Detecting Jamming Attacks in Ubiquitous Sensor Networks

Networking Lab
Kyung Hee University

Syed Obaid Amin
obaid@networking.khu.ac.kr

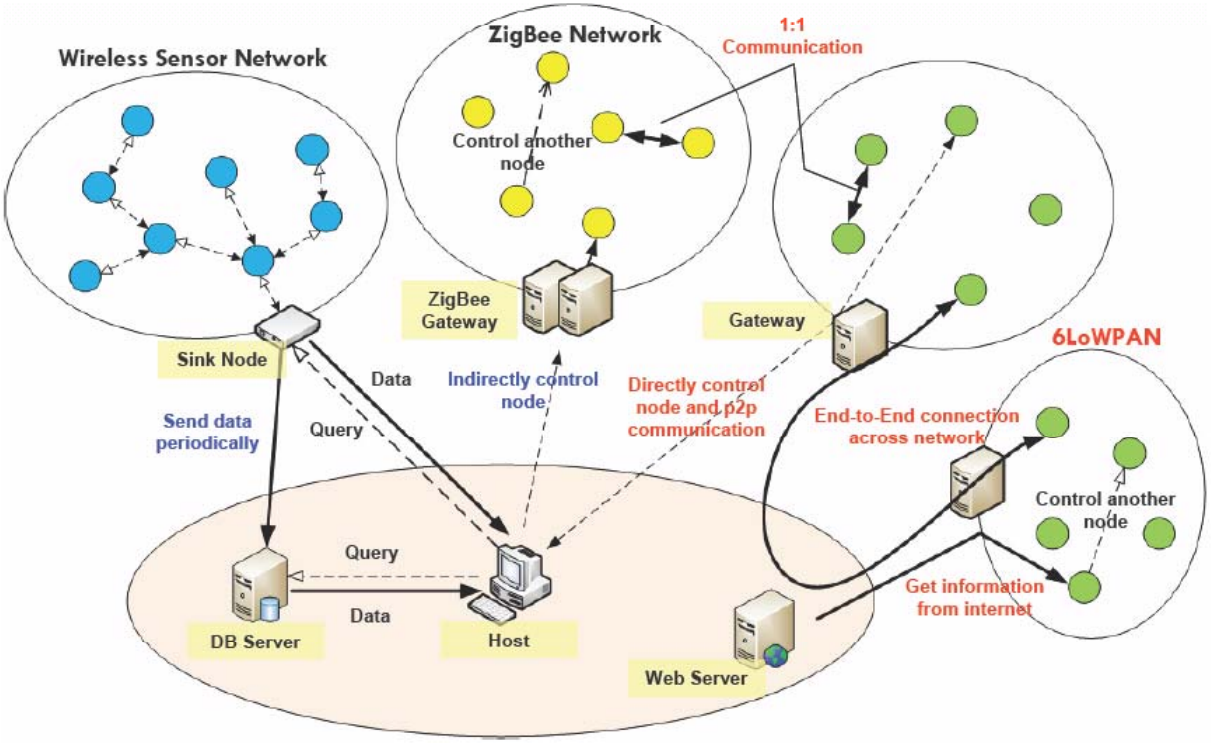
Date: February 11th, 2008

Contents

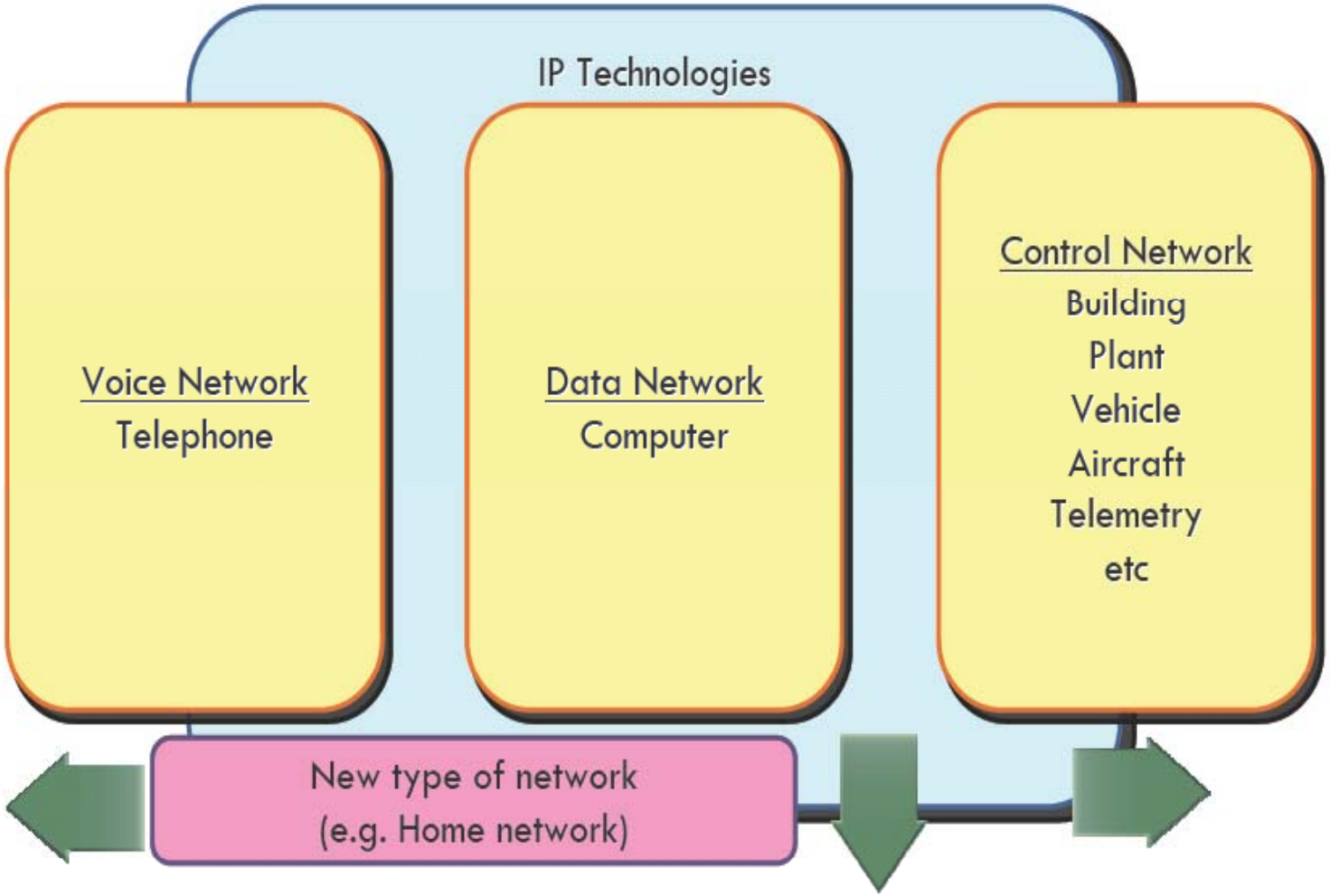
- Background
- Introduction
  - USN (Ubiquitous Sensor Networks)
  - Jamming
- IDRS (Intrusion Detection and Response)
- Conclusion

USN (Ubiquitous Sensor Networks)

- Specialized form of WSN (Wireless Sensor Networks)
- Everywhere, everything with RFID tags
- Sensing ID and environmental information
- Real-time monitoring & control via network
- Use for In-house deployment, mainly to provide ubiquitous environment



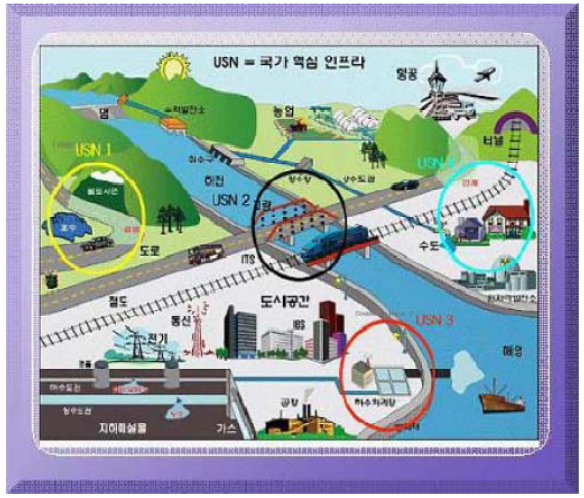
What is IP-USN



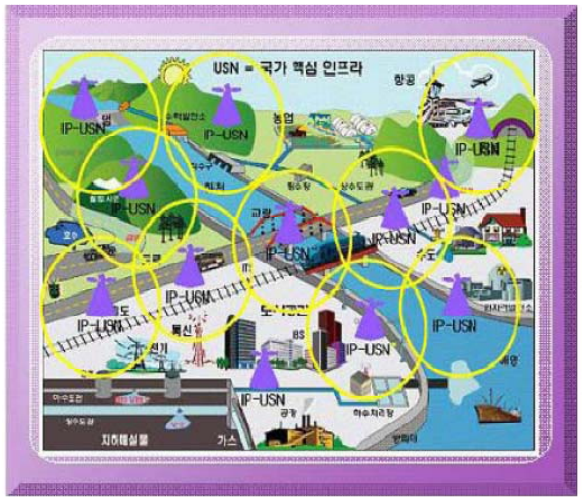
Advantages

- Enables to use existing infrastructure.
- Allow easy access of the nodes.
- Making it more understandable for nonproprietary users, as shown in figure.
- Auto configuration of addresses is also possible.
- In case of IPv6. Large address space

Non IP-USN



IP-USN



Independently Site, Service, Technology

ALL-IP based convergence network

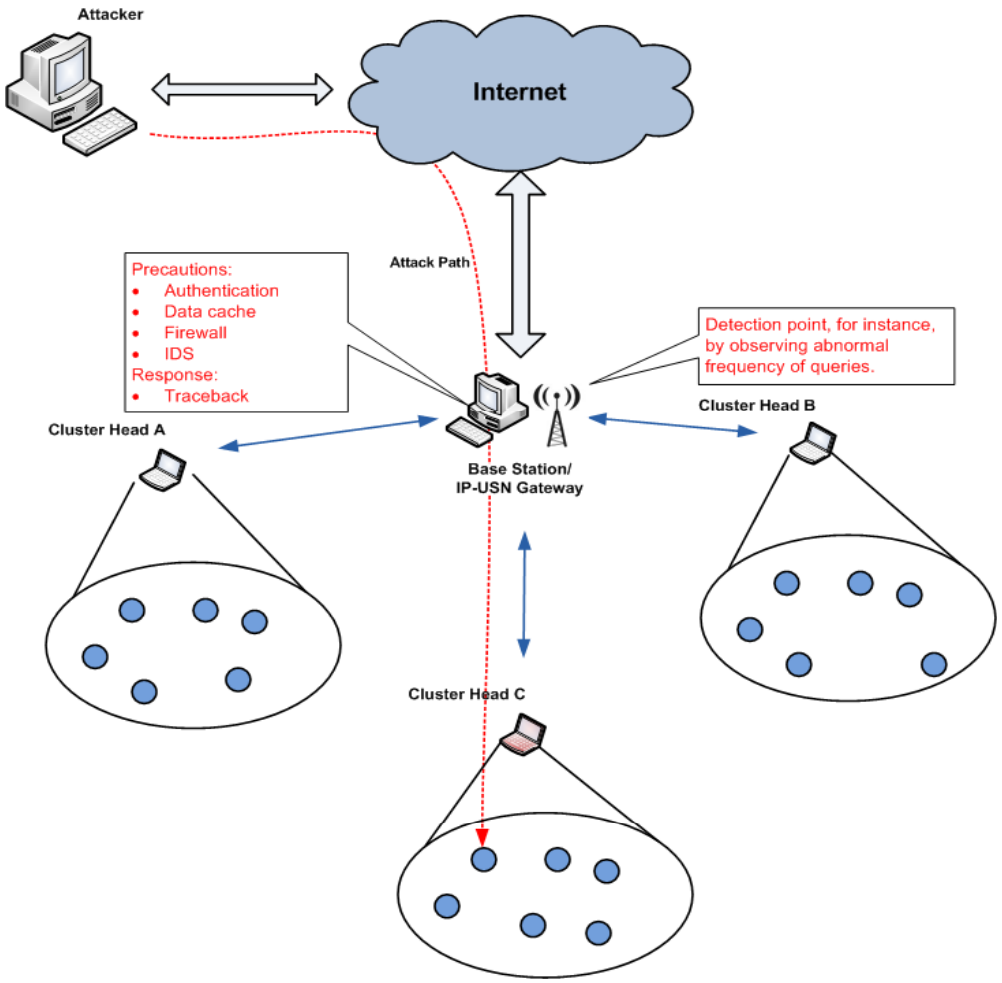
Research Goal

- This work is a part of our ongoing research on IDRS (Intrusion Detection and Response System) for IP-USN.
- We are trying to find out possible attack models in IP-USN environment.
- This presentation, specifically deals with an IDRS for one of the model discussed later.

Attack models on IP-USN

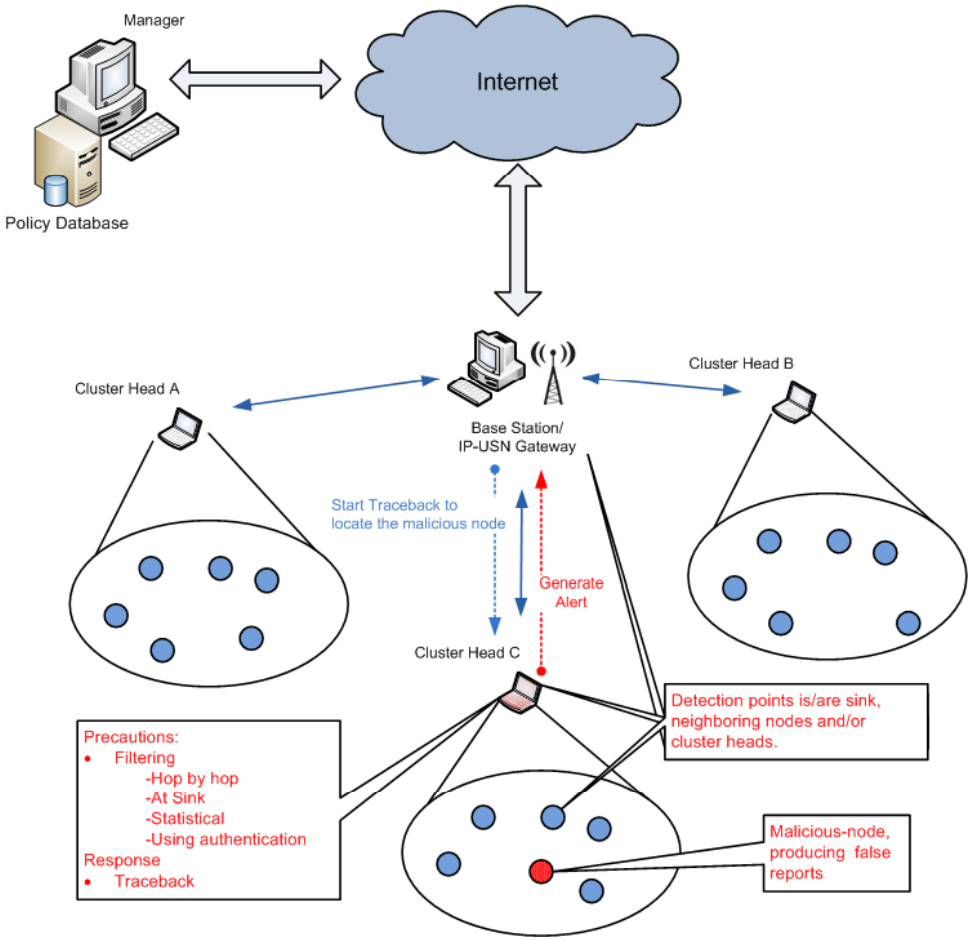
Scenario (1)

- Attacker trying to attack the sensor network via Internet.
  - Most likely, the detection point is base station or sink.
  - Precautions:
    - Authentication techniques, using IPSec between querier and Sink.
    - Data-caches: Sink answers the query with the most recent data in the cache. Sink can update the cache periodically.
    - Firewalls
    - IDSs
  - Response:
    - Traceback



Scenario (2)

- Compromised sensor nodes feeding the false data to the sink or to the legitimate user on the Internet.
- Detection point could be sink, intermediate nodes or the cluster head, depending upon the computational power of related nodes.
- Precautions:
  - Filtering
    - Hop by hop
    - At Sink (Same appraoches for cluter heads)
    - Statistical
    - Using authentication
- Response
  - Traceback
    - Identification of malicious node.

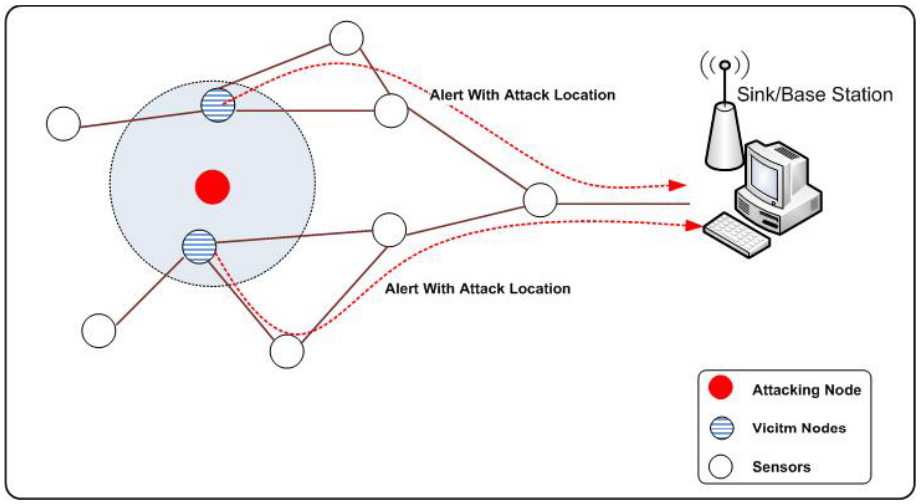


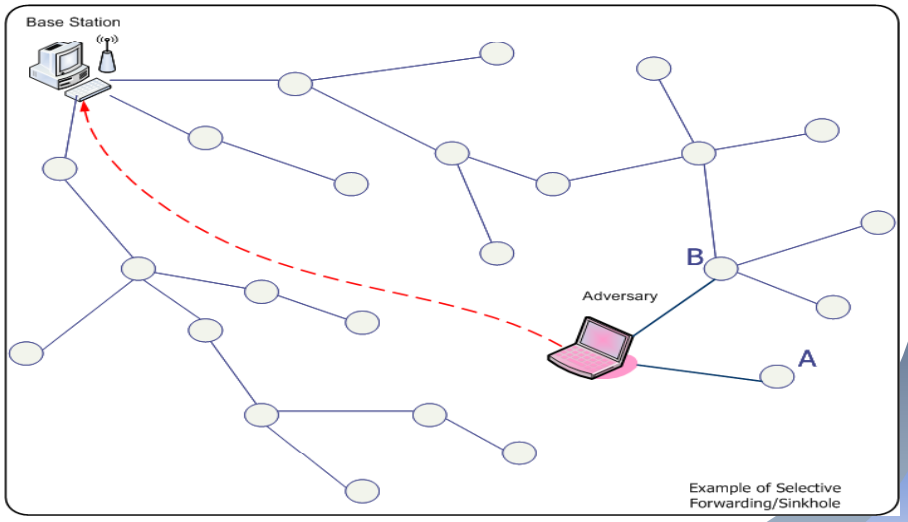
Scenario (3)

- Conventional sensor network attacks.
  - Lots of paper have already addressed the taxonomy of attacks on sensor networks.
  - Few of the attack types are listed as follows:
    - Selective forwarding, Sinkhole attacks, Wormholes.
    - Sybil attacks.
    - Acknowledgement spoofing.
    - Bogus routing information.
    - Jamming attacks.

Detecting Jamming Attacks

- Jamming Attacks:
  - Aim to flood the network with useless traffic.
    - Consumes network resources and prevents legitimate traffic from reaching the base station.
    - More importantly, it causes sleep deprivation of sensor nodes and wastes their energy.
- Selective Forwarding:
  - Occurs when a compromised node drops a packet that is bound for a particular destination.
  - An attacker can selectively filter traffic from a particular part of the network.





Types of Jamming

- **Constant jamming:**
  - Continually emits a radio signal,
  - Continuously sends out random bits to the channel without following any MAC-layer protocol.
- **Deceptive jamming:**
  - Constantly injects regular packets to the channel without any delay.
  - As a result, a normal communicator is deceived into believing there is a legitimate packet and be duped to remain in the receive state.

Effects of different ways of Jamming

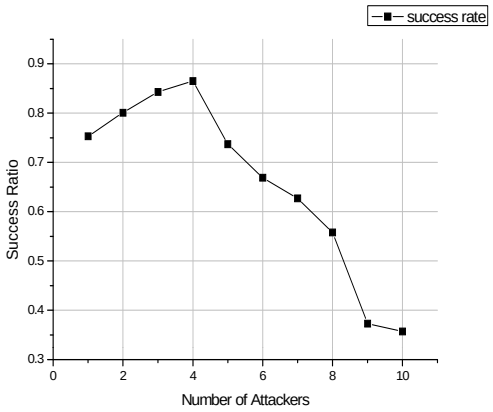


Figure 1(a). Success ratio vs. Number of attackers

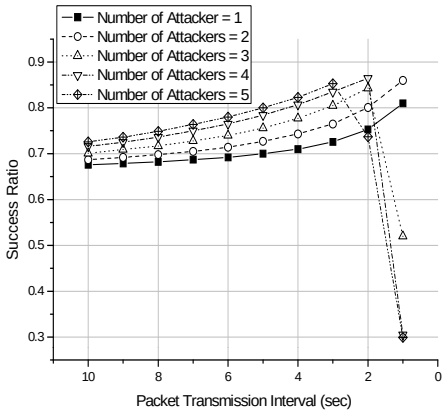


Figure 2(a). Success ratio vs. Transmission interval

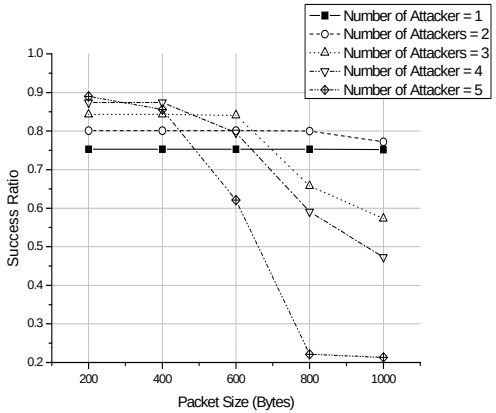


Figure 3(a). Success ratio vs. Packet size

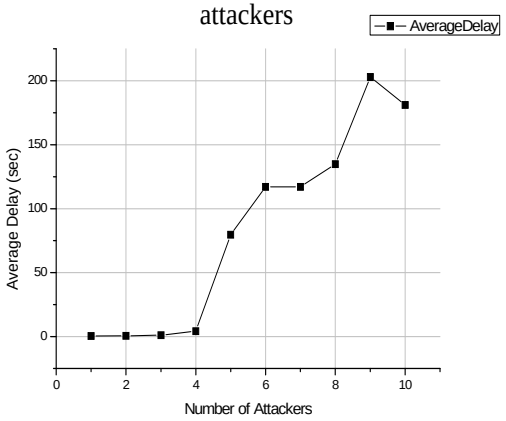


Figure 1(b). Average delay vs. Number of attackers

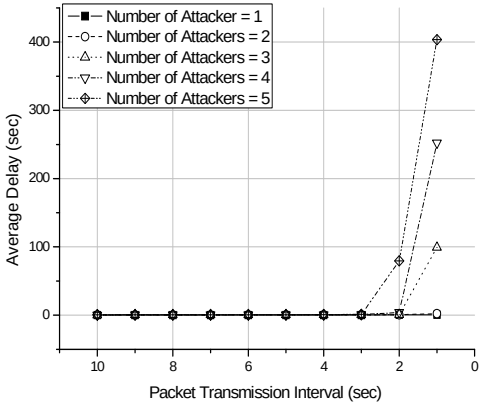


Figure 2(b). Average delay vs. Transmission interval

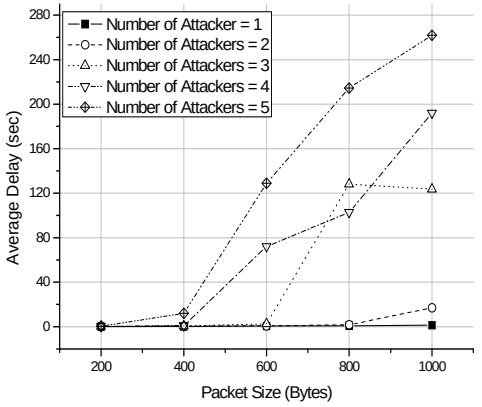


Figure 3(b). Average delay vs. Packet size

Collaborative Jamming Detection Scheme (1/2)

- To deter the jamming attack we propose a collaborative approach of intrusion detection.
- We define two separate components for detecting deceptive and constant jamming.
- In our proposal each node samples the MAC activity information for a given,
  - Deployment-specific period T; or
  - N number of packets and apply statistical models to infer the abnormality, in our simulation we use length of the buffer.
- By observing deviation of certain threshold, a sensor node generates an alarm to the base-station.
- The alarm contains the identification of an alarm generator which can be a location of a sensor node or its ID.
- Multiple paths are used to generate the request even in MAC jamming attacks.

Detecting Deceptive Jamming

- Each node samples the MAC activity information for a given,
  - Deployment-specific period T; or
  - N number of packets and apply statistical models to infer the abnormality, in our simulation we use length of the buffer.
- As sensor nodes are resource constrained devices, simple and efficient detecting algorithm is required.
- We use EWMA (Exponential Weighted Moving Average) instead of calculating mean for every packet arrival.
- Our scheme is not resource hungry as instead of calculating average of whole block we only take new values in account.

$$\bar{X}_k = \alpha \bar{X}_{k-1} + (1-\alpha) X_k$$

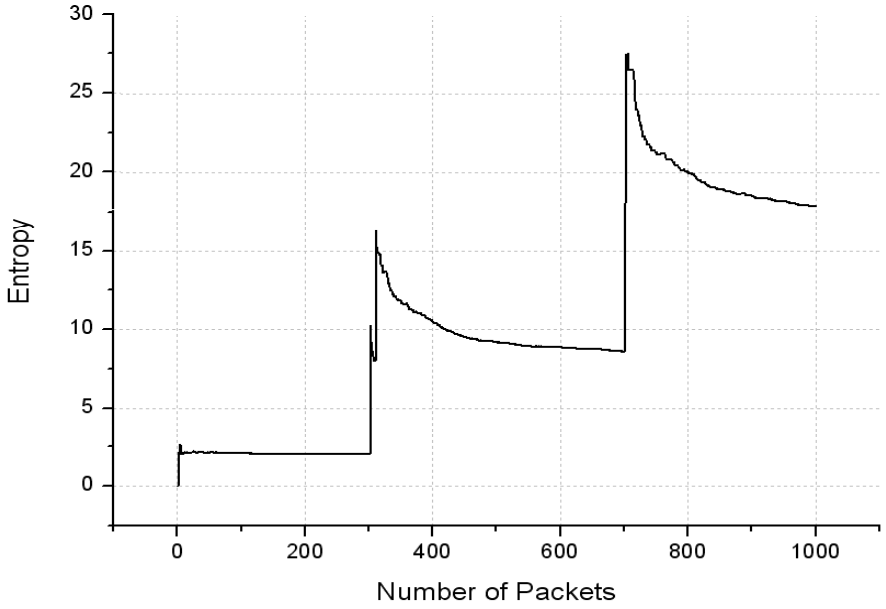
where

α=weight, higher values of α shows that we are giving lower weight to new entries.

X and $\bar{X}_{k-1}$ are the new value and mean up to k -1 elements respectively

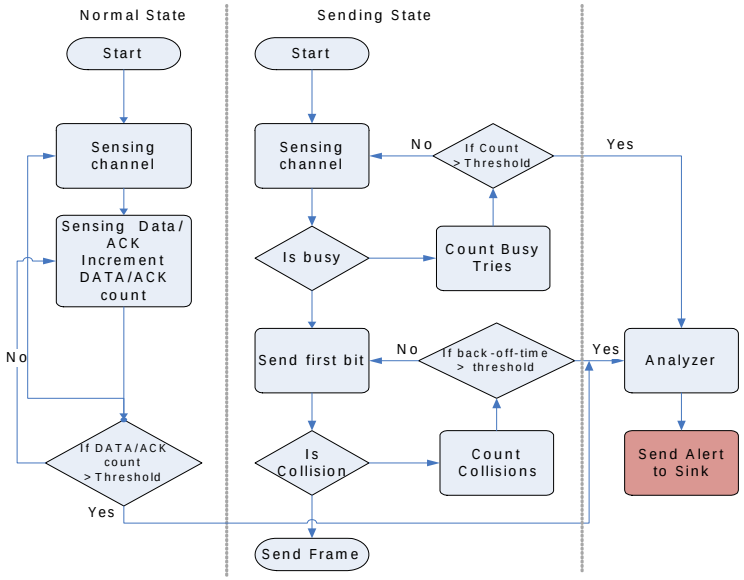
Detecting Deceptive Jamming

- Second component of deceptive jamming detector supports PAT calculator with entropy calculation.
- Entropy calculation is supportive
  - In reducing the false alarm rate.
  - In detecting uncertain behavior of a network.
- Simulation results show that
  - In normal conditions entropy values for *source address field* fall in a narrow range.
  - When the network is under attack these entropy values exceed these ranges in a noticeable manner.



Constant Jamming Detection

- We used following parameters in account for constant jamming detection
- *Increased frames:*
  - Of data and ACK packets
  - In addition, to access channel, the number of RTS and CTS frames are also increased.
- *Increased channel busy time:*
  - frequent busy time and
  - consequent transition from back-off state to defer stage which is an indication of heavy traffic.
- *Increased number of collisions:*
  - Increased retry count due to lack of ACK or CTS.
  - Large contention window (CW) which depends upon retry count and
  - Long lifetime of fragments.
- Threshold values in this case are entirely dependent upon the MAC protocol in use. In our simulation we use modified 802.11 protocol, with reduced data transmission rate.



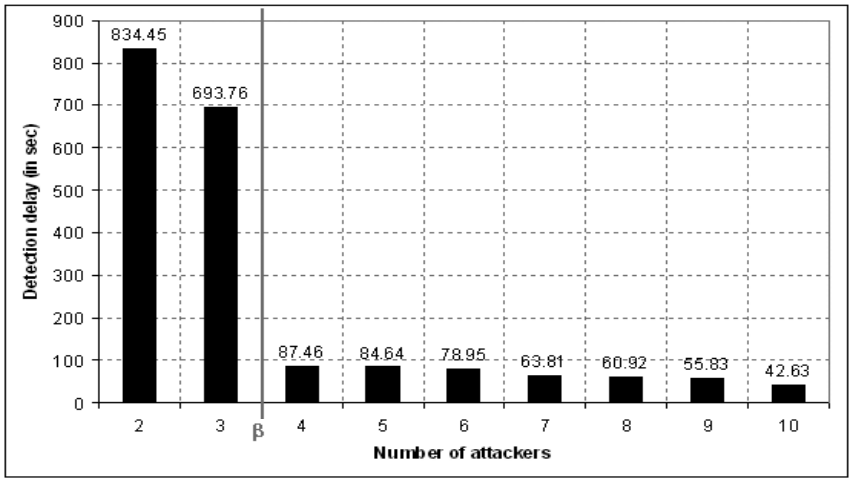
Evaluation results

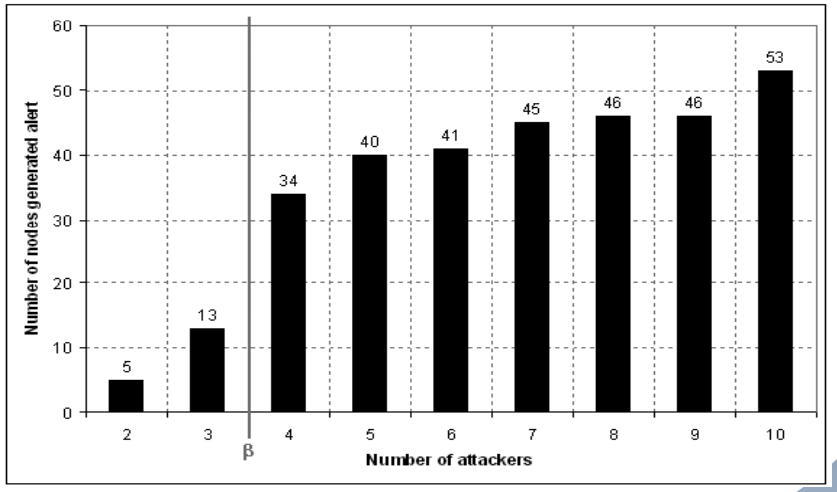
- We use SENSE (Sensor Network Simulator and Emulator) as a simulation tool.
- Sixty sensor nodes were placed randomly in a 500 m^2 terrain with a maximum transmission rate of 250Kbps.
- Modified 802.11 MAC protocol is used for reduced data rate.
- AODV, DSR and flooding are used as routing algorithms; however, here I'll only discuss results achieved by AODV.

Evaluation Results

Detection Delay and Messaging Overhead

- β is a threshold for a number of attackers after which attackers start to affect the network severely.





Conclusions

- This presentation discussed few of our initial investigations made for securing IP based USN.
- So far, we have designed a complete framework for all possible three attack models possible in IP-USN.
- Currently, we are in a phase of implementing security frame work on ZigBee devices.

Questions?