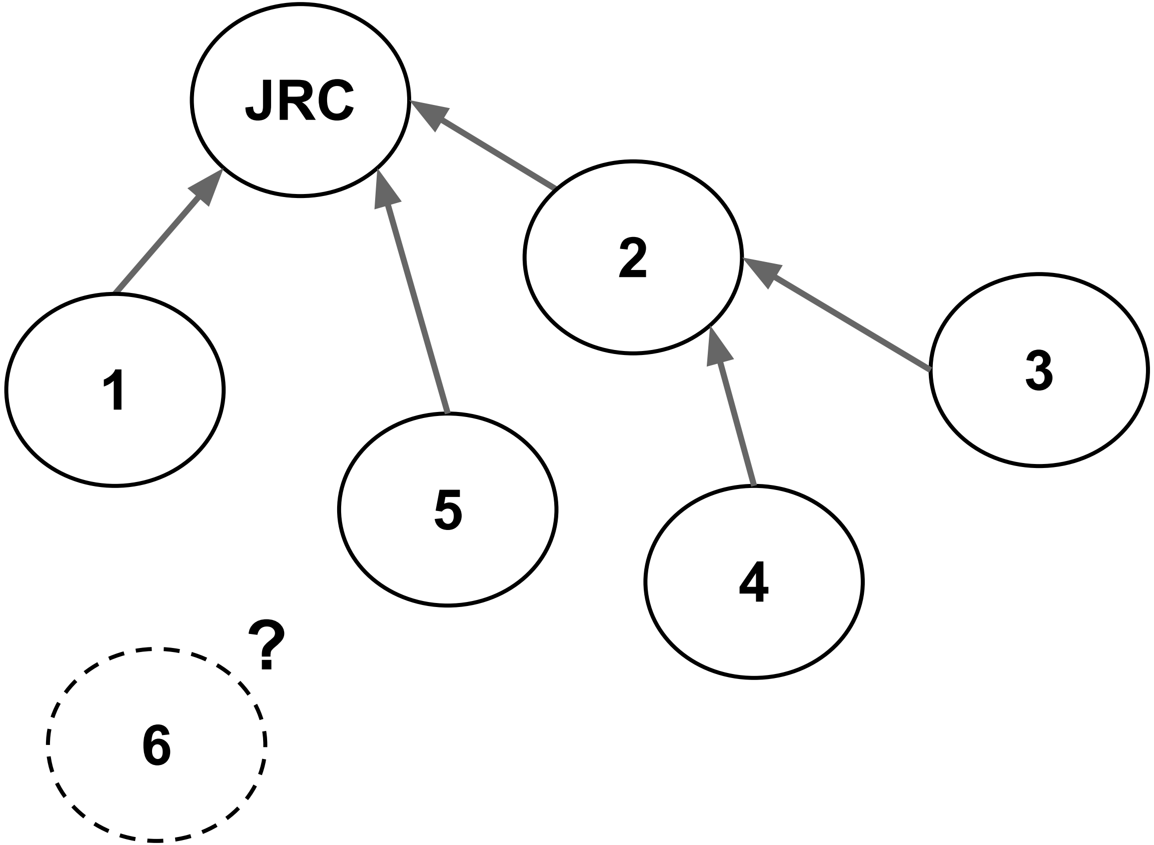


IoT Network Formation

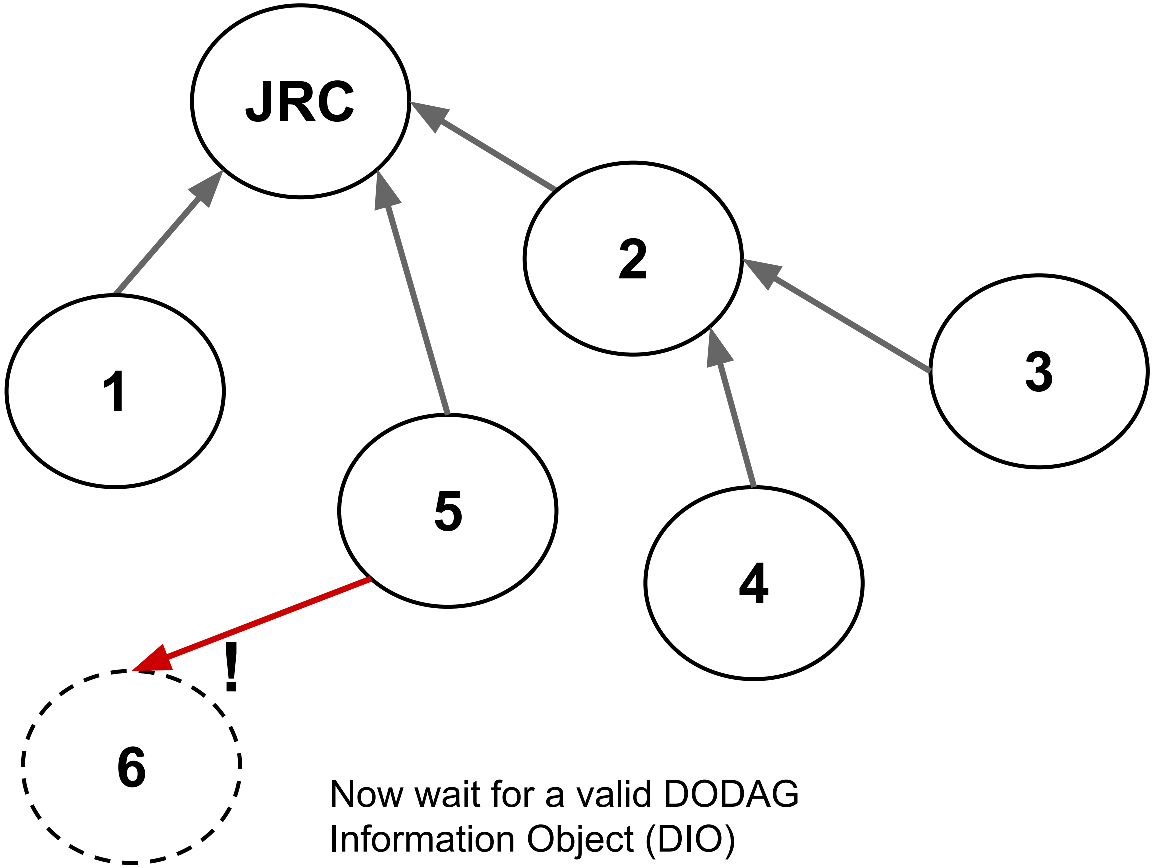
- The network is organized as a Destination Oriented Directed Acyclic Graph (DODAG)



When to Join?

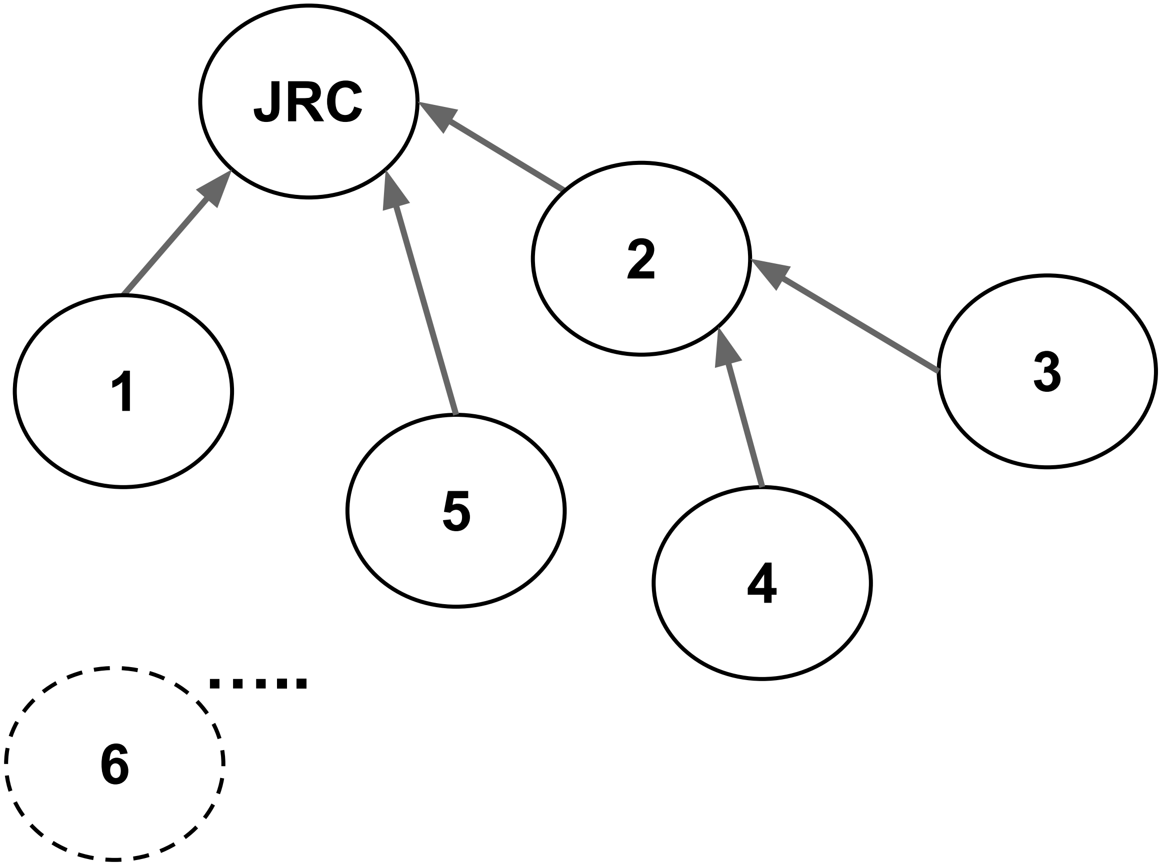


When to Join?

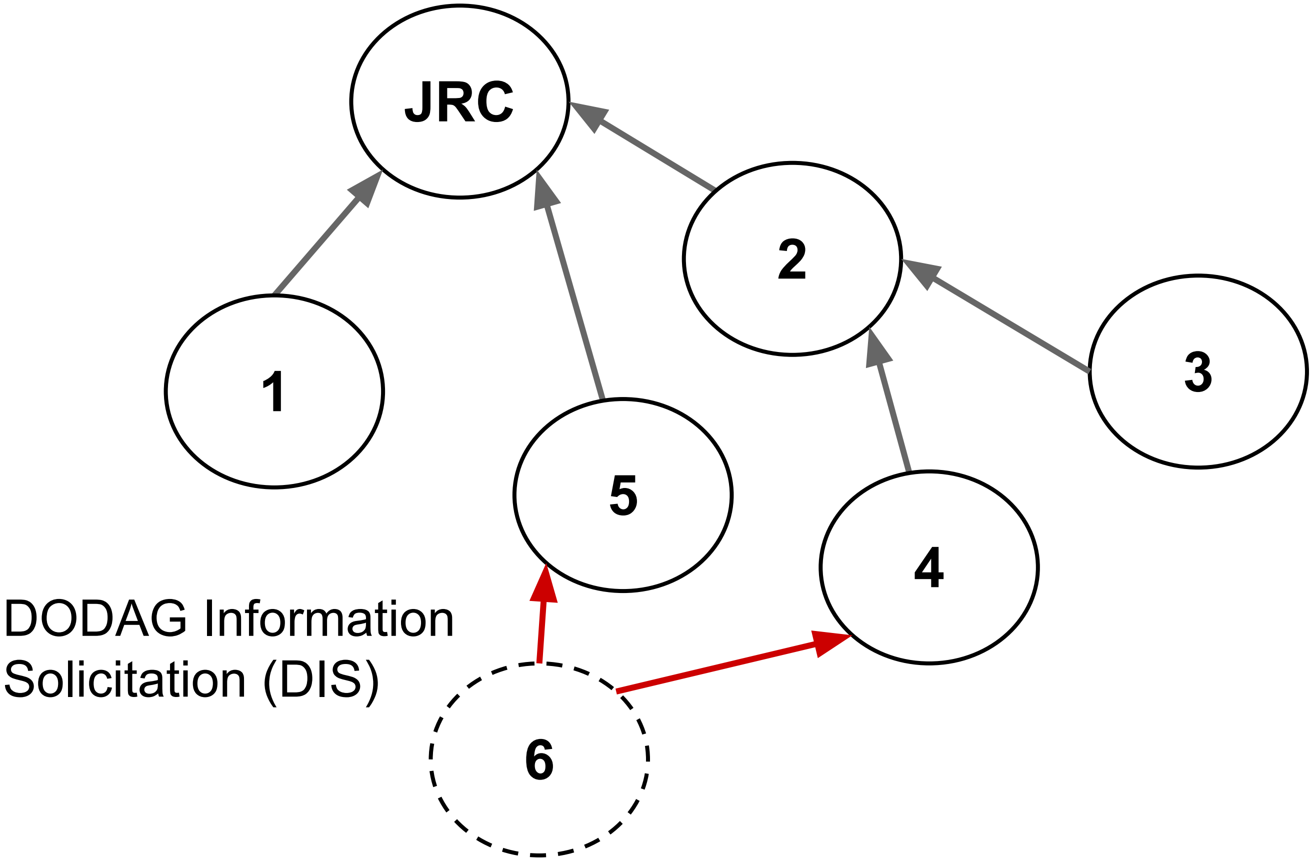


Now wait for a valid DODAG Information Object (DIO)

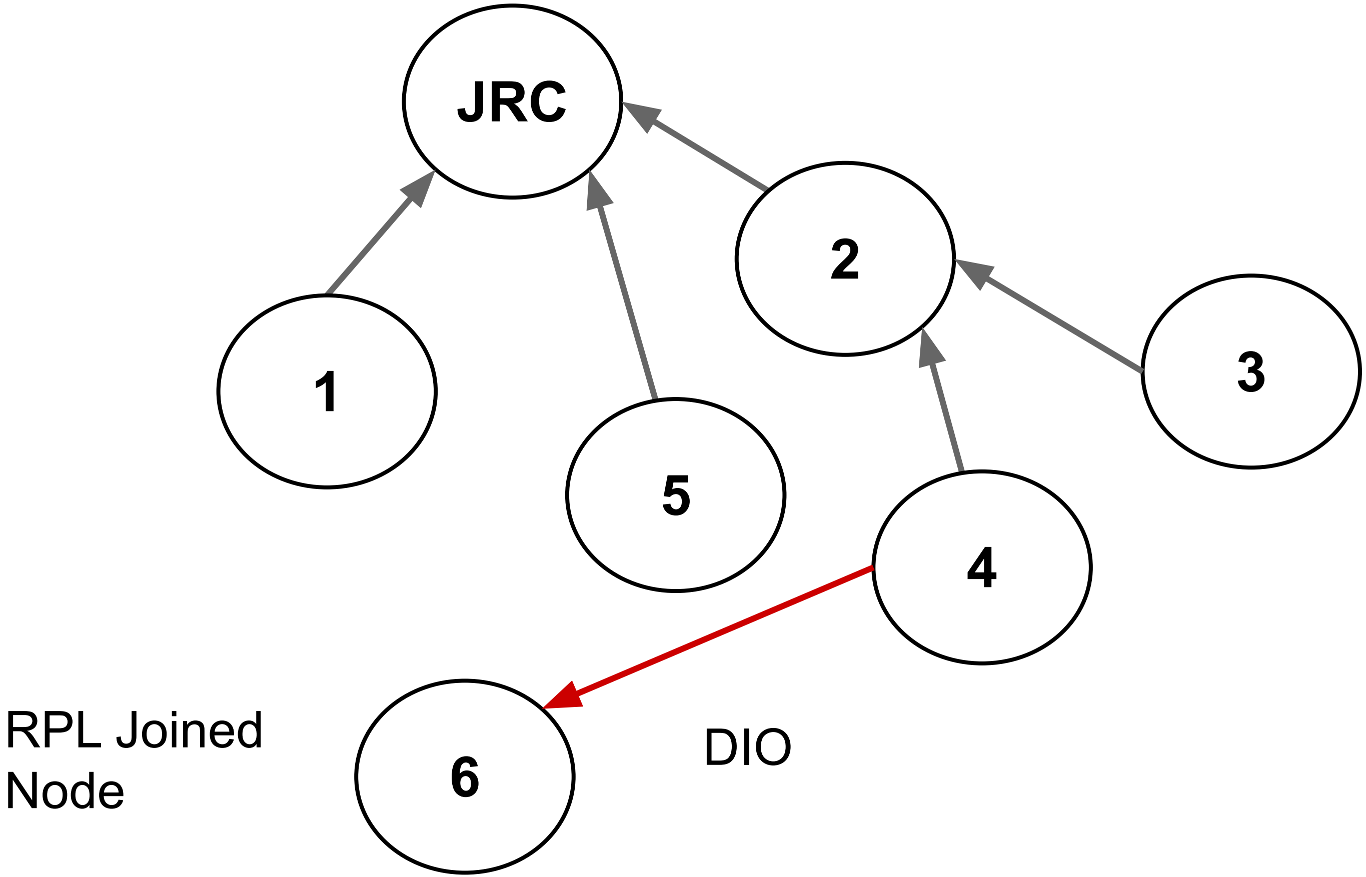
When to Join?



When to Join?



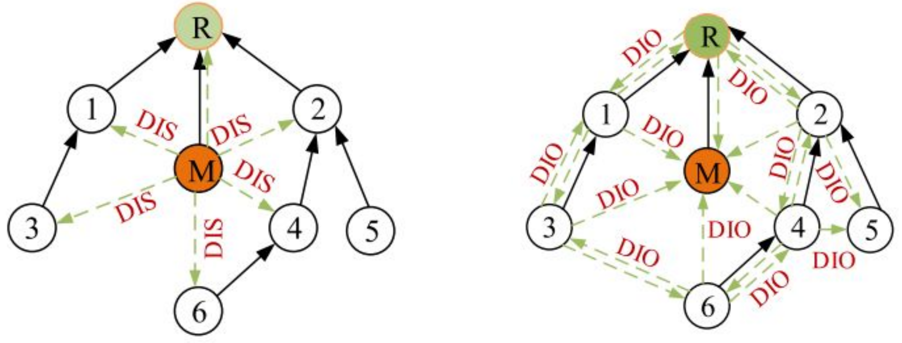
When to Join?



DIS Attack

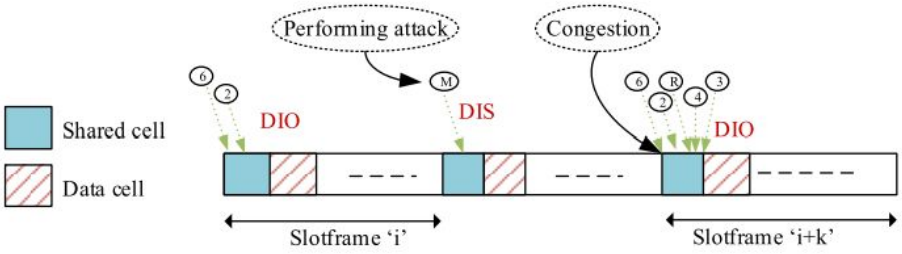
- DIS packets can be sent by arbitrary nodes to solicit the sending of DIO packets
- DIS attack: increase the number of transmissions in DIO packets in the network
- Goal: increase energy consumption and congest the shared slot

DIS Attack



(a) A malicious node transmits its DIS packet.

(b) Legitimate joined nodes transmit their DIO packet in response.



(c) Effect of DIS attack on shared cell's congestion.

Rank Attack

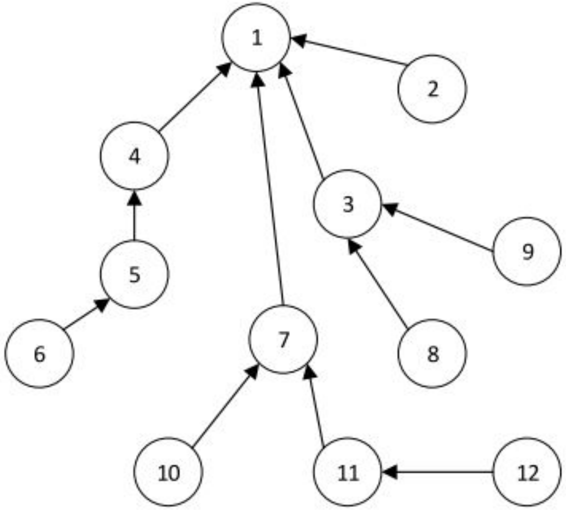
- Each node chooses its parent based on two values: the rank and objective function
- The rank should increase going downward in the DODAG, and the role of the preferred parent selection is to select the one with the best rank
- The objective of the attacker is to manipulate these values to affect the network topology

Rank Attack

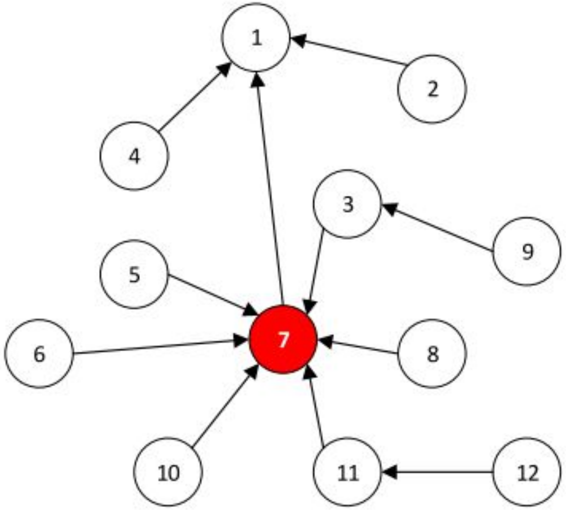
- Manipulation can be performed in two ways
- First, the attacker changes its rank by a specific values based on its neighbors rank value
- Second, the adversary manipulates its rank through the use of a different objective function to deceive legitimate nodes into giving the malicious node a better rank

Types of Rank Attack

- Decreased rank attack: malicious nodes advertise lower rank to other nodes resulting in many of them selecting the adversary as preferred



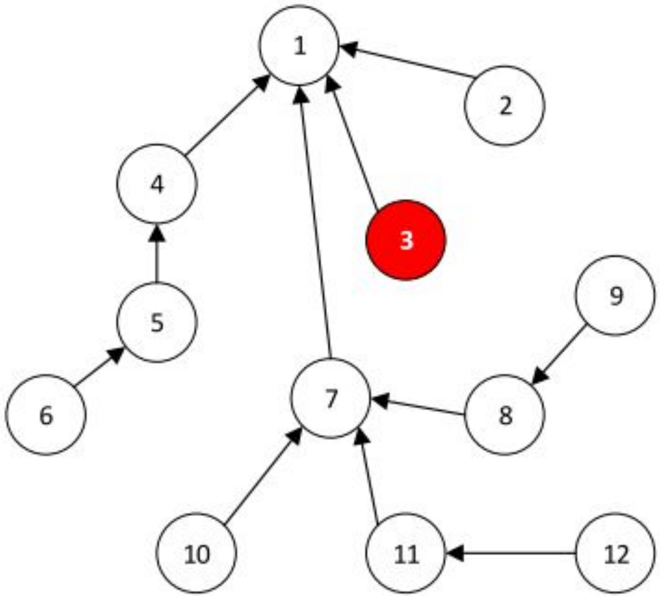
(a) Normal topology



(b) Decreased rank attack

Types of Rank Attack

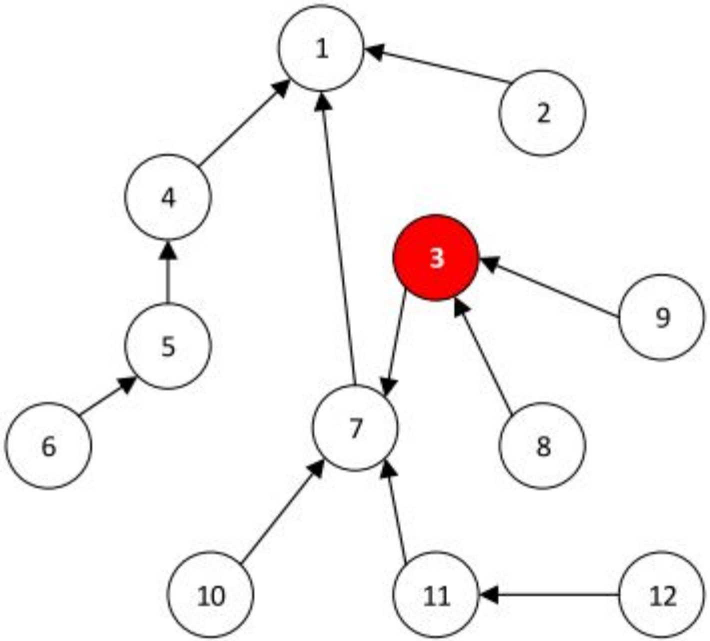
- Increased rank attack: the attacker is near the routing node and advertises higher rank and worse routing metrics
- The idea is to cause topology disruptions and delays, sa nodes will need to select further nodes as parents



(c) Increased rank attack

Types of Rank Attack

- Worst parent attack: the attacker advertises its tru rank but selects the worst parent for itself
- Deceive nodes into connecting to the attacker and cause delays due to the worst path they unwillingly select



Neighboring Attack

- In this attack, the attacker node will forward any received DIO message it gets to its neighboring nodes (no modification)
- This creates the illusion that the original sender is in the range of the neighboring nodes
- Worst case scenario: the original sender has a good rank and adversary's neighbors choose it as preferred parent although being out of range

Neighboring Attack

- Alone, the neighboring attack only causes a slight increase in the end-to-end delay
- However, suitably combined with other attacks gets more dangerous
- An adversary could launch a DIS attack to get DIO messages with better metrics, then selecting one of these messages to perform a neighbor attack, increasing the effect of such an attack

RPL Storing Mode

- RPL can work in a Point-to-Point fashion, i.e., create traffic between two nodes that are not root nodes of the DODAG
- In storing mode, each node keeps a downward routing table for its sub-DODAG and use it to forwards P2P traffic
- In practice, traffic goes upward up to a common ancestor of sender and destination that routes the packet to the destination node

RPL Storing Mode Attack

SPRITZ Security & Privacy Research Group
Università degli Studi di Padova

- Routing table overload: the adversary sends many bogus routes (via DAO) until the node saturates
- Route table falsification: a malicious node advertises fake routes to other nodes that might exists but not be part of the attacker’s sub-DODAG causing packet losses or longer delays
- All these attacks also cause resource exhaustion due to the increased overhead and repetitive repair attempts

Attacks Inherited from WSN

- Wireless Sensor Networks (WSNs) are the networks from which IoT was born
- Therefore, IoT inherited part of the routing attacks that existed in WSNs
- Although the working principle is the same, attacks needed to adapt to the new IoT paradigm

Blackhole and Selective Forward

- In a blackhole attack, a malicious node(s) will drop all packets it receives instead of forwarding them (DoS)
- To be less detectable, an attacker may decide to selectively drop packets (i.e., only forward RPL control messages) → selective forward or greyhole attacks
- Selective-forward attacks cannot be detected nor mitigated by the self-healing mechanisms of RPL because they pass control messages

Sinkhole attacks

- Malicious node(s) try to be sink for as much nodes as possible by advertising a fabricated link with better metrics
- Sinkhole by themselves are not very powerful, they need to be combined with other attacks
- These attacks can be performed by advertising DIOs with better metrics or having several adversaries directing all passing traffic toward another adversary

Wormhole attacks

- To create this attack, two adversaries need to cooperate to create a tunnel between them and transmit traffic through it instead of the regular path
- Three ways to create a wormhole:
  - Packet encapsulation: malicious nodes use a legitimate path between them and encapsulate packets to hide the hop count
  - Relay: deceive nodes to be neighbors
  - Out-of-band link: create links that are not part of the network

Clone ID and Sybil attacks

- In Clone ID attack, a malicious node(s) takes the identity of another legitimate node
- In Sybil attacks, each malicious node takes several identities from legitimate nodes
- With sybil attacks an attacker can submit forged information to manipulate the system, disturb the routing topology and reputation-based systems
- Can be mitigated by adding location information and DHTs

Mitigation Techniques

- To detect some of these attacks (or their declinations) there have been many proposals in terms of Intrusion Detection Systems (IDSs)
- Signature-based IDSs: use a database of signature patterns of the attacks
- Anomaly-based IDSs: create a normal behavior profile and compare the current observations with the normal behavior
- Specification-based: create a normal profile based on protocol specification
- Hybrid IDSs: combine two of the aforementioned methods

Placement of IDSs

- Centralized IDS: the IDS resides either on the root node or on a dedicated host and uses the traffic passing by to detect attacks
- In many cases, it is required that the central node of the IDS send periodic request for updates to unmonitored areas
- Advantage: most of the heavy works occurs inside a powerful node, usually capable of performing firewall functionalities as well
- On the other hand, challenging to monitor the network during the attack

Placement of IDSs

- Distributed IDS: each node will have a full IDS implementation, making it responsible for detecting attacks around it
- Usually nodes collaborate to increase the efficiency of the detection
- However, this approach consumes a lot of resources throughout the network
- It is usually required to optimize the IDS periodically to minimize its effects

Placement of IDSs

SPRITZ Security & Privacy Research Group

Università degli Studi di Padova

- Hybrid IDS placement: to get the best of both worlds
- Central nodes with more resources are responsible for computationally intensive tasks (analyzing data, decision making)
- Normal nodes are responsible for lightweight duties (e.g., monitoring neighbor nodes, send info about traffic passing through them, responding to requests from central nodes)
- Requires optimization