SRNET: A Real-time, Cross-based Anomaly Detection and Visualization System for Wireless Sensor Networks

Eirini Karapistoli[1], Panagiotis Sarigiannidis[2], and

Anastasios A. Economides[1]

[1] COmputer Networks & Telematics Applications (CONTA) Laboratory
Department of Information Systems,
University of Macedonia, Thessaloniki, Greece
[2] Department of Informatics and Telecommunications Engineering,
University of Western Macedonia, Kozani, Greece

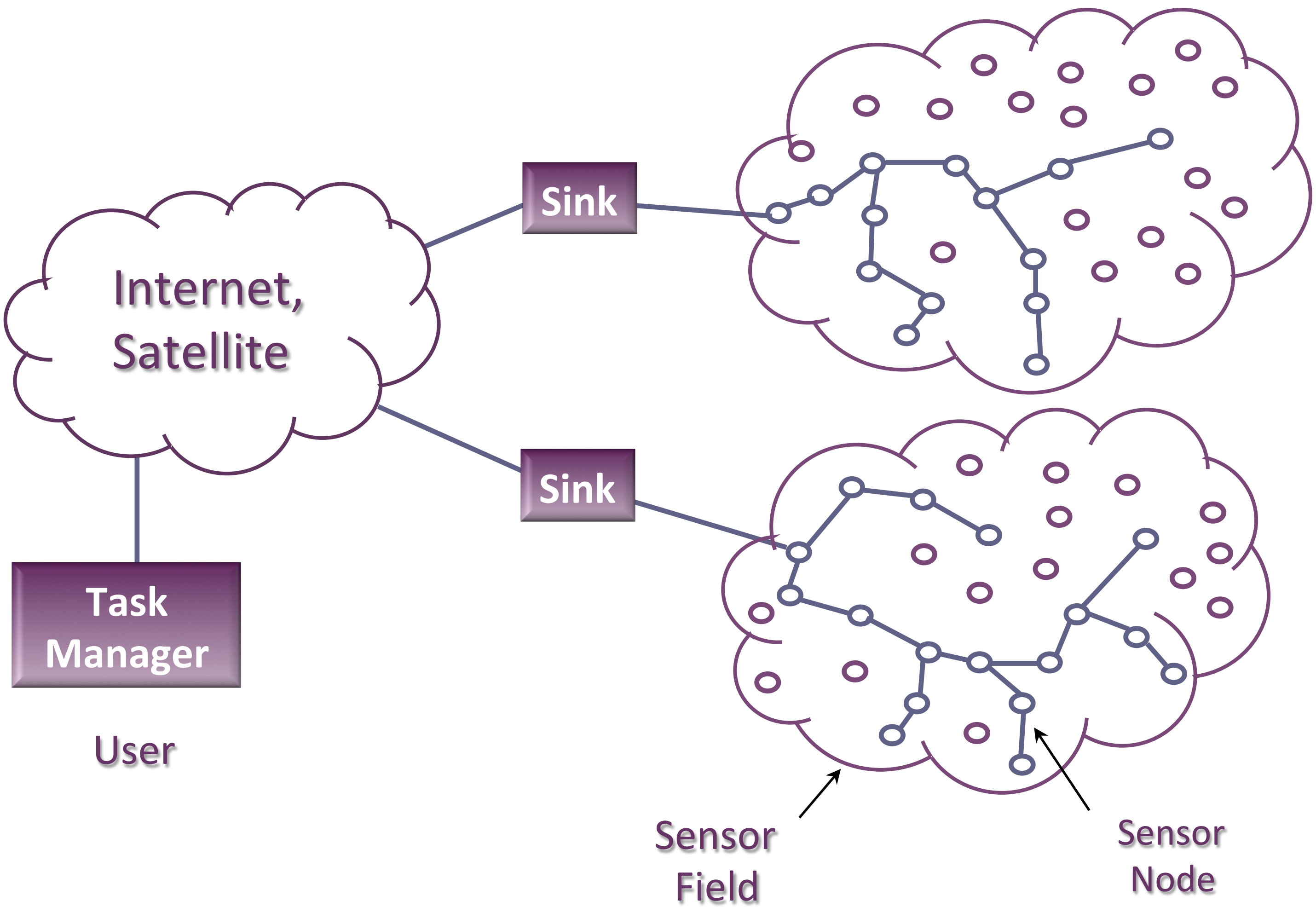
Overview

- An introduction to Wireless Sensor Networks (WSNs)
- Security in WSNs
  - Are WSNs secure?
  - Attacking the IEEE 802.15.4 standard
- The SRNET Visualization System
  - The Graphical User Interface (GUI)
  - The Four Coordinated Views
- Performance Evaluation
- Conclusions

Definition

- The term Wireless Sensor Network (WSN) refers to a wireless network consisting of a large number (often in the order of thousands) of autonomous, battery-operated sensors that are spatially distributed in an area of interest in order to:
  a) cooperatively monitor physical or environmental conditions, such as temperature, sound, vibration, motion, pollutants, etc.,
  b) store the measurements temporally, and
  c) transmit the collected sensory information upon request to a remote server for further processing.
- In achieving these objectives, the sensor nodes have sensing, processing and communication capabilities.
- Depending on the application, sensor nodes may generate massive amounts of data.

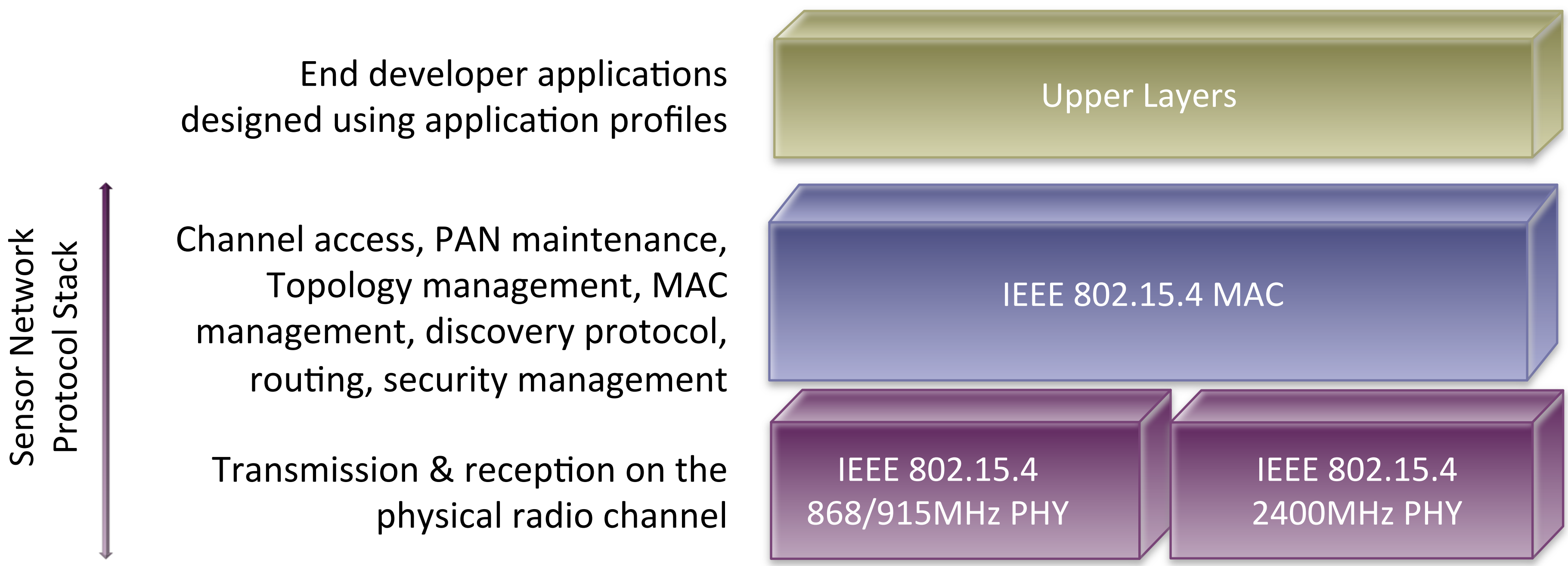
WSN Architecture



Standardization

The IEEE 802.15.4 Standard

- The IEEE 802.15.4-2011 standard is a dominant communication standard developed to provide low-power and highly reliable wireless connectivity among inexpensive, battery-powered devices.
- The standard defines the physical "PHY" and medium access control "MAC" layers.



IEEE 802.15.4 MAC Basics

- Network formation
  - Star, cluster-tree, and P2P topologies
- Mode of operation
  - Non-beacon enabled mode: where the coordinators do not emit regular beacons
  - Beacon-enabled mode: where the Personal Area Network (PAN) coordinators rely on a superframe structure to enable transmission and reception of message.
- Channel accessing
  - Slotted CSMA-CA
  - Unslotted CSMA-CA
- Low power operation (sleep mode)

- Device Types
  - Full Function Devices (FFD)
  - Reduced Function Devices (RFD)

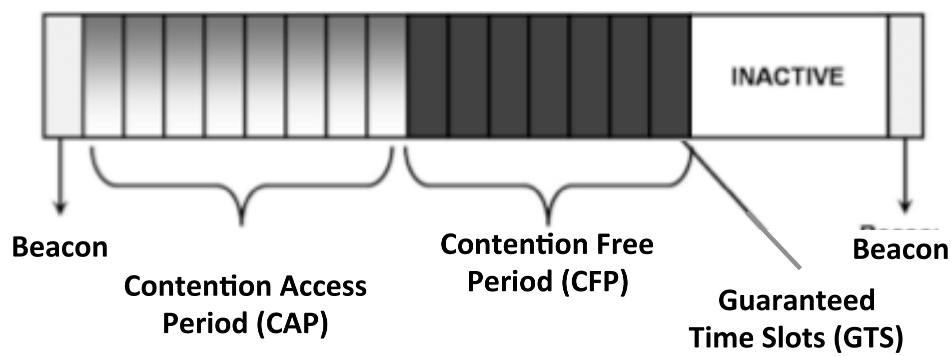
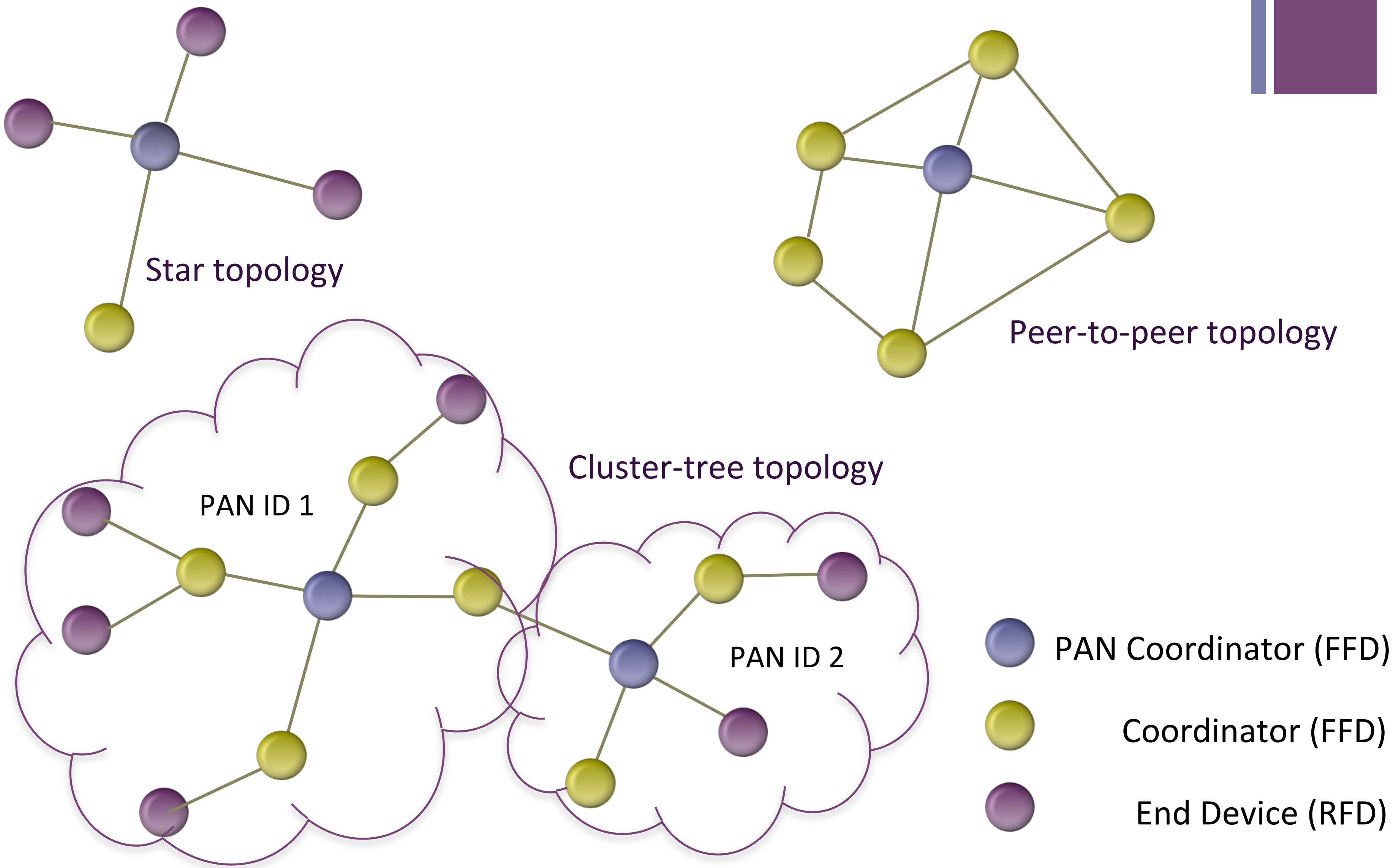


Figure – Superfame structure

Network formation modalities



IEEE 802.15.4 MAC Basics

- Network formation
  - Star, cluster-tree, and P2P topologies
- Mode of operation
  - Non-beacon enabled mode: where the coordinators do not emit regular beacons
  - Beacon-enabled mode: where the Personal Area Network (PAN) coordinators rely on a superframe structure to enable transmission and reception of message.
- Channel accessing
  - Slotted CSMA-CA
  - Unslotted CSMA-CA
- Low power operation (sleep mode)
- Device Types
  - Full Function Devices (FFD)
  - Reduced Function Devices (RFD)

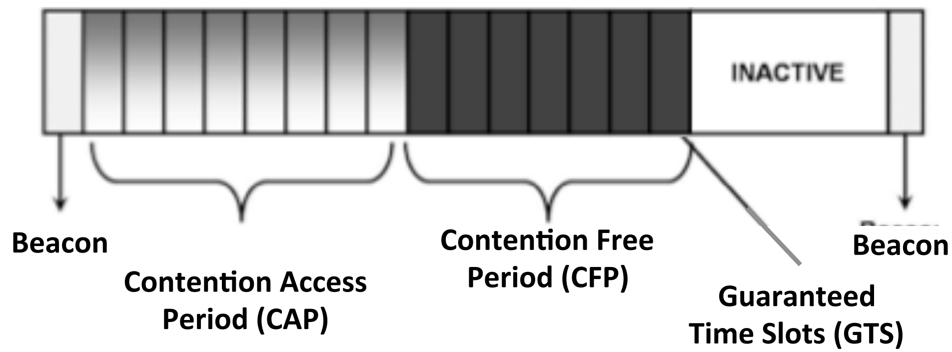
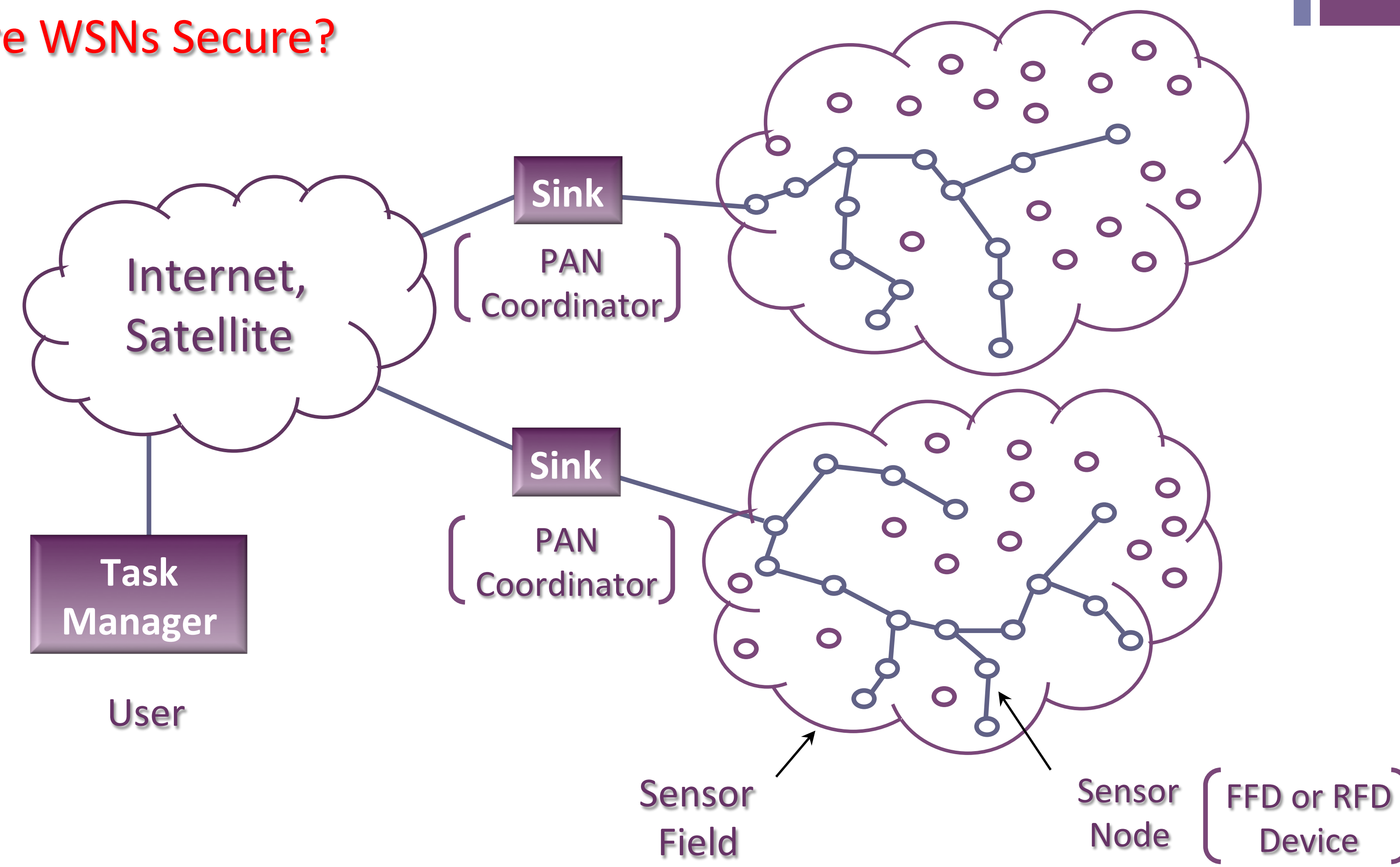


Figure – Superfame structure

WSN Architecture

Are WSNs Secure?



Security Challenges

- ***Constrained Resources***
  - All security approaches require a certain amount of resource for their implementation. However, these resources are very limited in a wireless sensor node.
- ***Unattended Operation***
  - Depending on the function of a particular WSN, the sensor nodes may be left unattended for long periods in an environment open to adversaries. The longer a sensor is left unattended the more likely an adversary will compromise it.
- ***Unreliable Communication***
  - WSNs are vulnerable to security attacks due to the broadcast nature of the transmission medium. This means that eavesdropping can be easily performed.
- ***Self-organization***
  - This inherent feature brings a great challenge to several network security schemes (for instance to public key cryptography techniques).

Threats and Attacks

Attacking the IEEE 802.15.4 Standard

An attack can be defined as the action that intentionally aims to cause damage to the network by exploiting a particular vulnerability

- Attacks can either cause
  - Service degradation or service disablement (i.e., through jamming)
- Types of attacks:

Attack	Mechanism under attack
Hello Flood Attack	The network setup procedure
Denial-of-Service (DoS) attack	The data transmission during the CAP and CFP portions of the superframe
Selective Forwarding & Black hole attacks	The proper forwarding of the sensed data to the BS
Wormhole, Sinkhole & Sybil attacks	The sensor network rooting protocol

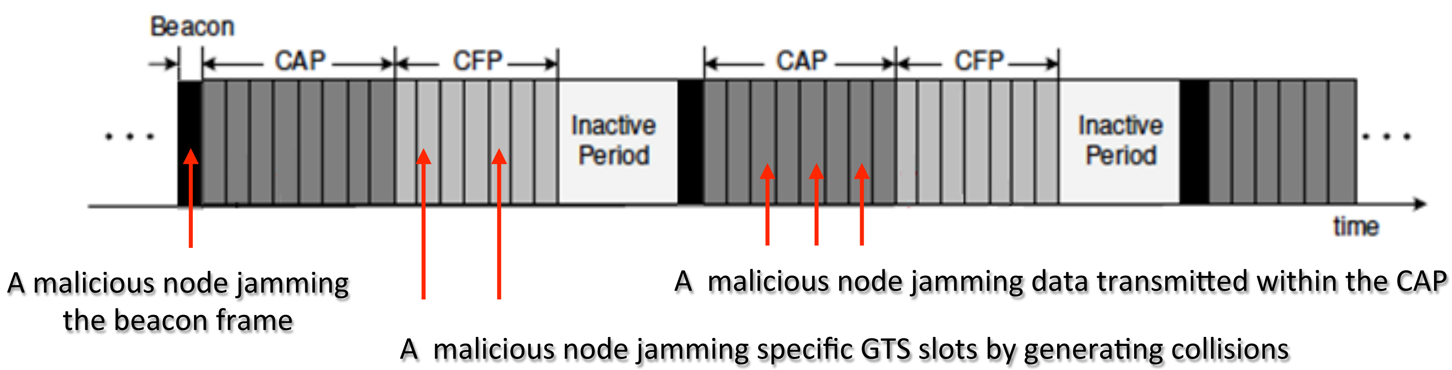
+

Denial of Service (DoS) Attack

- In this attack, the attacker has the ability to jam:
  - either the beacons or
  - the data transmitted within the CAP and CFP portions of the superframe.

- In order to jam the beacons the malicious node must be aware of the start of the superframe boundary.

- In the 2nd case, it may corrupt the communication between a device and the coordinator by jamming one or multiple GTS slots or data slots within the CAP.



Selective Forwarding and Black hole Attacks

- In disseminating packets in the network, it is assumed that nodes faithfully forward the received messages.

- In a selective forwarding attack, a malicious node refuses to forward a subset of the packets it receives and simply drops them.

- More dangerous case: When a malicious node drops all the packets, it performs a black hole attack.

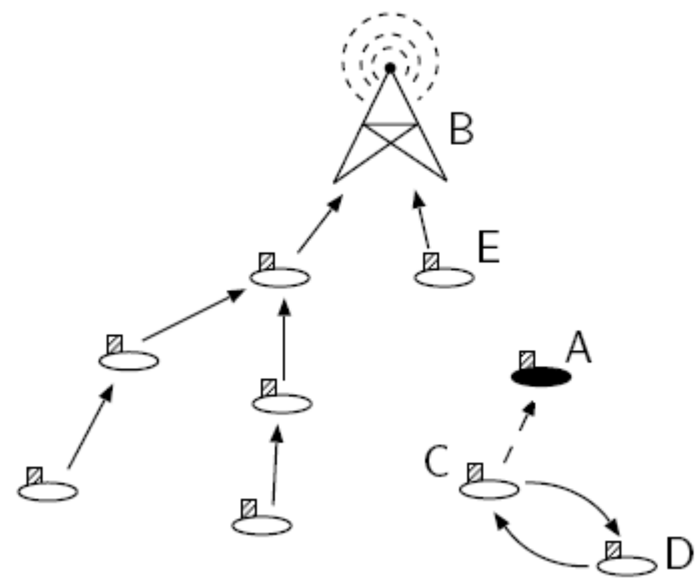


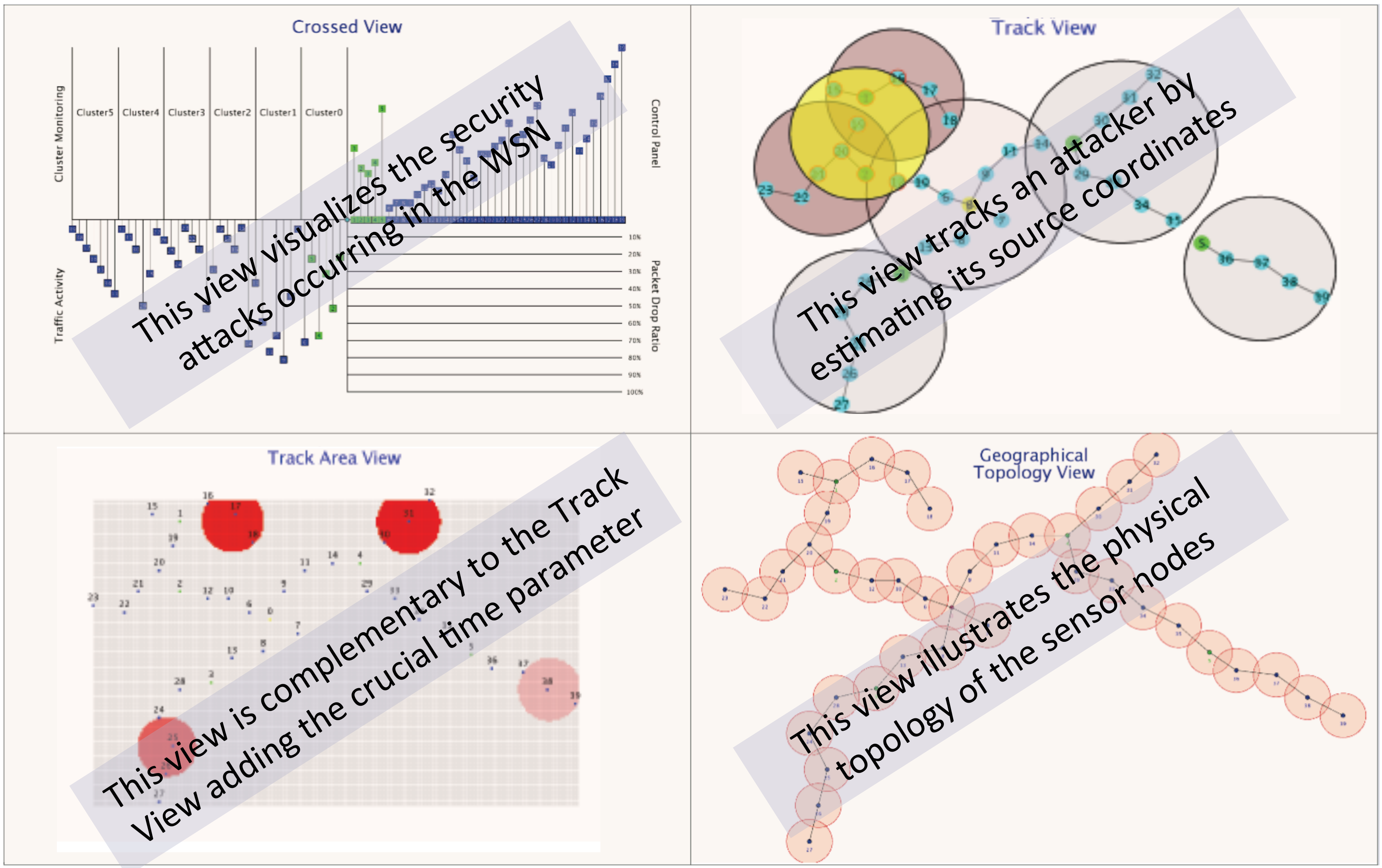
Figure – Node A performs a black hole attack

The Problem

- Despite the fast development of automated Intrusion Detection Systems (IDSs), these systems lack the reasoning ability that is crucial for making decisions about anomalous data that may or may not be a threat, with the typical consequence of an extreme high false positive rate.
- In addition, the scale and complexity of the generated sensory data further challenge the representation and understanding of the security-relevant information.
- Two problems arise as a result:
  1) the problem of information growth on one hand, and
  2) the problem of the increased cyber-/net-criminality on the other hand.

To address the so-called security overload problem
we turned to **visual analytics**

The SRNET Visualization System



Major Features of the SRNET System

- So far, limited work has been contacted on securing IEEE 802.15.4-compliant WSNs using visualization methods.
- We propose a visual-based anomaly detection system to defend against two major classes of sensor network attacks.
- Our system differentiates from existing computer-based IDSs in that:
  - ✓ It can defend against sophisticated attackers that are capable of launching multiple, distributed attacks against the large-scale WSN.
  - ✓ It develops novel views and visual analytics algorithms for visually detecting two major classes of sensor network attacks in one single display.
  - ✓ It provides a multidimensional, consolidated, and effective view of the network status.
  - ✓ It offers a user-friendly animated illustration of potential threads/attacks, which concurrently forms the magnitude of each thread.

+

The Geographical Topology View

- The Geographical Topology View illustrates the physical topology of the sensor nodes resembling a multi-cluster tree structure similar to the IEEE 802.15.4 Std.

- Pre-attentive objects on the Node Link Graph:

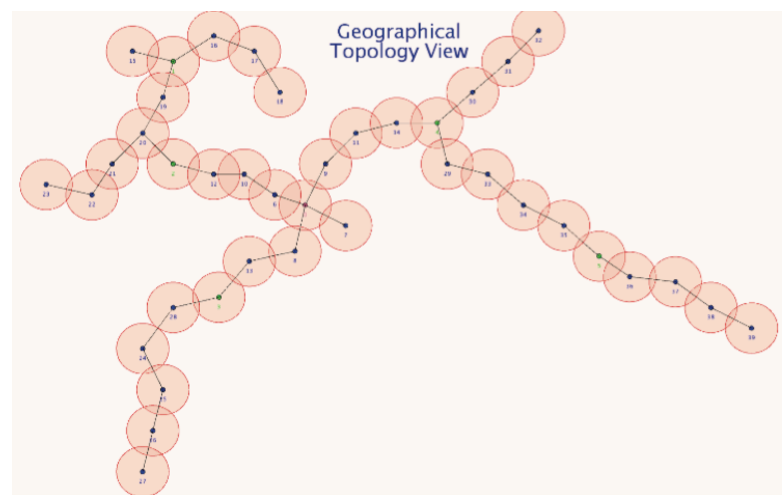
① Form - Shape: Each node is illustrated with a circle.

② Form - Enclosure: A ring shows the transmission range of each node.

③ Color: Differentiates the role of each node. A node can either act as:

- ❑ a coordinator or
- ❑ a device.

④ Position: Physical placement in the 2D sensor field.



The Crossed View

- The Crossed View dictates the type, magnitude, cluster-related location, and evolution of the attack in a simple, animated, and sophisticated way.

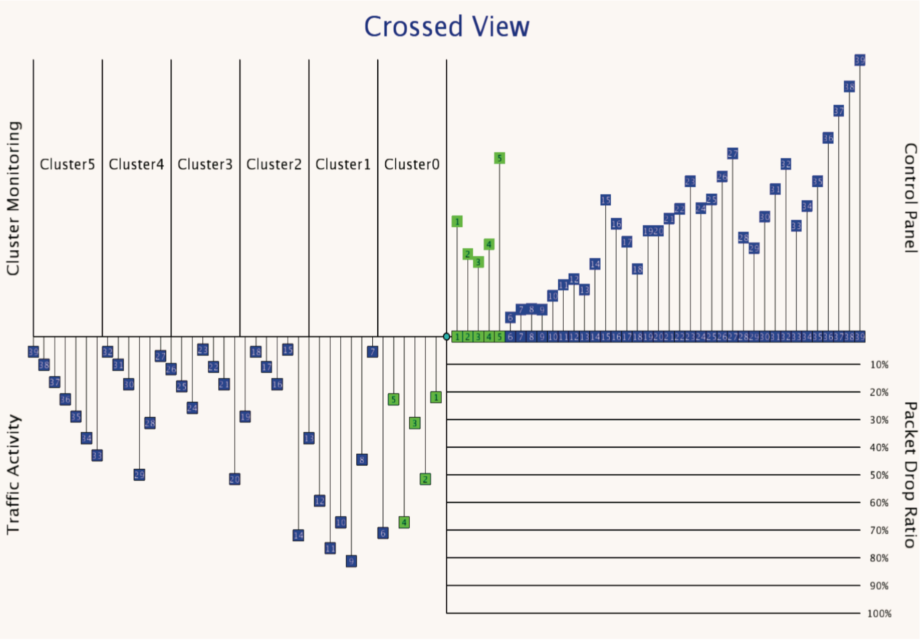
- It provides a 4-to-1 display, formed in a four quarter view.

  - The *Upper-Right Quarter* defines the control panel of the system.

  - The *Lower-Right Quarter* reveals potential Selective Forwarding attacks.

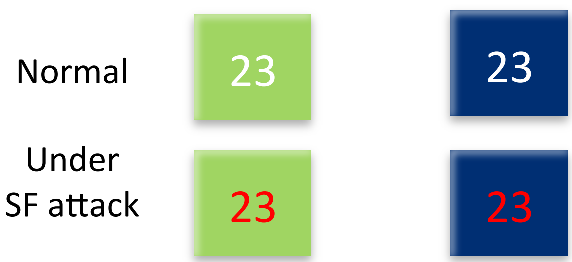
  - The *Lower-Left Quarter* monitors potential jamming collisions.

  - The *Upper-Left Quarter* adaptively encodes system analytics.

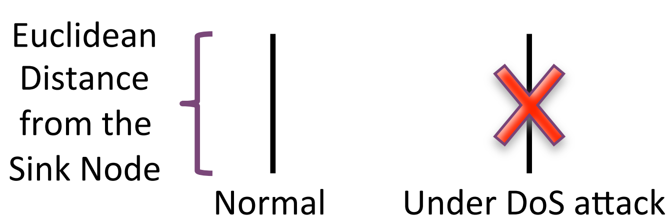


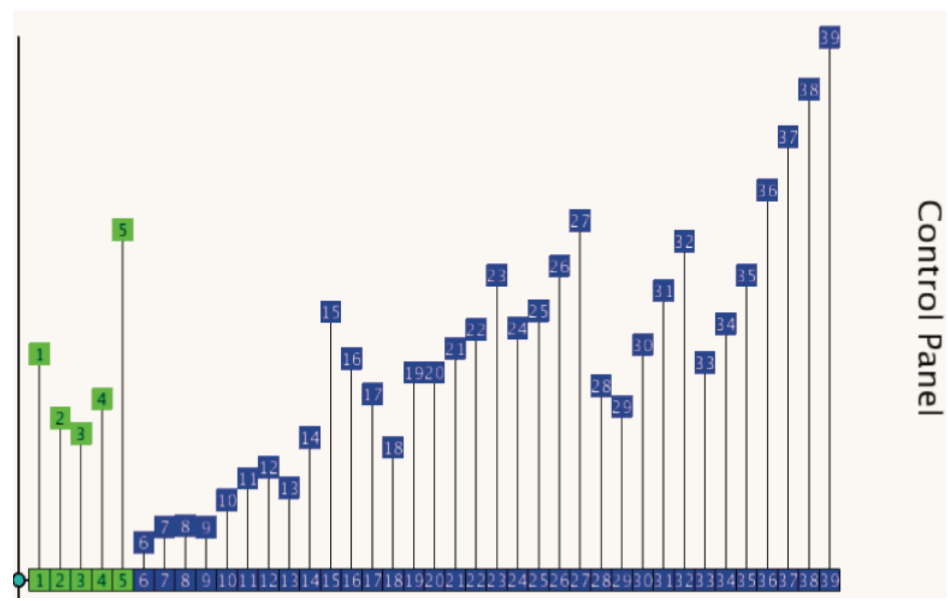
The Upper-Right Quarter$^{(1/2)}$

- The Upper-Right Quarter reorganizes the network topology in a single view.
- The placement of the nodes is static and represents the Euclidean distance from the sink node (also referred to as the central PAN coordinator).
- Pre-attentive objects:
  - Form-Shape/Color: Labeled, Colored Square

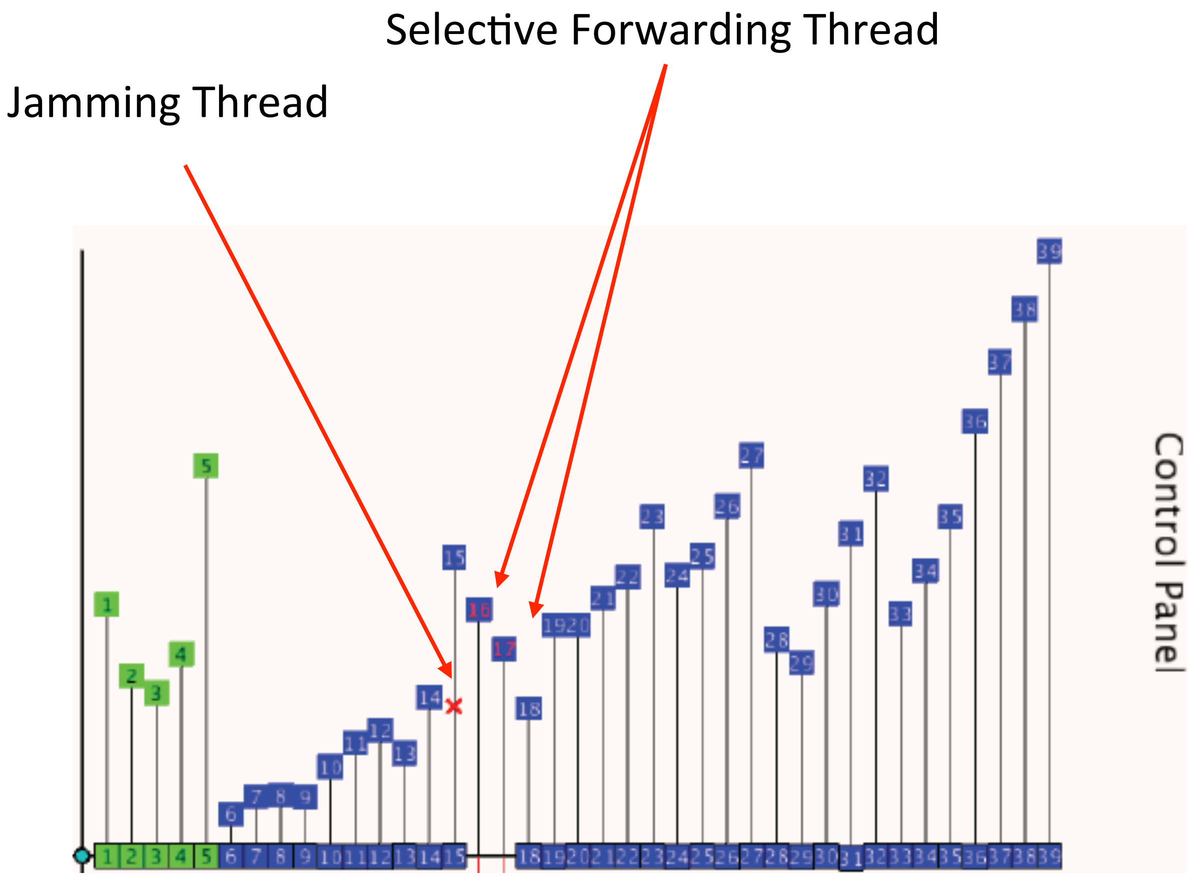


  - Link-Length/Color: Marked Line



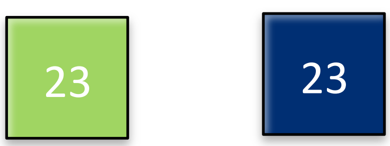


The Upper-Right Quarter$^{(2/2)}$



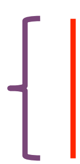
The Lower-Right Quarter(1/2)

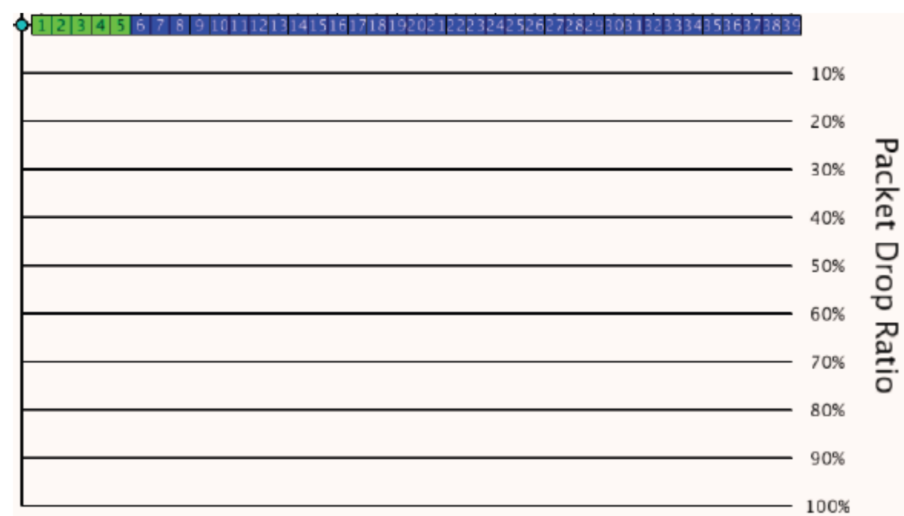
- The Lower-Right Quarter illustrates the percentage of dropped packets each sensor node sustains in a scaled animation.
- Each block representing the sensor node is progressively moving to the observed value as an animated figure.
- Pre-attentive objects:
  - Form-Shape/Color: Labeled, Colored Square



  - Link-Length: Scaled Line.

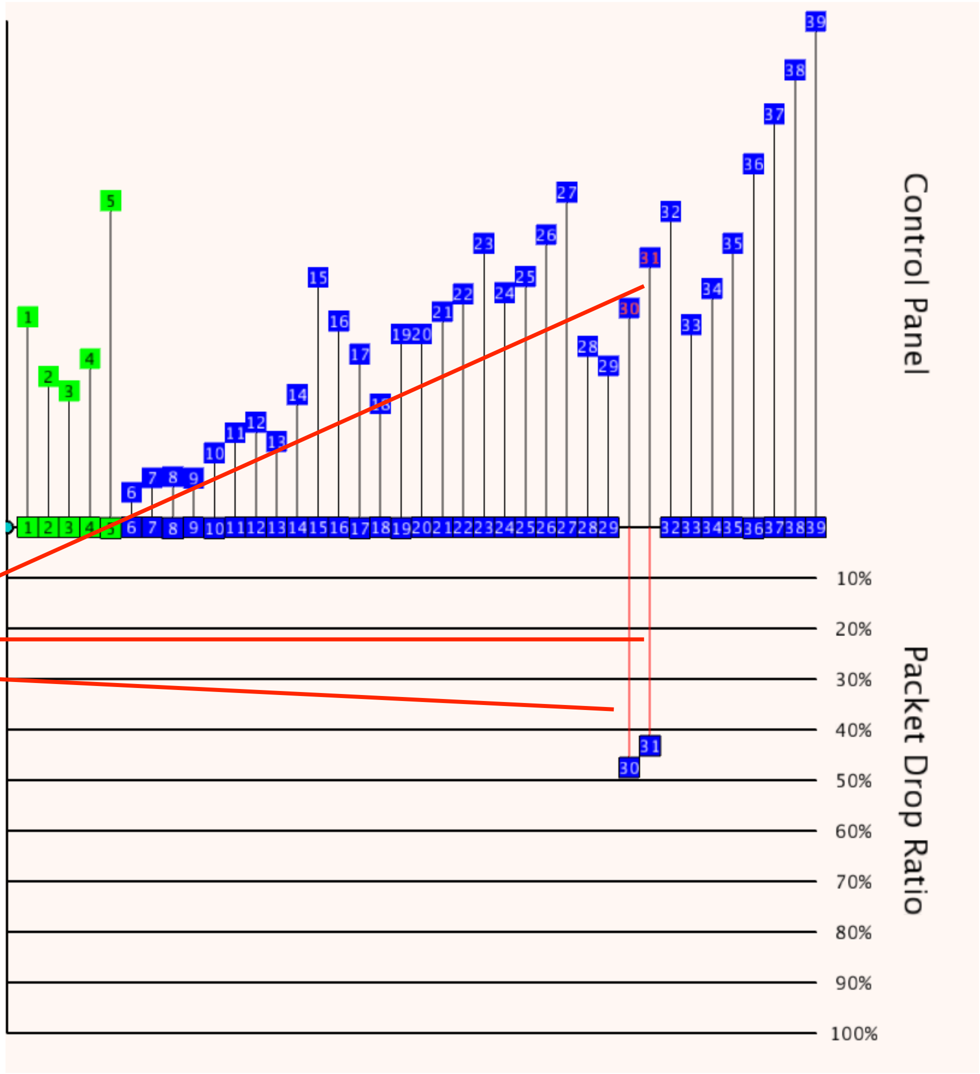
Packet Drop Ratio (0-100%)





The Lower-Right Quarter(2/2)

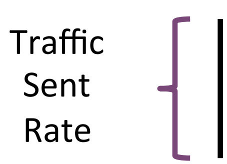
Nodes 30 and 31 are under Selective Forwarding Attack. These nodes suffer a packet drop ratio > 40%.

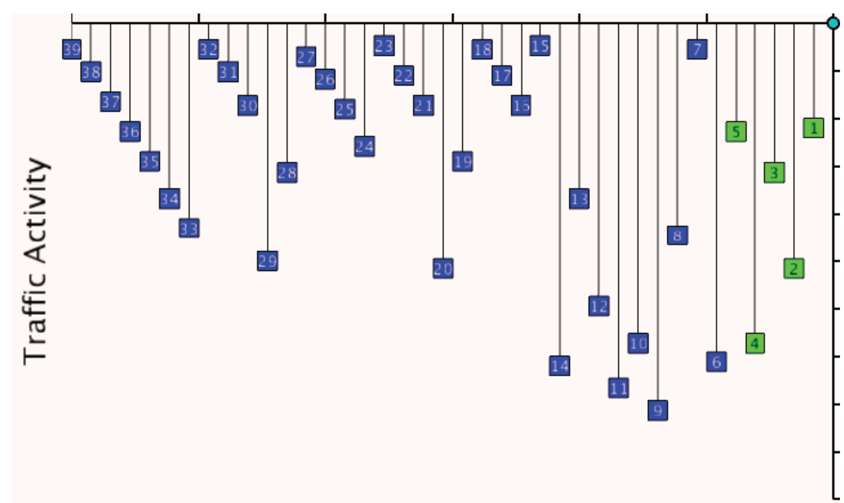


The Lower-Left Quarter(1/2)

- The Lower-Left Quarter effectively shows potential jamming attacks. Sensor nodes, shaped a squares, are constantly moving showing a normal operation.
- The height where a node is placed reveals its traffic sent rate in packets/sec.
- A sensor node that is under jamming attack is unable to send and forward data, hence the number of sent and received data packets tends to zero.
- Pre-attentive objects:
  - Form-Shape/Color: Labeled, Colored Square

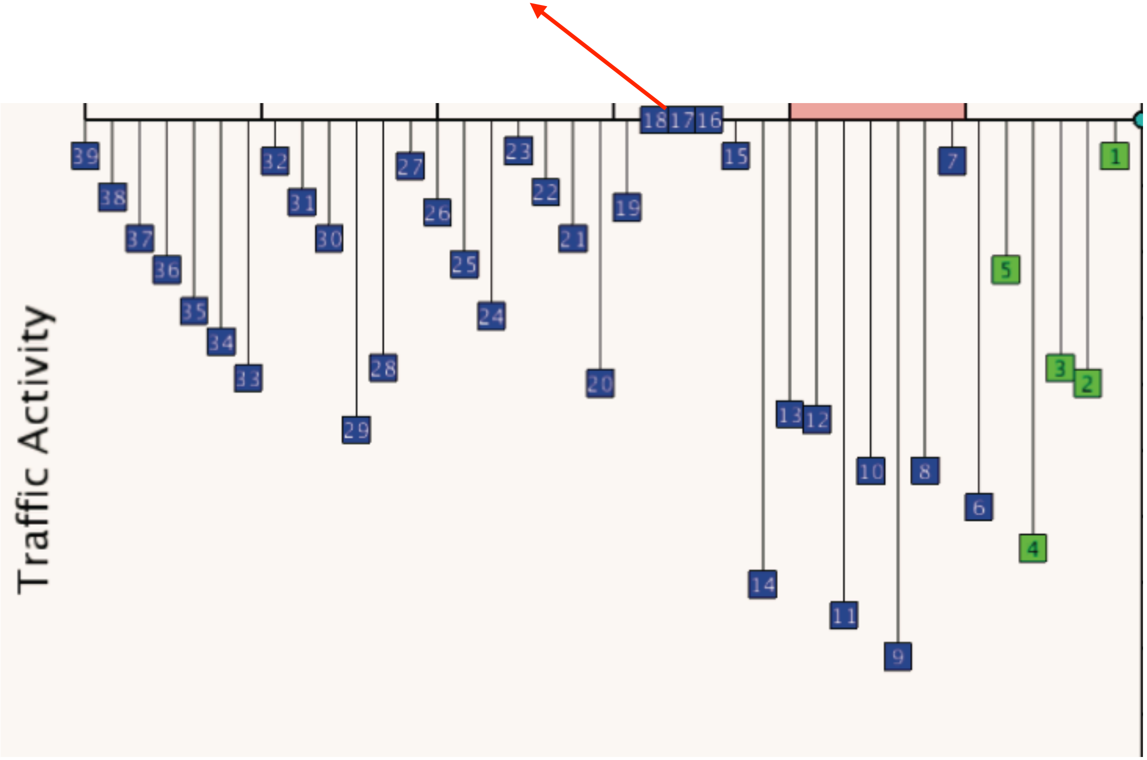
  - Link-Length: Scaled Line





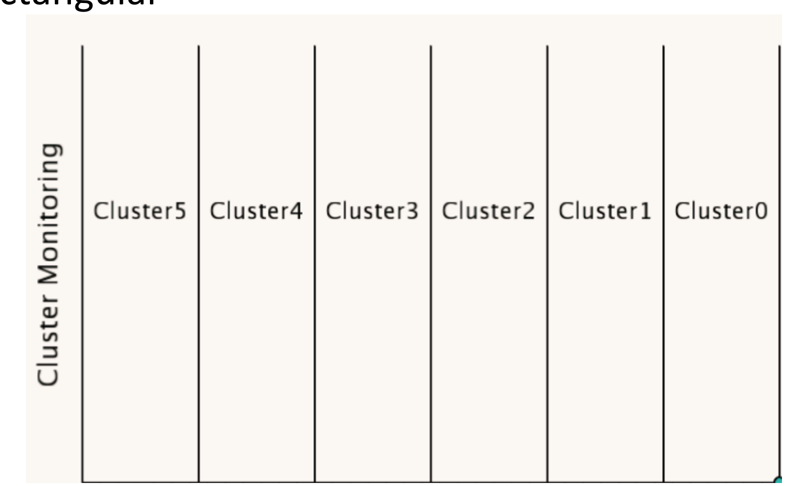
The Lower-Left Quarter(2/2)

Nodes 16, 17 and 18 present abnormal behavior by sustaining harmful jamming



The Upper-Left Quarter(1/5)

- The Upper-Left Quarter encodes analytics from the network cluster's perspective.
- A set of adjacent columns, one for each existing cluster, dynamically change color introducing the level of granularity of the threads upon each cluster.
  - An administrator is able to determine the granularity and localization factors, such as where the thread is moving and what is the level of the thread.
- Pre-attentive objects:
  - Form-Shape/Color: Labeled, Adaptively Colored Rectangular

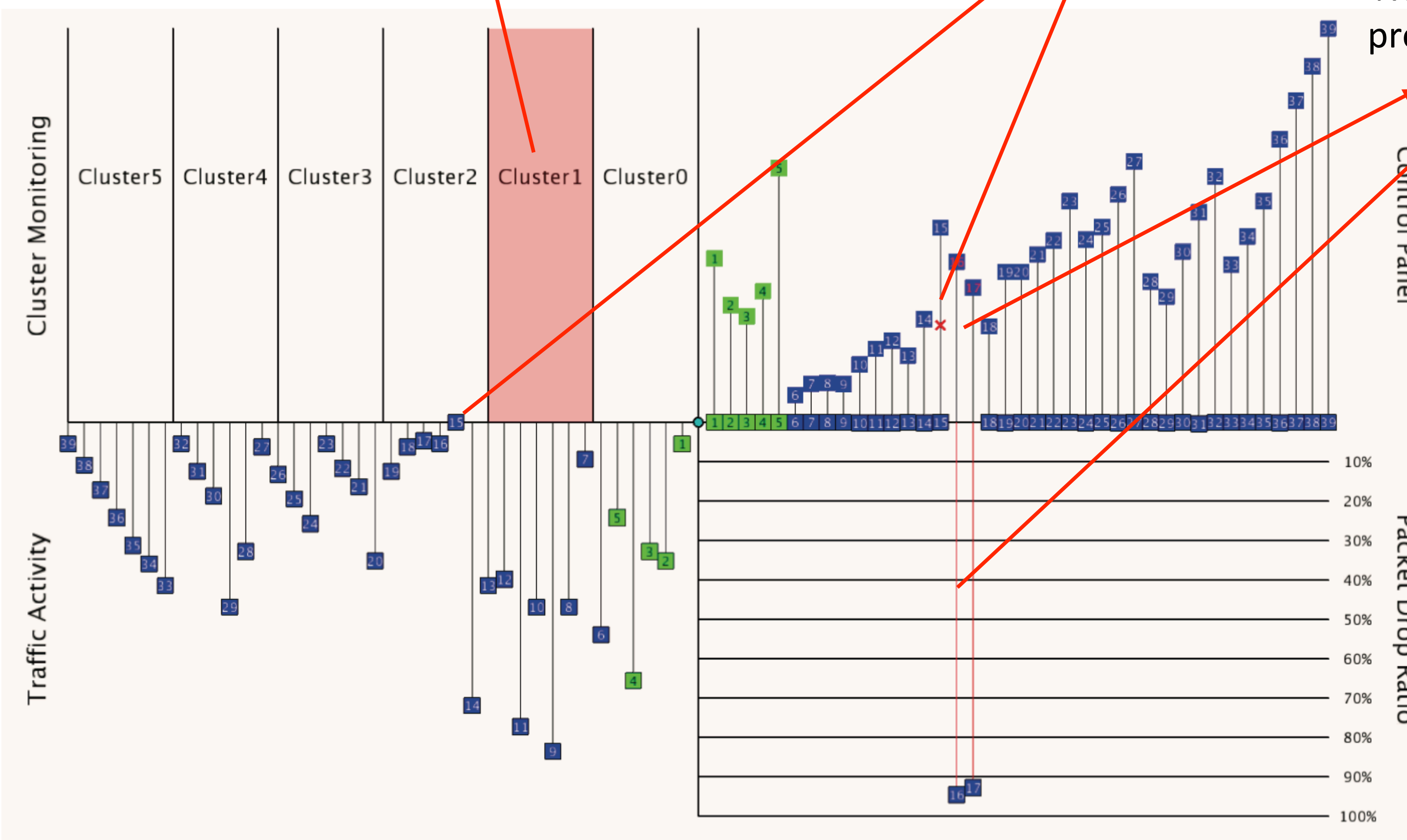


The Upper-Left Quarter(2/5)

The Cluster Monitoring view indicates abnormal activity within Cluster 1 and its nodes (15, 17, and 18)

Node 15 is under jamming attack

Nodes 17 and 18 present a notable drop ratio



The Upper-Left Quarter (3/5)

- How it works?
- Introduction of the Highlight Function (HF^{i})

$$HF^{i} = w_{SF} \times SFIM^{i} + w_{J} \times JIM^{i}$$

  - i denotes the cluster ID.
  - $SFIM^{i}$ represents the impact of the selective forwarding thread in the cluster i.
  - JIM^{i} represents the impact of the jamming thread in the cluster i.
  - The weighting factors w_{SF} and w_{J} provide the relative significance of the two threads to the determination of the HF^{i} function.

- The HF^{i} function employs the color opacity feature in order to highlight the cluster rectangular. It takes values in the range [0,255], thus the HF^{i} function should satisfy the following constraint:

$$0 \leq HF^{i} \leq 255 \Rightarrow 0 \leq w_{SF} \times SFIM^{i} + w_{J} \times JIM^{i} \leq 255$$

+

The Upper-Left Quarter (4/5)

- Given that the measurement of a node that is under selective forwarding attack is between 0% (no thread) and 100% (complete attack), the $SFIM^{i}$ function is defined as:

$$SFIM^{i} = D^{i} \times 125$$

- The parameter D^{i} denotes the drop ratio of the i-th cluster. Hence, it holds:

$$0 \leq D^{i} \leq 1$$

- The JIM^{i} function corresponds to the results obtained by a jamming attack to a single or to multiple sensor nodes. Thus, the result is a true/false value.
  - This phenomenon is formed based on the number of nodes identified as (potential) jamming victims divided by the number of nodes the cluster includes.
  - The parameter J^{i} expresses the portion of the jamming's victim nodes in a single cluster:

$$JIM^{i} = J^{i} \times 125$$

The Upper-Left Quarter(5/5)

- The weights offer the ability to dynamically re-adjust the viewpoint regarding the two attacks.
  - For instance, an administrator may consider the jamming attack more important than the selective forwarding attack due to the environmental dynamics.
- The summation of the two weight factors yields one:

$$w_{SF} + w_{J} = 1$$

- Initially, both parameters are treated equally:

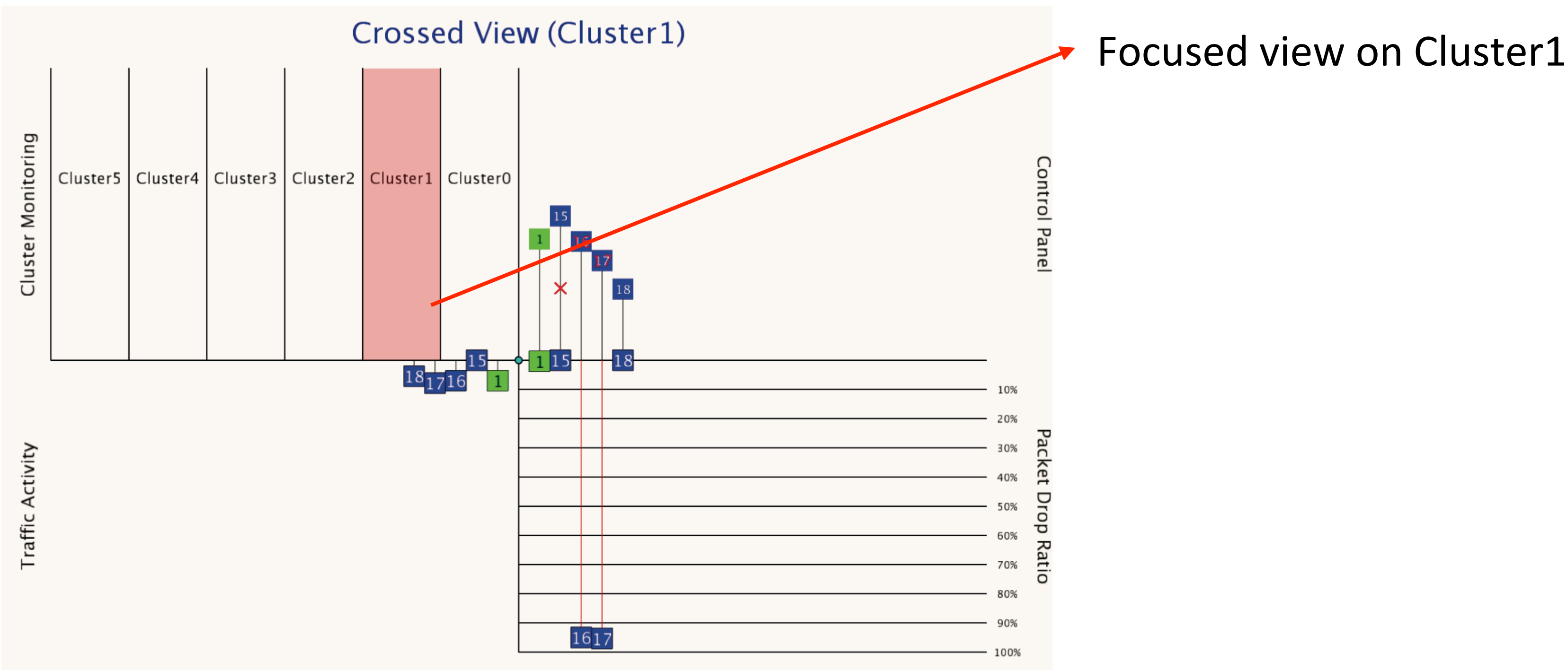
$$w_{SF} = 0.5,\ w_{J} = 0.5$$

- A dynamic formula for weight value determination is proposed:

$$w_{SF} = SFI/SFI+JI\ , w_{J} = JI/SFI+JI\ , \forall\ SFI+JI \neq 0$$

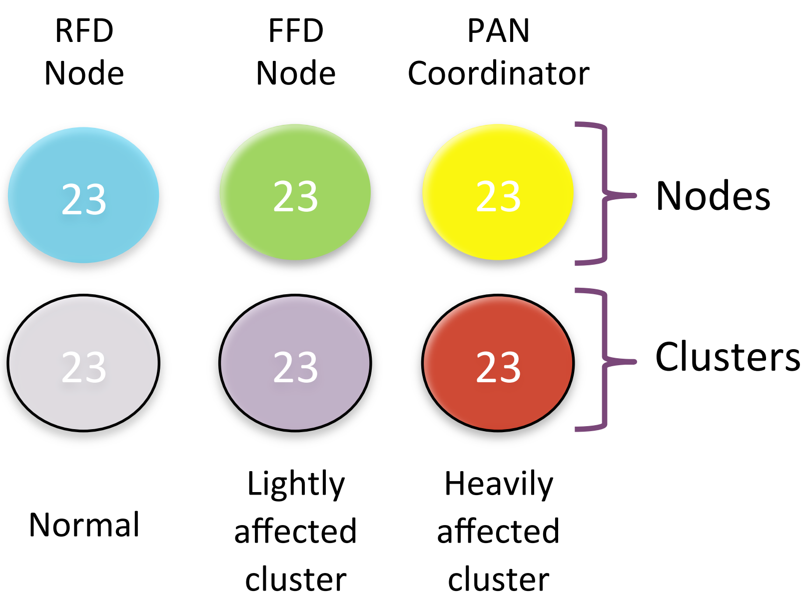
The Crossed Cluster View

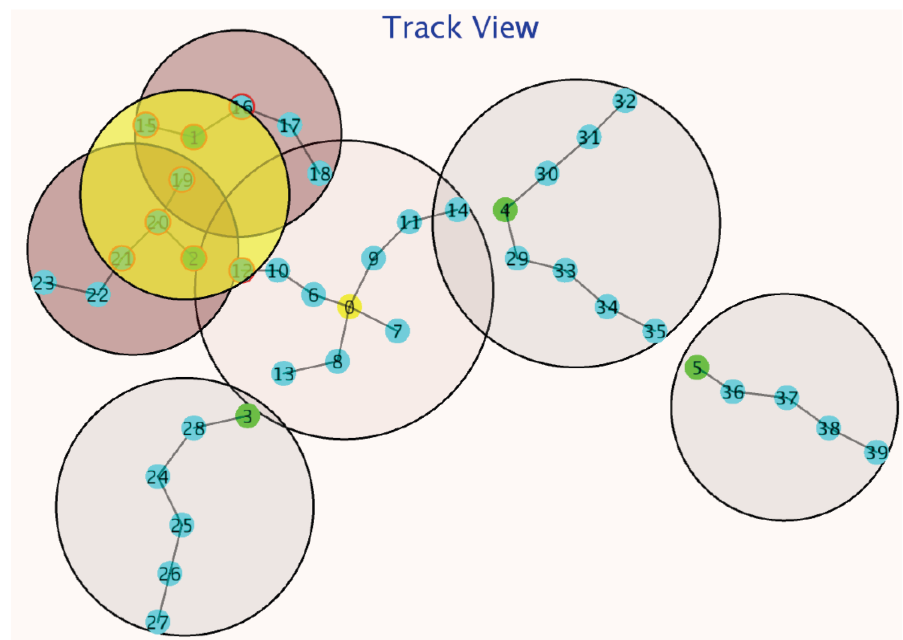
- The Crossed View graphical interface may induce scalability issues.
- Solution: The Crossed Cluster View in a single click…



+ The Track View[1/3]

- The Track View reveals the localization feature of a potential thread.
- Main focus: the tracking of a potential thread by estimating its source coordinates.
- Pre-attentive objects:
  - Form-Shape/Color: Labeled, Colored Circle

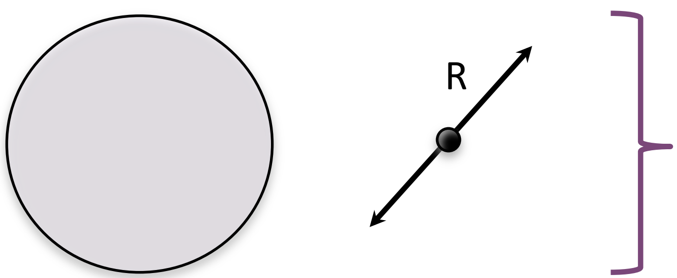




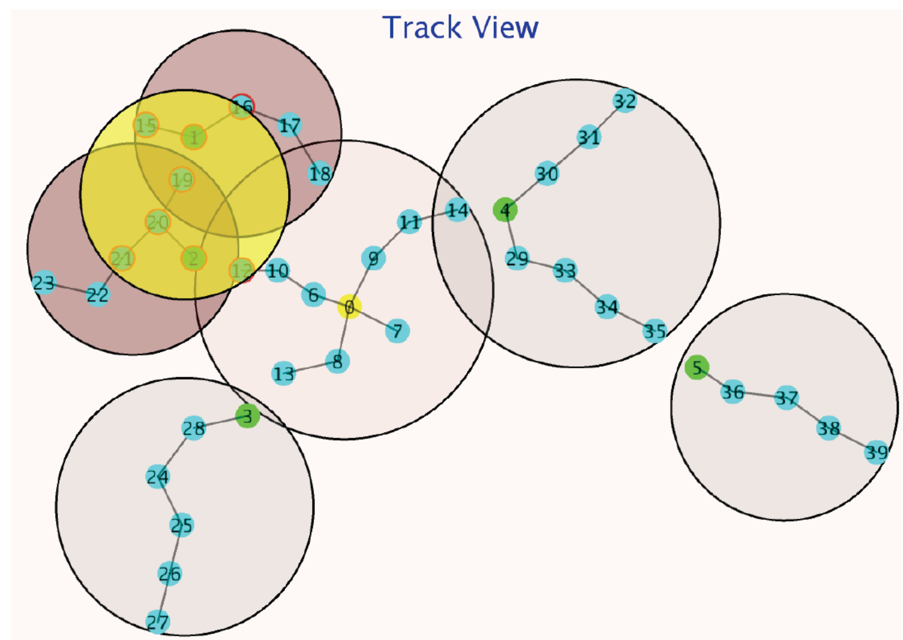
The Track View$^{2/3}$

- Pre-attentive objects:

- Form-Enclosure regarding Clusters: Black Ring with Radius R



Cluster Area



- Form-Enclosure regarding Nodes:

Node under Selective Forwarding attack

Normal

Node under Jamming attack

The Track View$^{3/3}$

- Operation?
- The Track Algorithm: the algorithm calculates the central point of the Track Surface formed by the coordinates of the nodes under attack.

Algorithm 1 Track Algorithm

Input: The coordinates of z nodes under jamming attack $(N = N1_X, N1_Y, N2_X, N2_Y, ...Nz_X, Nz_Y)$.

Output: The estimating coordinates of the jamming source (J_X, J_Y) and the its radius $(RADIUS)$.

{ Find the Activity Center }

$tempSumX = 0$

$tempSumY = 0$

for each node i under jamming attack **do**

  $tempSumX = tempSumX + Ni_X$

  $tempSumY = tempSumY + Ni_Y$

end for

$J_X = tempSumX/z$

$J_Y = tempSumY/z$

$MaxDistanceFromSource = 0$

for each node i under jamming attack **do**

  if $Euclidean\_Distance(J_X, J_Y, Ni_X, Ni_Y) > MaxDistanceFromSource$ **then**

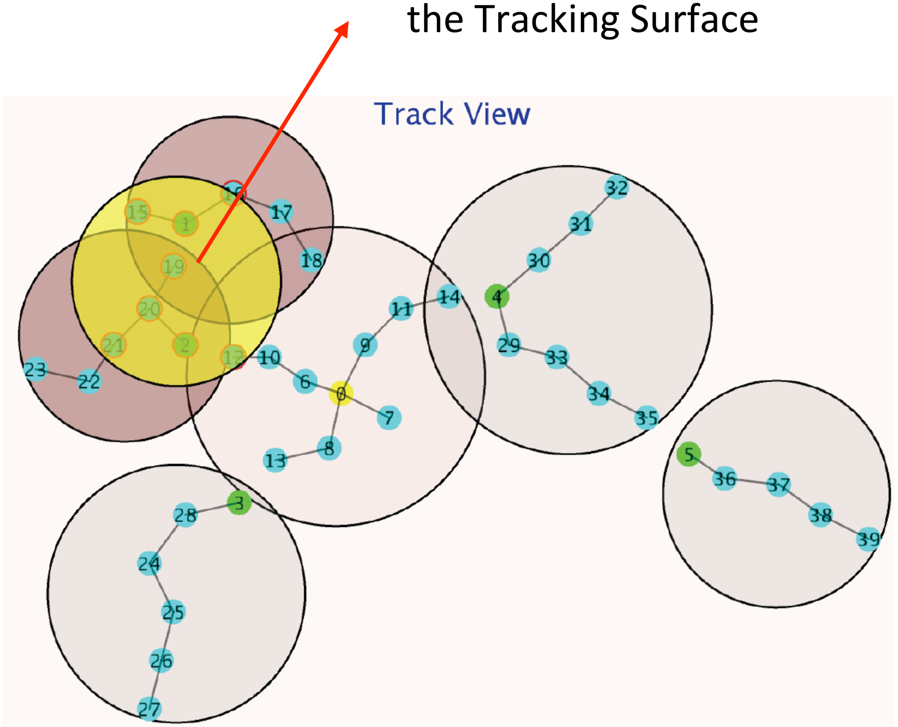
    $MaxDistanceFromSource = Euclidean\_Distance(J_X, J_Y, Ni_X, Ni_Y)$

  end if

end for

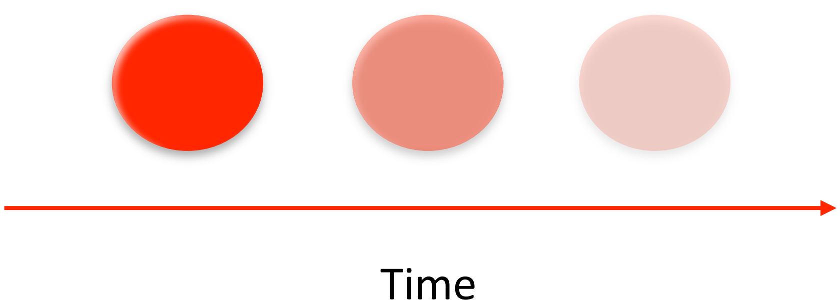
$RADIUS = MaxDistanceFromSource$

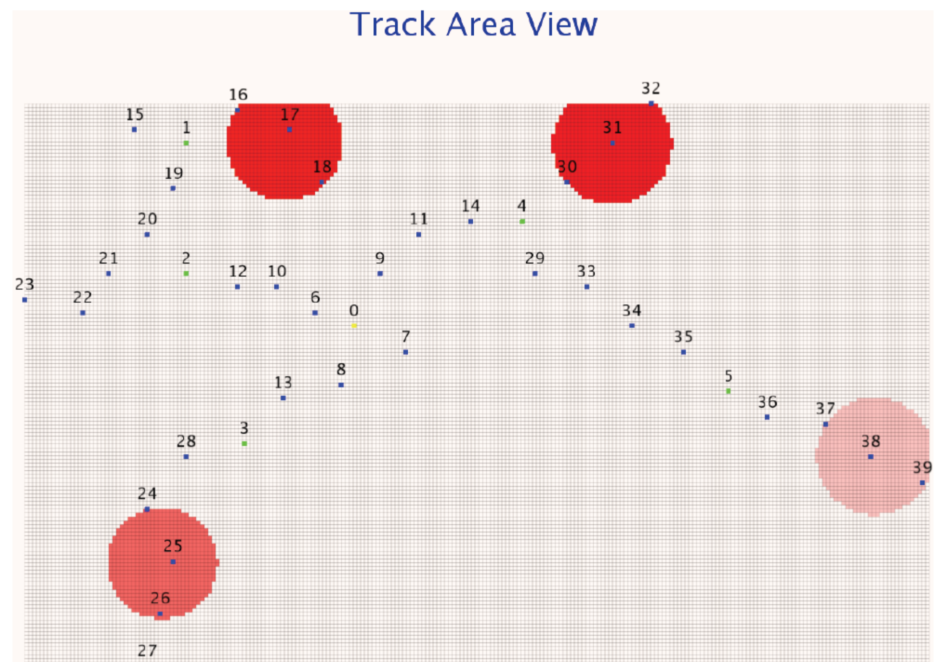
A light yellow circle indicates the Tracking Surface



The Track Area View[1/2]

- The Track Area View addresses localization issues but misses the time parameter.
- Pros: It enhances the obtained image with the time dimension.
- Pre-attentive objects:
  - Form-Shape/Color: Colored Circle.





The Track Area View$^{2/2}$

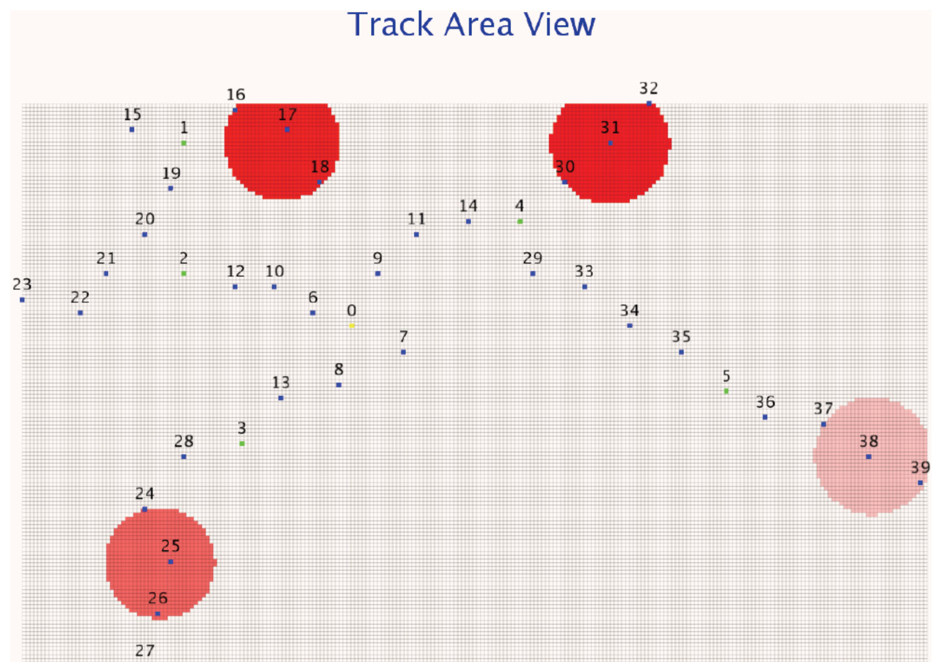
- How it works?
- The Track Area Algorithm: It determines the ‘red’ area and paints it accordingly.

Algorithm 2 The Track Area Algorithm

Input: .
The number of available tiles (TI)
The coordinates of a tile of the given network area (T_x,T_y)
The coordinates of the estimated jamming source (S_x,S_y)
The estimated range of the jamming source S_{range}
The refresh period $T_{refresh}$
A flag denoting whether there is an active jamming attack (jamming_thread)
Output: The new color value $T_{opacity}$.

Algorithm 3 The Phases of the TAA Algorithm

```
{ Refresh Phase }
for each period T_refresh do
  for each tile TI do
    if T_opacity > 0 then
      T_opacity = T_opacity − 1
    end if
  end for
end for
{ Update Phase }
if jamming_thread == TRUE then
  if Euclidean_Distance(T_X, T_y, S_x, S_y) ≤ S_range then
    T_opacity = 255
  end if
end if
```



System Input

- A local or remote data stream feeds the SRNET system. This stream shall include:
  - The number of sensor nodes.
  - The number of coordinator nodes.
  - The position of each node (in 2D coordinates).
  - (optional) The parent-child relationship of each node with its peers.
  - (optional) The ID of each node.
  - Traffic parameters such as source and destination id, arrival time, packet size and type, etc.
- The system updates the monitor periodically keeping a stable fps equal to 20.
- (optionally) It is able to support a report containing various graphs, and figures.

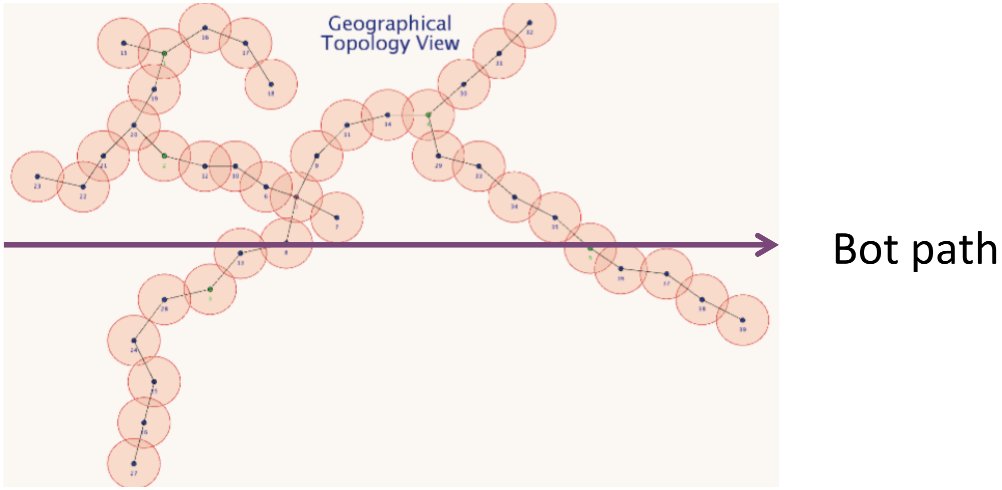
Performance Evaluation

- **Simulation Parameters:**
  - Simulated Topology : An 802.15.4 cluster-tree topology
  - Simulation Area : 1000m x 800m
  - Number of Nodes : 40 (1 sink node, 5 coordinators and 34 devices)
  - Communication Radius (POS) : 50 m
  - Traffic Load: 10 packets/second per leaf node
- **Simulation Metrics:**
  - TAA's Tracing Accuracy: the Euclidean distance between the estimated and the actual coordinates of the attack source.

+

Analysis of the Tracing Accuracy[1/2]

- **Scenario**: A bot machine launching a jamming attack moves through the sensor field.
  - The bot follows a fixed path starting from the middle of the network left side and finishing in the middle of the network right side.
  - The bot changes position with a speed of 50 distance points (i.e., meters) per 60 seconds.
- Assessment of the average distance error of the Track Area Algorithm.
  - The difference between the estimated central point of the attack compared to the actual coordinates of the bot.



Analysis of the Tracing Accuracy$^{2/2}$

- **Key Observations:**
  - The average distance error of the Track Area Algorithm depends on the range of the attack.
    - Larger jamming radius leads to more precise estimations. Why? More nodes is sensed under jamming attack, hence the Track Area Algorithm becomes more accurate.
  - The error level is reduced as the range of the attack becomes larger.

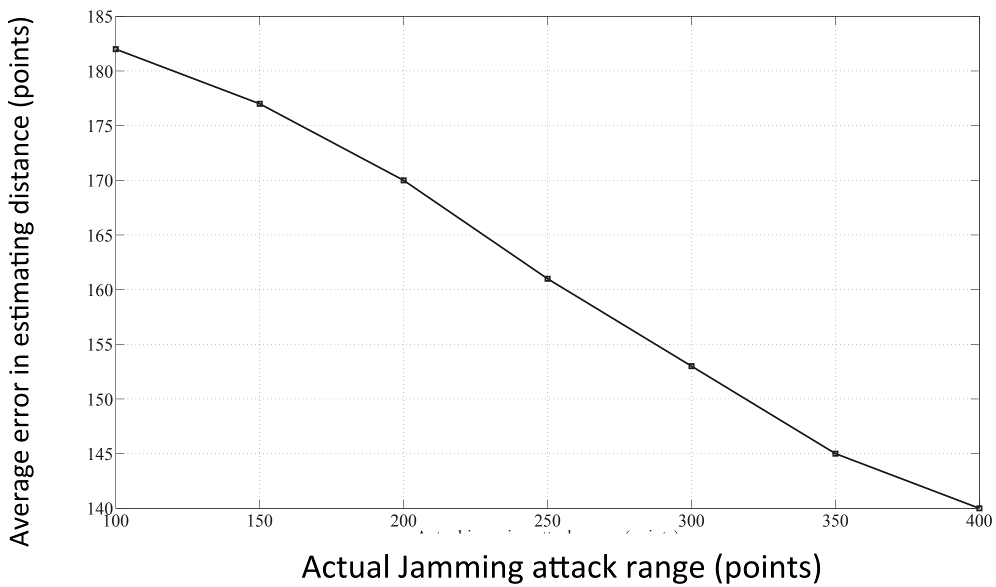
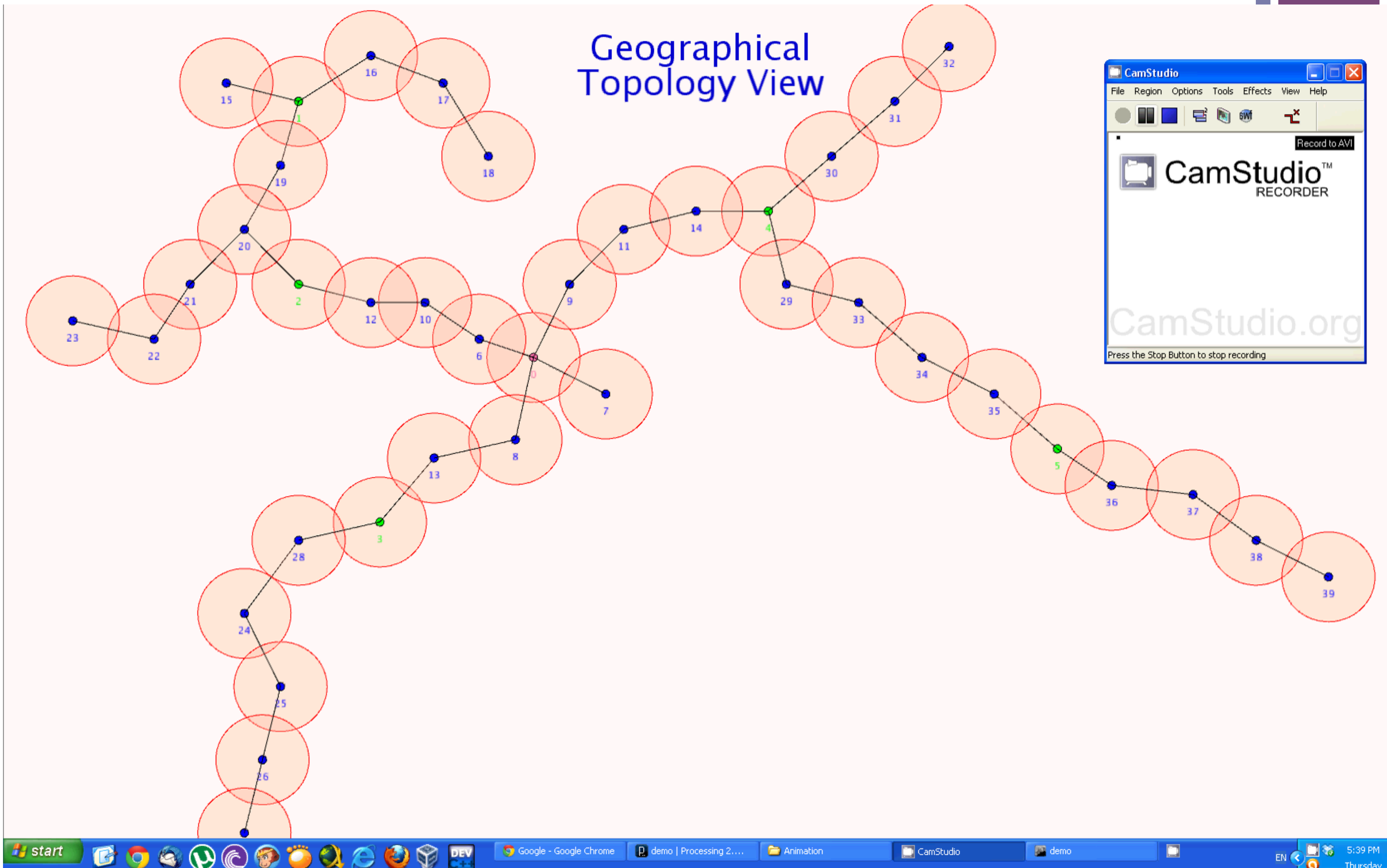


Figure – Average distance error of the Track Area Algorithm in terms of distance units

Demo



Geographical
Topology View
CamStudio
File Region Options Tools Effects View Help
Record to AVI
CamStudio™
RECORDER
CamStudio.org
Press the Stop Button to stop recording
start
Google - Google Chrome
demo | Processing 2....
Animation
CamStudio
demo
EN
5:39 PM
Thursday

Conclusions

- In our research, we explored the area of security visualization for WSNs.
- SRNET offers the following contributions:
  - A multi-dimensional crossed view enhanced with a highlight function that monitors the evolving status of selective forwarding attacks and jamming attacks in WSNs.
  - A crossed view perspective combined with a track view, which is introduced in order to timely locate the source of the correlated anomaly.
  - A novel track area view that tracks the source and the pattern of a potential jamming attack and which enables attribution of the attacker.
- Future work:
  - To validate SRNET through extended user studies where network analysts will use the system and provide feedback on its usability.
  - To enable the detection of a series of new attack patterns, such as Sybil, Sinkhole, Wormhole attacks, etc.

Major References

- Akyildiz I.F. , Su W. , Sankarasubramaniam Y., Cayirci E. (2002), *Wireless Sensor Networks: A Survey*, Computer Networks (Elsevier) Journal, vol.3, no. 4, pp. 393-422.
- Perrig, A., Stankovic, J., and Wagner, D. (2004). *Security in Wireless Sensor Networks*. Communications ACM, vol. 47, no. 6, pp. 53-57.
- J. R. Goodall. *Introduction to visualization for computer security*. In VizSEC 2007, Mathematics and Visualization, pages 117. Springer Berlin Heidelberg, 2008.
- Greg Conti. *Security Data Visualization: Graphical Techniques for Network Analysis*. No Starch Press, 2007.
- Raffael Marty. Applied Security Visualization. Addison-Wesley Professional, 2008.
- Ivan Herman, Guy Melancon, and M. Scott Marshall. Graph visualization and navigation in information visualization: A survey. IEEE Transactions on Visualization and Computer Graphics, 6:2443, January 2000.
- H. Shiravi, A. Shiravi, and A. Ghorbani, *A Survey of Visualization Systems for Network Security*. IEEE Transactions on Visualization and Computer Graphics, vol. 1, no. 99, pp. 1{19, 2011.
- IEEE 802.15.4 (2011). IEEE Standard for Local and Metropolitan Area Networks - Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs).

Thank you

Questions?

Dr. Eirini Karapistoli

Email: ikarapis@uom.gr