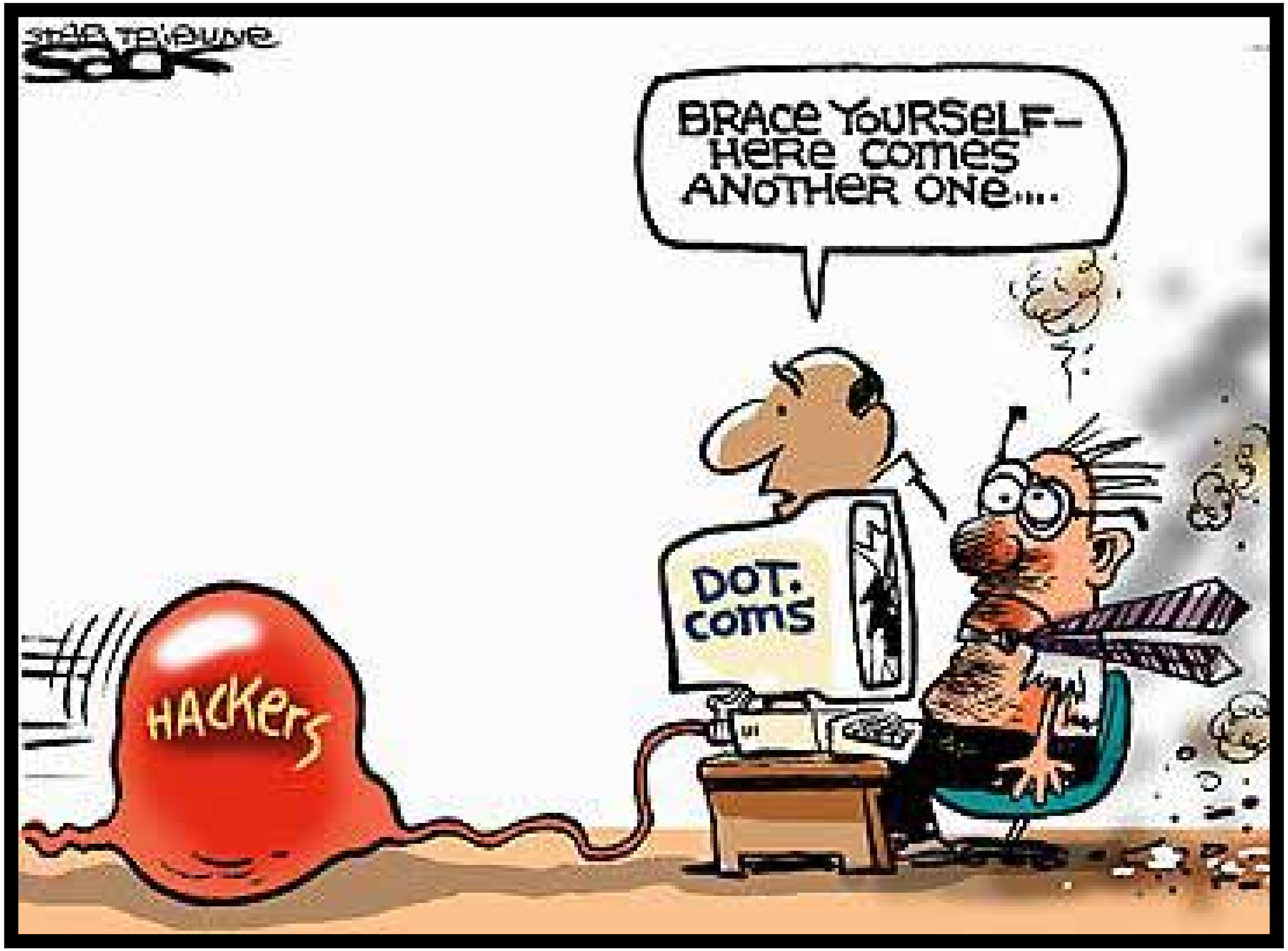
Introduction to USN Security and its Application

cshong@khu.ac.kr, Choong Seon Hong, KHU

Contents

- Objectives
- Traditional IDRS System for IP networks
- Intrusion Response Techniques
- Attack models, Intrusion Detection and Intrusion Response in IP-USN
- IDRS for IP-USN
- Current Research Activities
- Lightweight Intrusion Detection for USN
- Future Work


BRACE YOURSELF—
HERE COMES
ANOTHER ONE....
DOT.
COMS
HACKERS

Objectives

- To avoid conditions shown above. ☺
- To design an IDRS (Intrusion Detection and Response System) for USN (Ubiquitous Sensor Networks)
- Tasks:
  - Identifying the types of intrusion possible in USN.
  - Development of an architecture to detect as much intrusion types as possible.
  - Development of a response mechanism to deal with aftermaths of an intrusion.

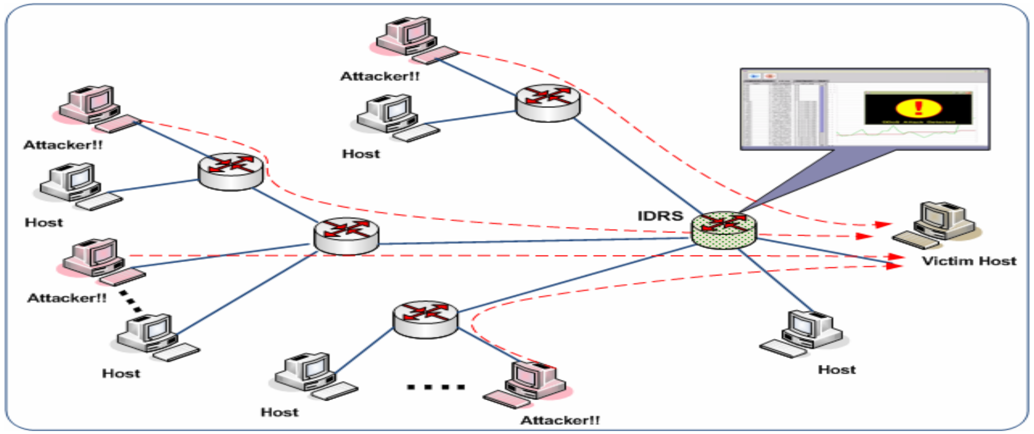
Traditional Ways of Intrusion Detection and Response

IDS and IDRS - Definitions

- An IDS (Intrusion Detection System) is used to detect many types of malicious network traffic and computer usage that can't be detected by a conventional firewall, mainly (D)DoS attacks.
- An IDRS (Intrusion Detection and Response System) is a combined term for a system which is capable of detecting an intrusion and can respond to avoid the intrusion.

Traditional IDRS

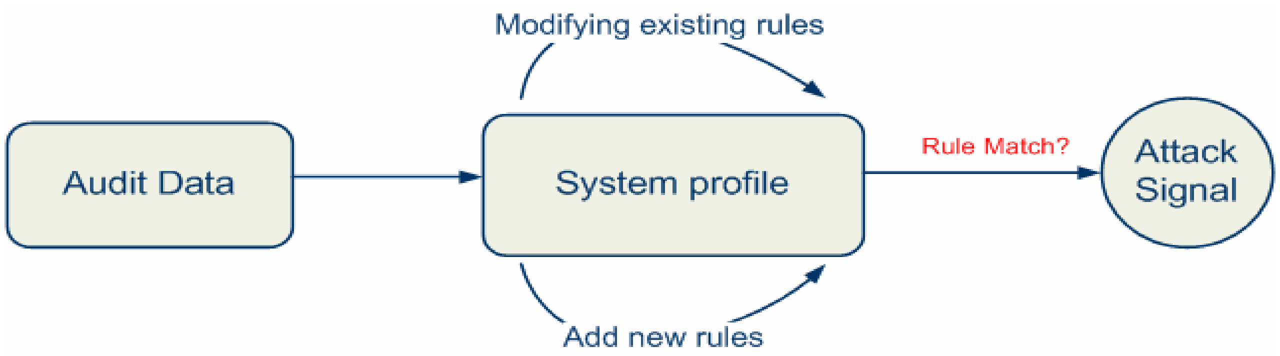
- IDRS (Intrusion Detection and Response System) has already been addressed in literature extensively.
- In [1] and [2] we have proposed Intrusion Detection and Response System and Traceback scheme for IP networks respectively.
- The IDRS scheme proposed for IP networks cannot work for USN (Ubiquitous Sensor Networks) or IP-USN.
- Usually intrusion detection systems requires high end processing, which is not possible in resource constrained ubiquitous sensor networks.
- Above all reason elevates the need of an IDRS which is specifically tailored for IP-USN.



A typical DDoS attack

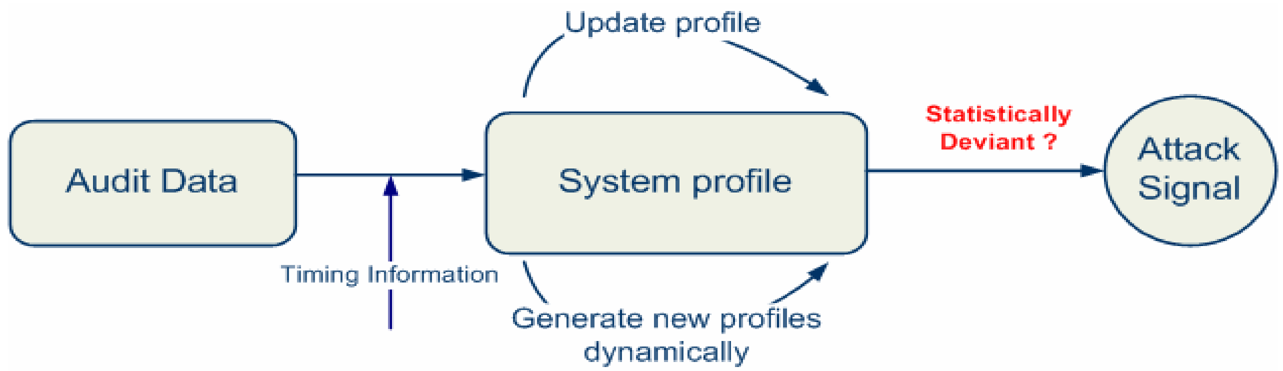
Approaches for Intrusion detection

- Signature based/Misuse detection
  - Decisions are made based upon prior knowledge of intrusion pattern or signature.
  - Difficult to have signatures of all intrusion.



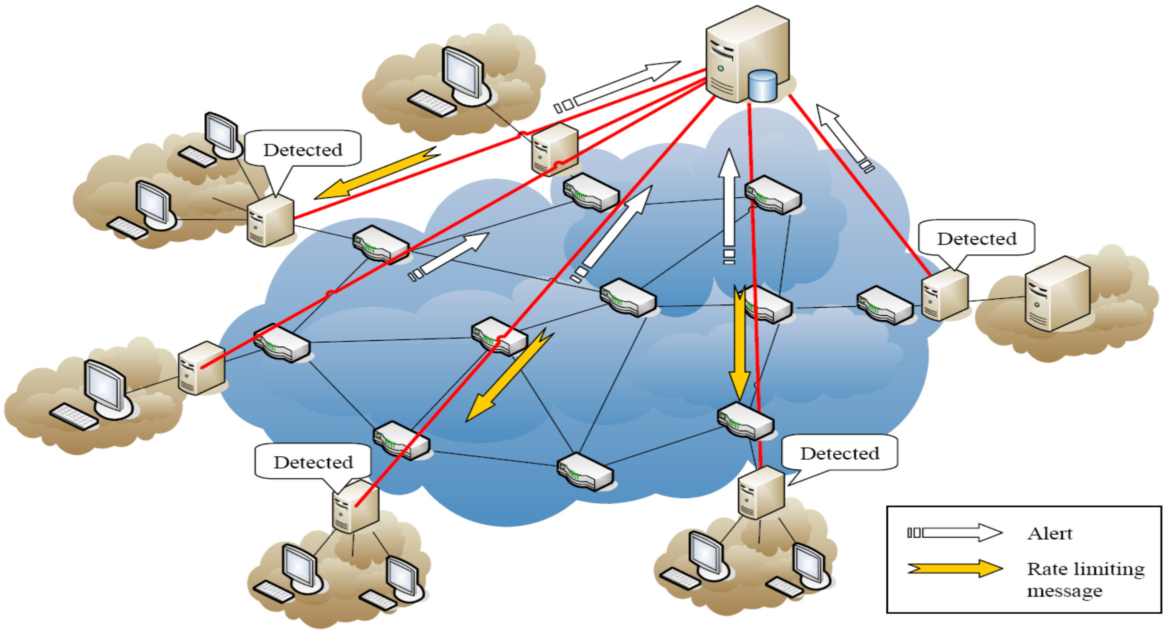
Approaches for Intrusion detection

- Anomaly detection
  - A system baseline is provided.
  - Any deviated system activity would be considered as an intrusion.



Collaborative Defense Mechanism Using Statistical Detection Method against DDoS Attacks

- In [1], we proposed an anomaly detection method by using a cooperation scheme among distributed IDSs, namely source-end and victim-end IDRS.
- Each IDRS uses a proposed statistical detection scheme for reducing false negative rates (misses).

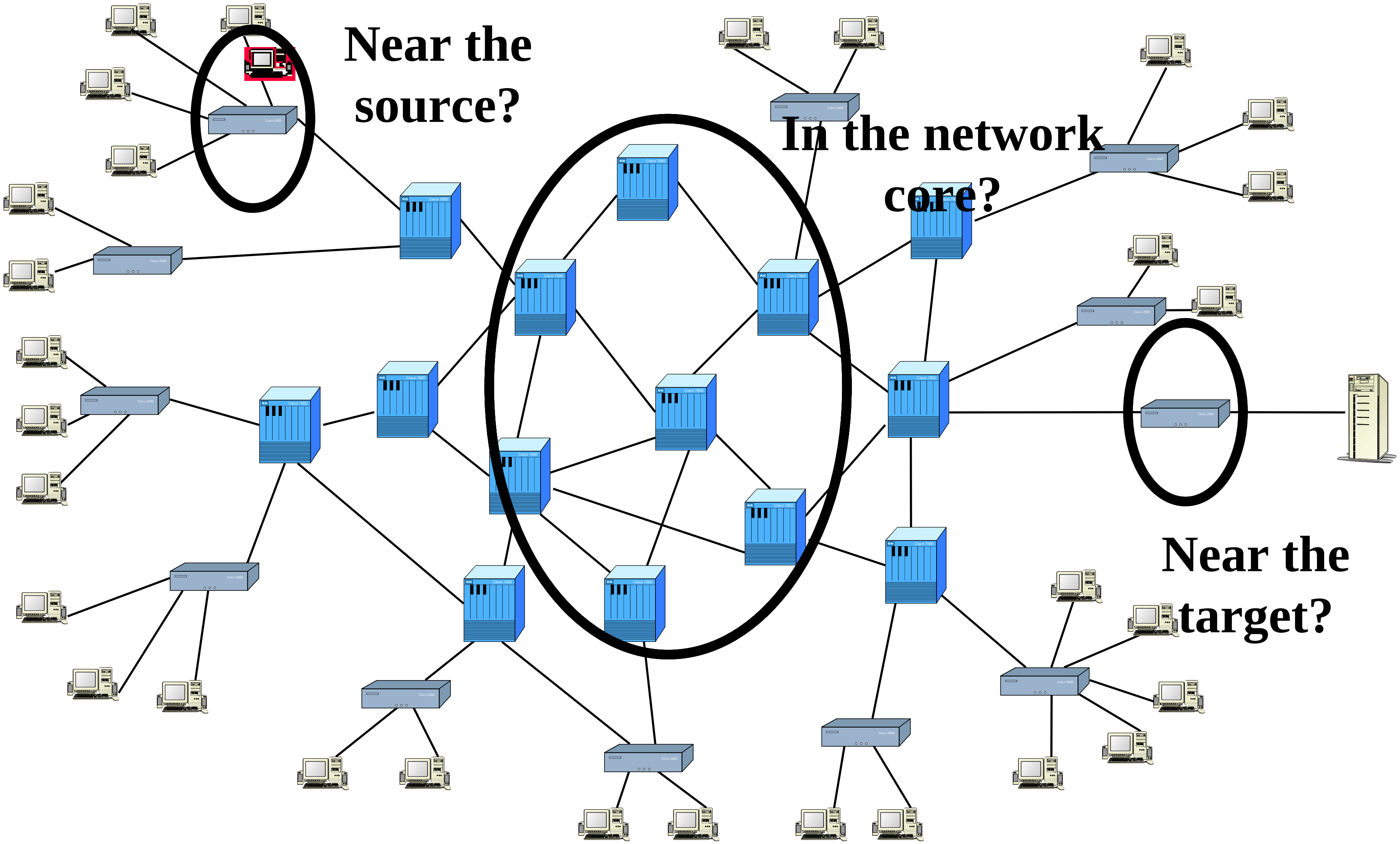


Intrusion Response Techniques

Approaches for Intrusion Response

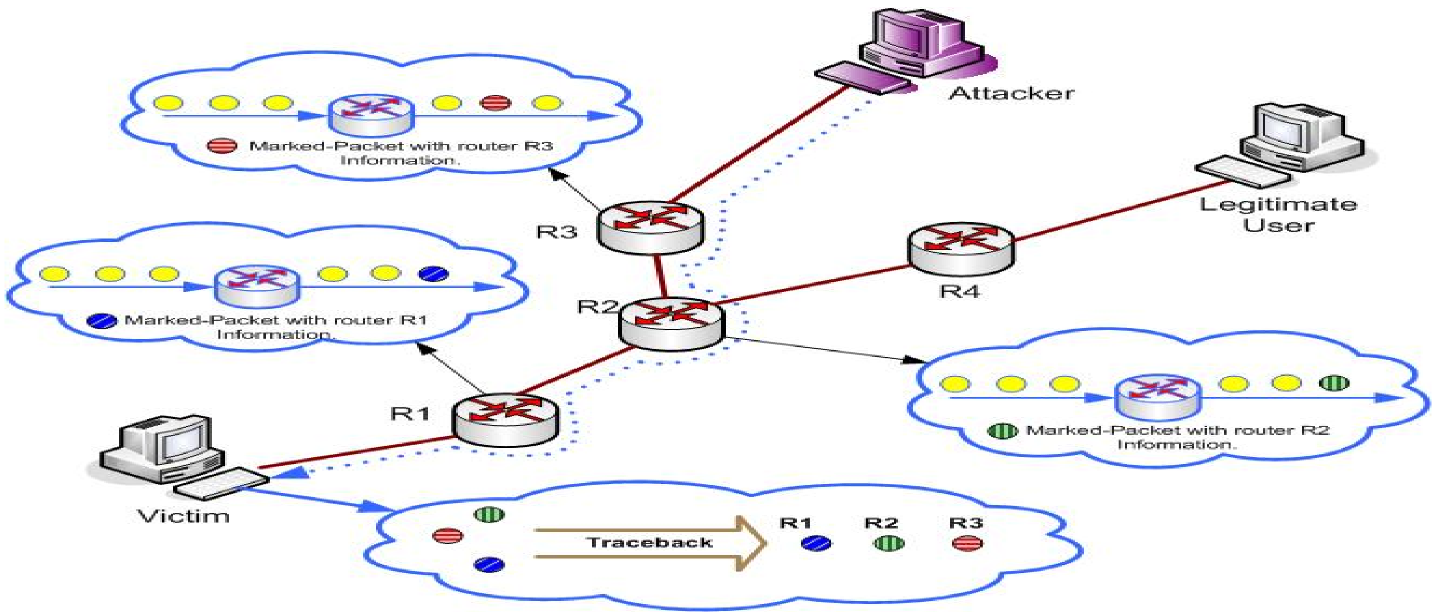
- Filtering
  - After identification of intrusion pattern a victim can filter the attack packets.
  - However this raise another issues about the place of filtering, as shown in next slide…..
- Traceback
  - Identification of the source of an attack.
  - Not trivial, in case of spoofed attacks.
  - Three basic ways of doing traceback:
    - Packet marking
    - Messaging
    - Logging

Where Do You Filter? : In multiple Places



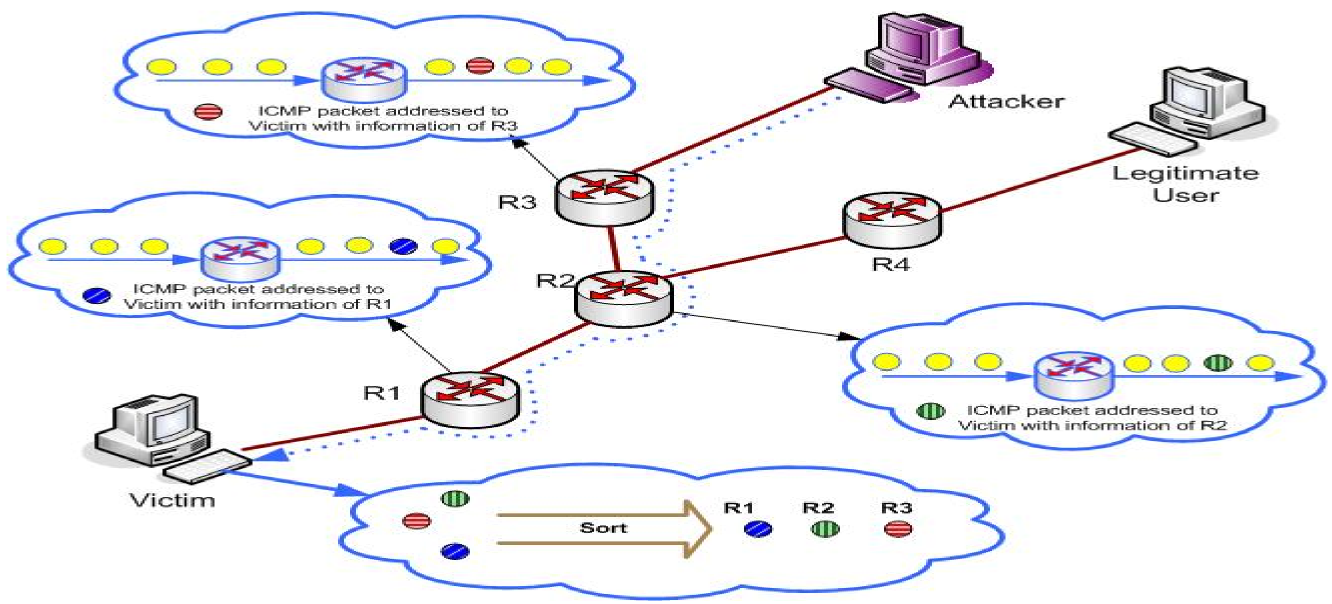
Traceback approaches

- Packet Marking
  - Routers probabilistically or deterministically mark path information in packets as they travel through the Internet.
  - Victims reconstruct attack paths from path fragments embedded in received packets.
  - Packet marking techniques can be subdivided in Deterministic Packet Marking (DPM) and Probabilistic Packet Marking (PPM).



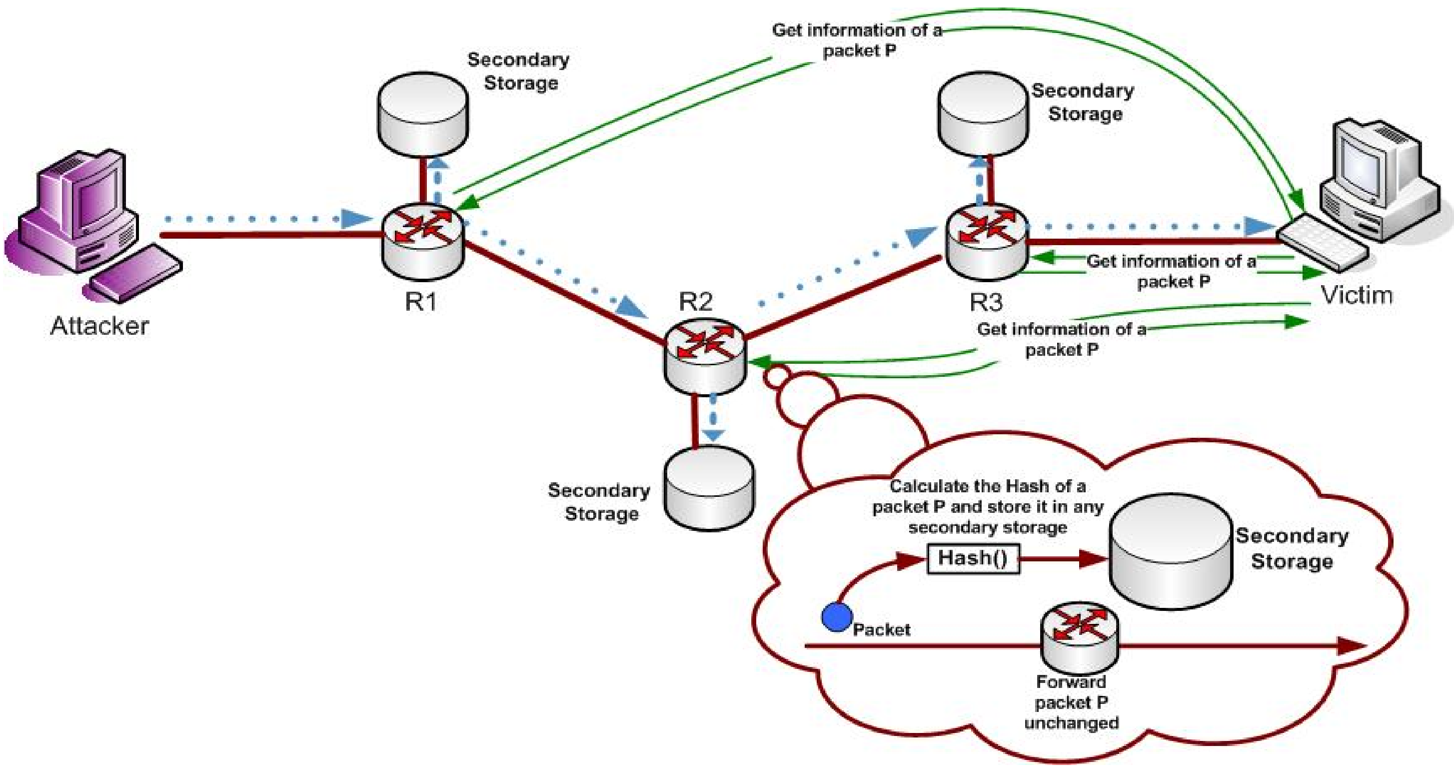
Traceback approaches

- Messaging
  - Routers probabilistically send messages, which contain the information of forwarding nodes the packet travels through, to the destination node.
  - Victims reconstruct attack paths from received messages.



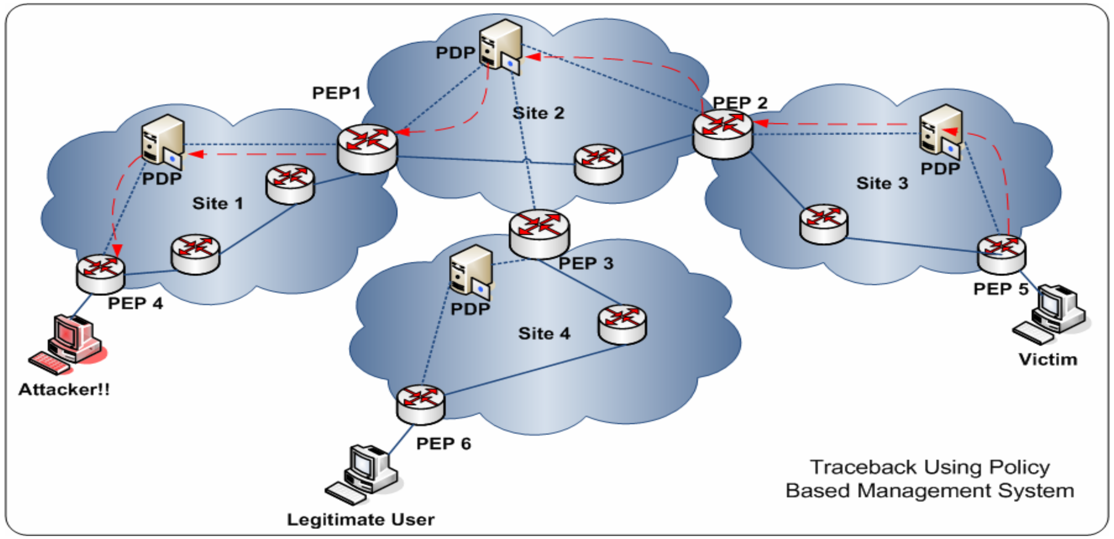
Traceback approaches

- Logging
  - Routers probabilistically or deterministically store audit logs of forwarded packets to support tracing attack flows.
  - Victims consult upstream routers to reconstruct attack paths .



Policy Based Traceback Scheme for IPv6 Networks

- Following figure shows our proposed IPv6 traceback scheme, namely PBIT (Policy Based IP Traceback) [2].
- According to the best of our knowledge, PBIT is the first traceback scheme for IPv6 networks.
- PBIT, uses messaging for controlling the traceback procedure, and packet marking for performing the postmortem of an attack.
- We used COPS protocol for the messaging, due to its object oriented nature.



Attack models, Intrusion Detection and Intrusion Response in IP-USN

Intrusion Detection and Response in IP-USN

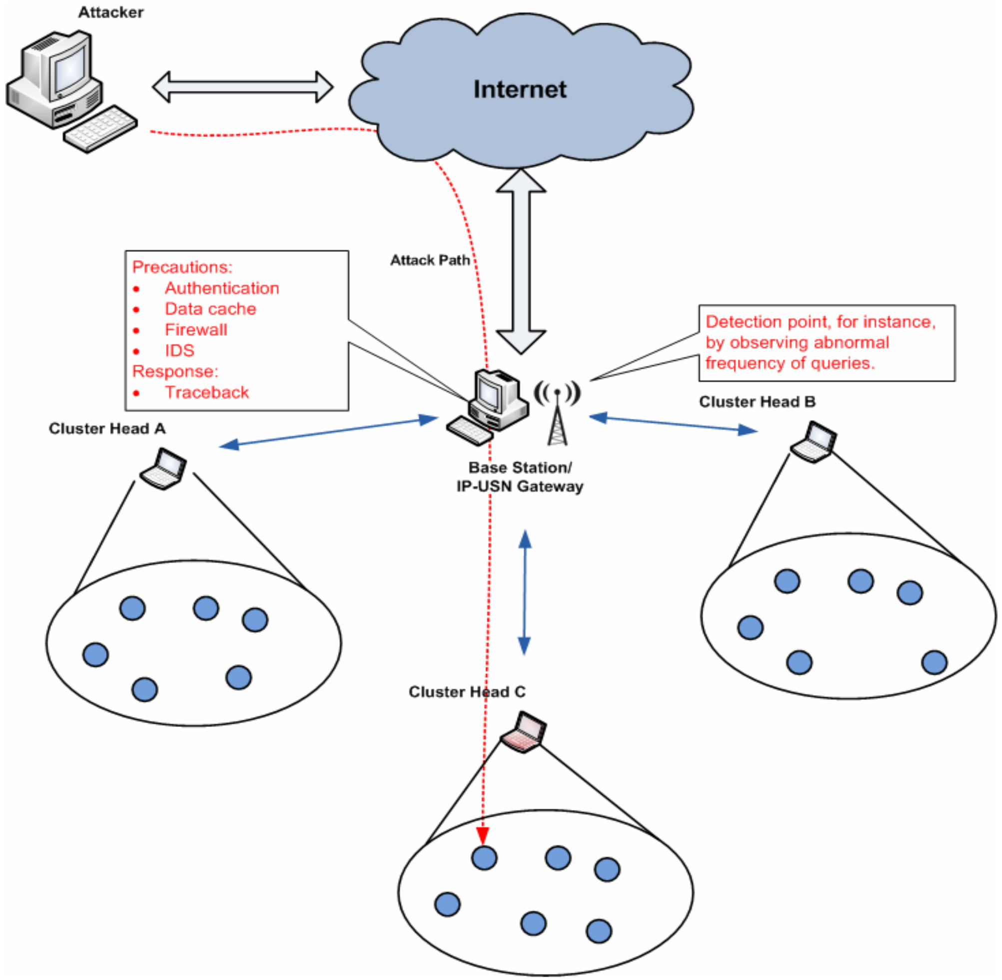
- IP-USN is in fact an integration of two different network paradigms.
- Merits and demerits of both worlds co-exist.
- IP-USN also embosses new security threats as discussed in following slides.

Attack models on IP-USN

- There are different possible attack scenarios in IP-USN:
  - Attacker trying to attack the sensor network via Internet.
  - Malicious or compromised sensor nodes feeding the false data to the sink or any user on the Internet.
  - Conventional sensor network attacks.

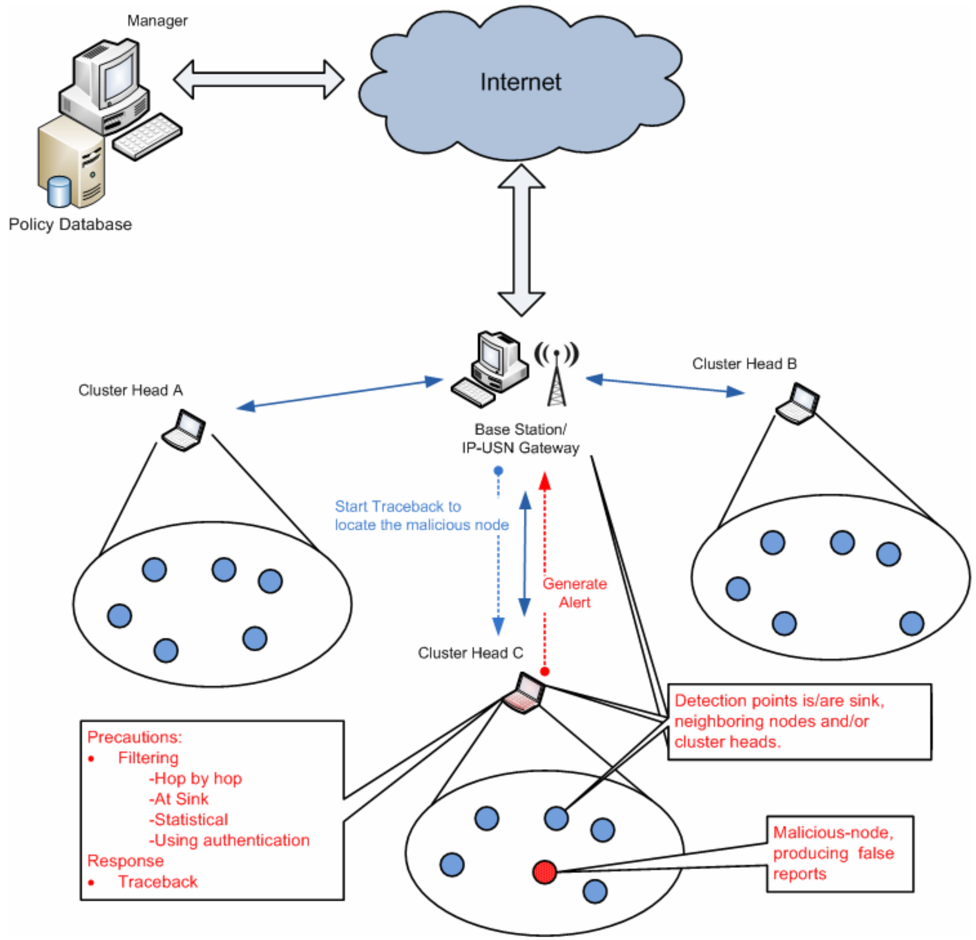
Scenario (1)

- Attacker trying to attack the sensor network via Internet.
  - Most likely, the detection point should be 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
      - Using authentication
    - At Sink (Same approaches for cluster heads)
      - By statistical way
- Response
  - Traceback
    - Identification of malicious node.

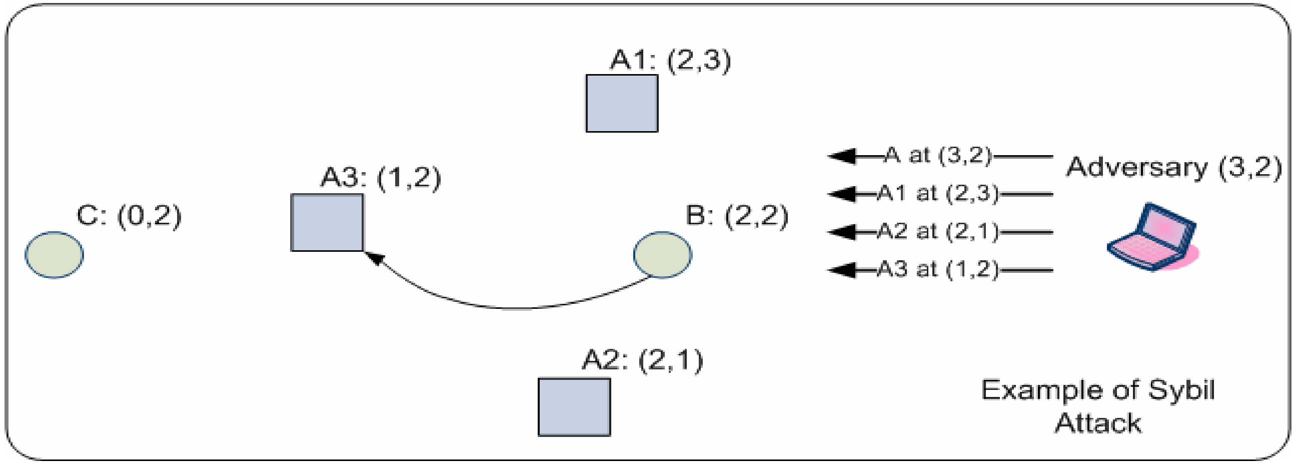


Scenario (3)

- 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
    - Wormhole attacks
    - Sybil attacks
    - Bogus routing information
    - Jamming attacks

Sybil attacks

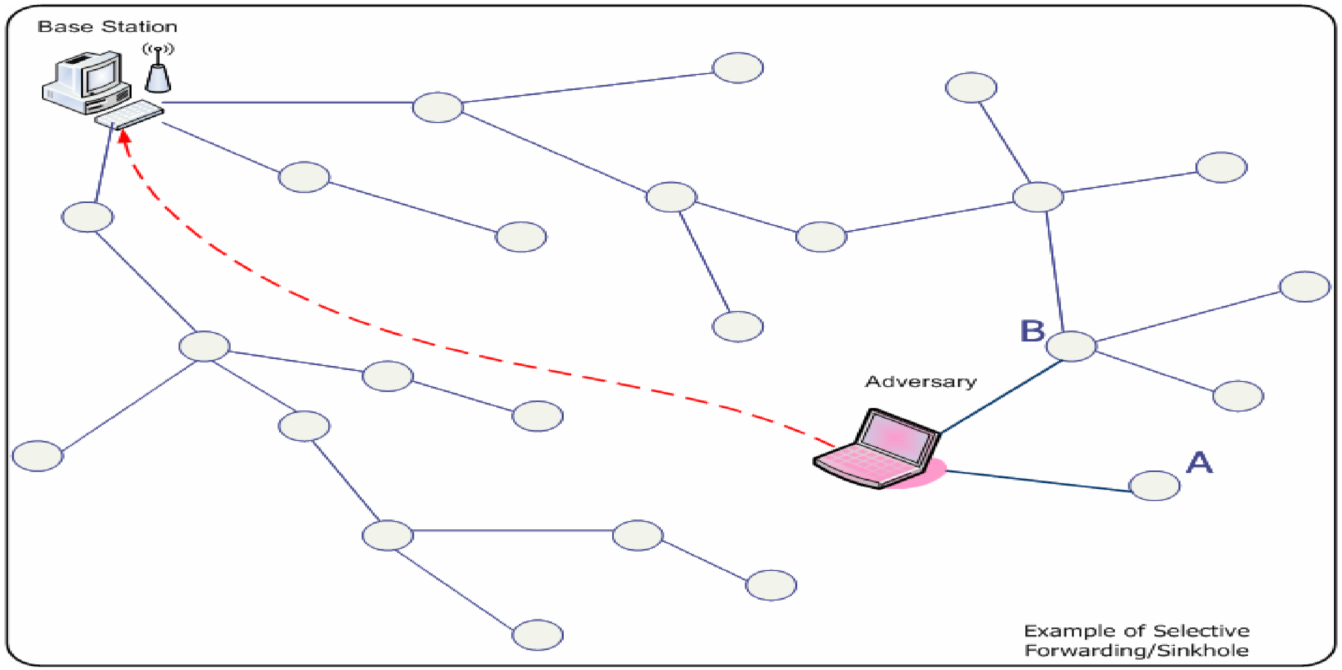
- A single node presents multiple identities to other nodes in the network.
- The Sybil attack against geographic routing.
  - Adversary at location (3,2) forges location advertisements for non-existent nodes A1, A2, and A3 as well as advertising his own location.
  - After hearing these advertisements, if B wants to send a message to destination (0,2), it will attempt to do so through A3.
  - This transmission can be overheard and handled by the adversary.
- Possible counter measure is to use authentication techniques.



Example of Sybil Attack

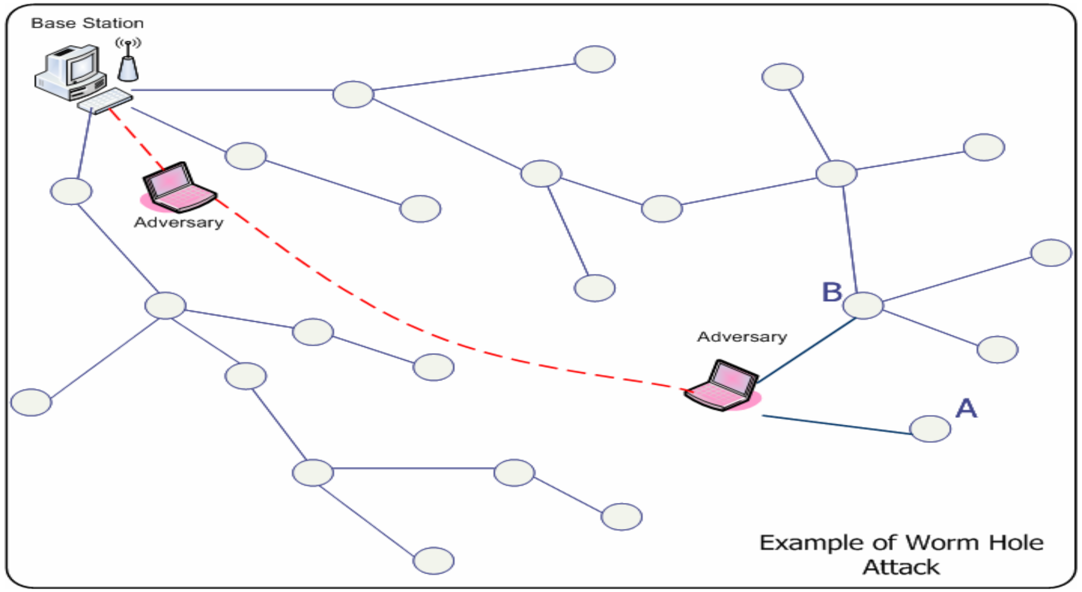
Selective forwarding, Sink hole Attack

- In a selective forwarding attack, malicious nodes refuse to forward certain messages and simply drop them.
- In a sinkhole attack, the adversary's goal is to bait nearly all the traffic from a particular area through a compromised node, creating a metaphorical sinkhole with the adversary at the center.
- Possible counter measure is to use statistical detection techniques



Worm Hole Attack

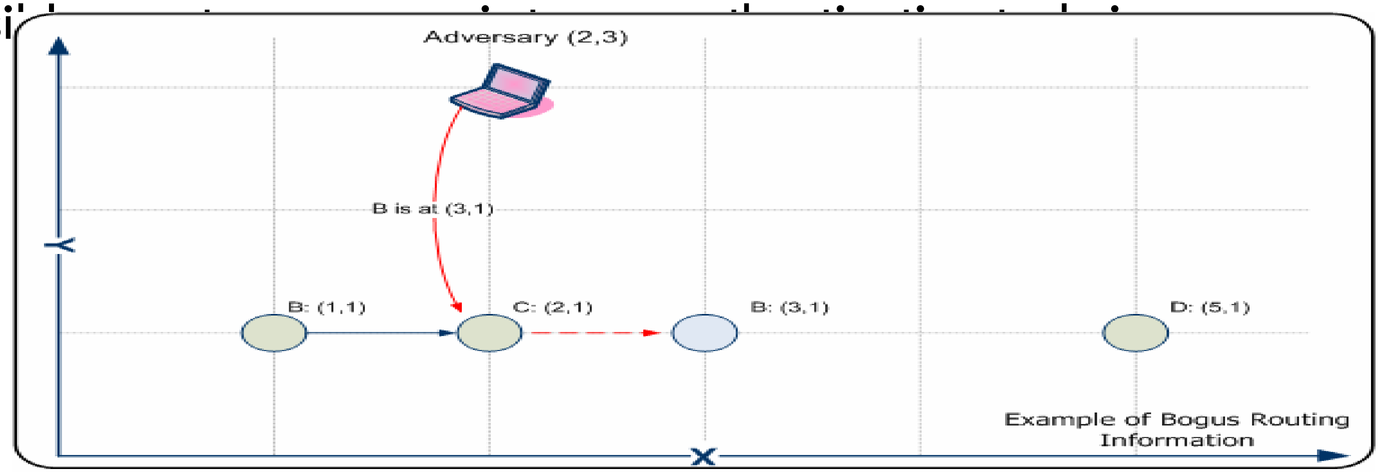
- An adversary tunnels messages received in one part of the network over a low latency link and replays them in a different part.
- Usually involves two distant malicious nodes colluding to understate their distance from each other by relaying packets along an out-of-bound channel available only to the attacker.



Example of Worm Hole Attack

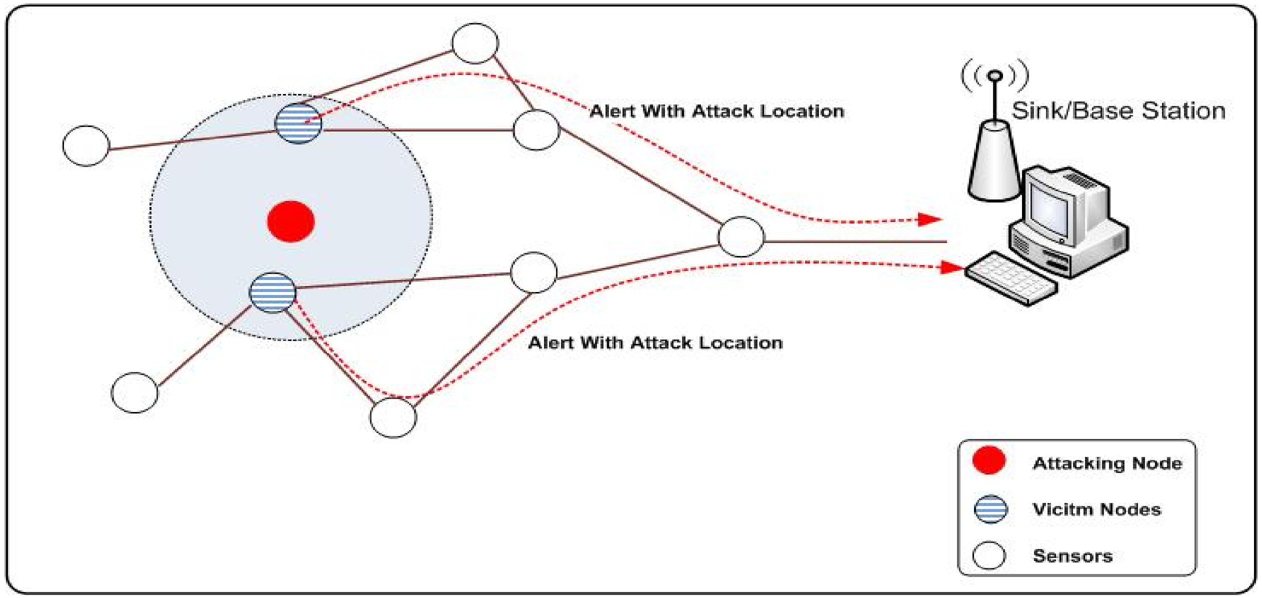
Bogus routing information

- With bogus routing information, adversaries may be able to:
  - Create routing loops,
  - Attract or repel network traffic,
  - Extend or shorten source routes,
  - Partition the network, increase end-to-end latency, etc.
- From B →D, Adversary forges a wrong information to claim B is in (3,1), so C will send packets back to B which causes loop at last.
- Possi



Jamming attacks

- Can be done at Physical, MAC and Application level.
- Simple to implement.
- Could be severe for resource constrained sensor nodes.



Current Research Activities

Current Status

- Handling the jamming attacks on IP-USN.
- Jamming attacks can be launched by
  - Attacker trying to attack the sensor network via Internet, this case can be avoided by:
    - 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.
  - Within sensor network:
    - By compromised nodes
    - By external nodes

Types of jamming attacks on IP-USN

- Other than physical layer the (D)DoS attack can be performed at
  - MAC Layer
    - With the help of MAC layer jamming, by violating the rules imposed by specific MAC layer. For instance,
      - In 802.11, using minimum $CW_{min.}$
      - Using reduced DIFS
      - Allocating large NAV timers and so on.
    - Difficult to launch, but could cause a severe damage.
    - Detecting MAC layer jamming allow victim to switch to another channel for data transmission and reception.
  - Application layer
    - Generating useless data at high speed so that network congestion occurs.
    - Easy to launch, however relatively easy to be caught.
- We've implemented the detection algorithm for application layer flooding attacks and working on MAC layer flooding attacks.

Attack Model

- We consider the active jamming type in-network (D)DoS attacks.
- In general, jamming-type (D)DoS attacks have the property of abnormal traffic volume.
- Moreover, we assume that, attackers can disguise their location using incorrect/spoofed addresses and attacks may persist for tens of minutes.
- The attacker can compromise the nodes and can have the critical information including secret keys.

Network Model

- Densely deployed sensor nodes:
  - So that there are more than one path to reach the sink and/or there are multiple sinks to receive data.
- Secure networking protocol is working on the network, such as μTesla *(Micro version of Timed, Efficient, Streaming, Loss-tolerant Authentication Protocol)*
- Any MAC protocol which relies on RTS/CTS/DATA and ACK packets is running on a medium access layer.
  - Capable to adapt other MAC protocols however; abnormality criterion must be defined for those scenarios.
- Here we only present the effects of application layer jamming using AODV routing.
- Same scenario has been implemented in flood based routing and the results were much worse than AODV.

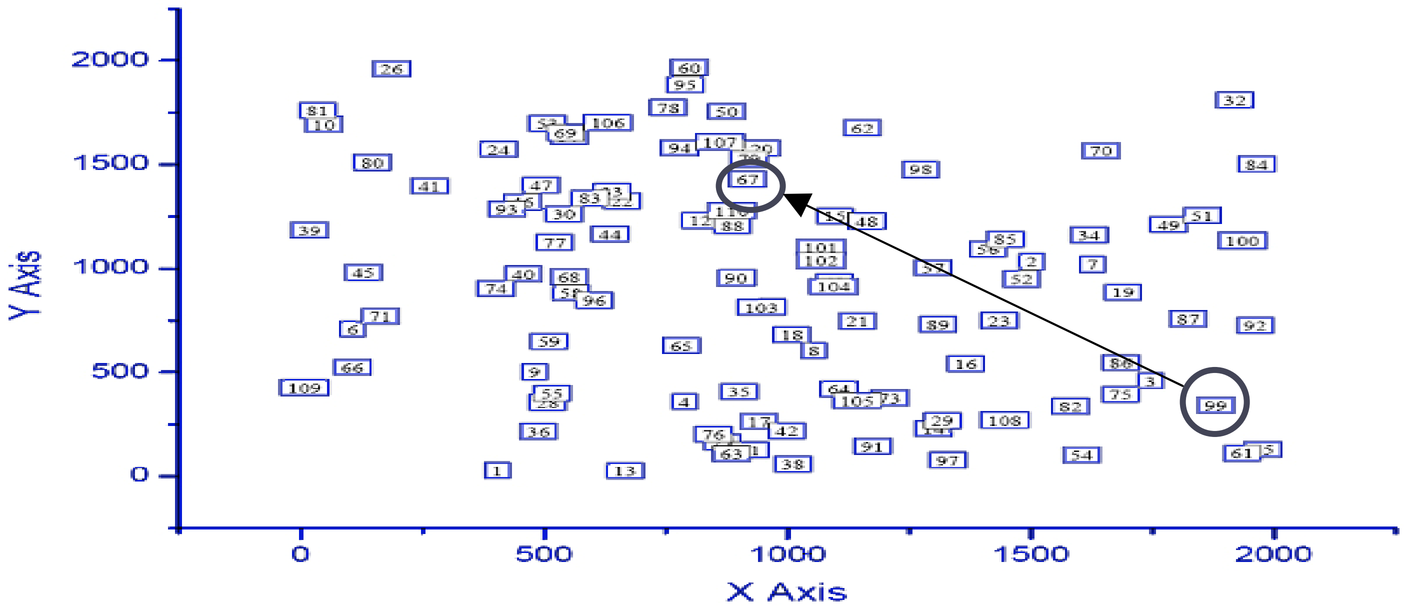
Simulation parameters

Using SENSE (Sensor Network Simulator and Emulator) :
http://www.ita.cs.rpi.edu/sense/index.html

Parameter	Value
Terrain	*2000 x 2000 meters*
Number of nodes	*110*
Number of attackers	*1 to 10*
Packet size	*500 Bytes*
Data rate	*250Kbps*
MAC protocol	*Modified 802.11 (for data rate)*
Attacker transmission Interval	*2 ms*

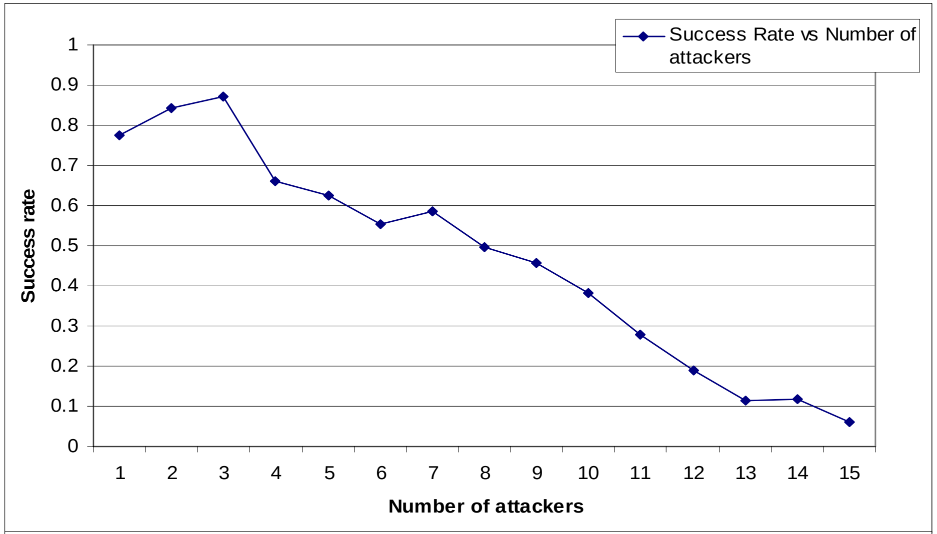
Network Topology

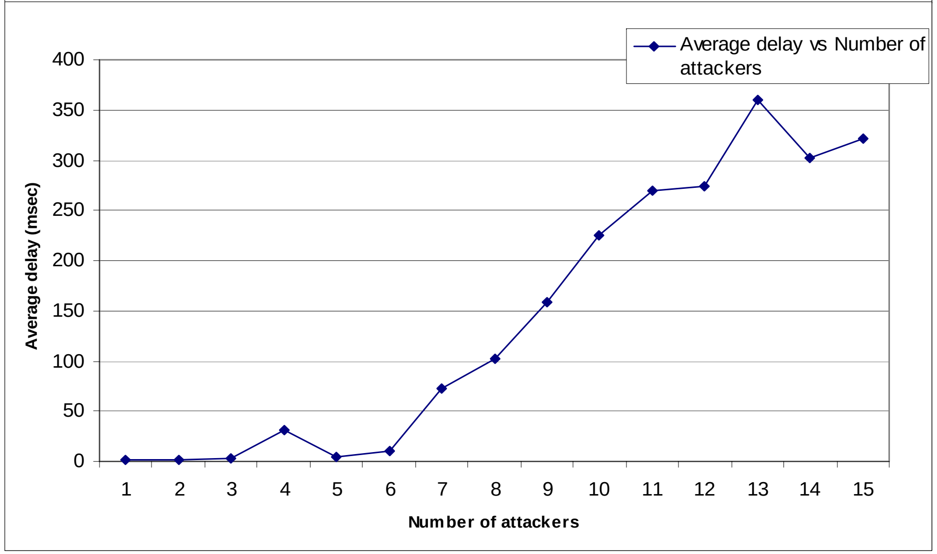
- To derive the motivation we perform the simulation to see the results of jamming attacks on IP-USN performance.
- For this purpose we took the following network model.
- Sender/receiver pair is made randomly out of this topology.
- For example, in this figure, node number 99 sending data at high rate to node 67, as a result all the nodes en route, experience congestion. As shown in following slides.



Effects of jamming on network performance (1/3)

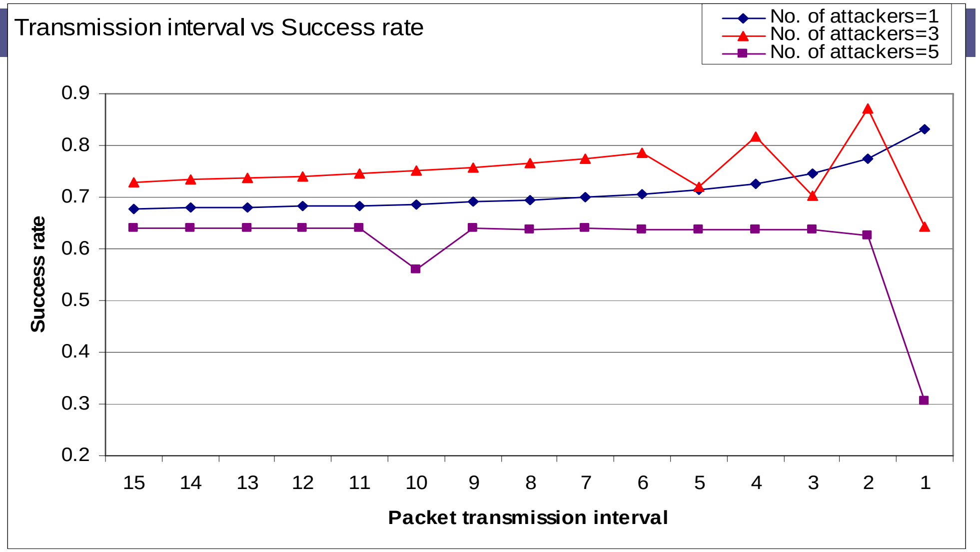
- According to our study, the jamming attacks reduce the performance of sensor network drastically.
- Graph on top shows the success rate with increasing number of attackers and constant packet size of 1000 bytes.
- Bottom graph shows the average delay (ms) in packet transmission.
- It is evident that as number of attackers increases the success rate decreases and average delay increases.

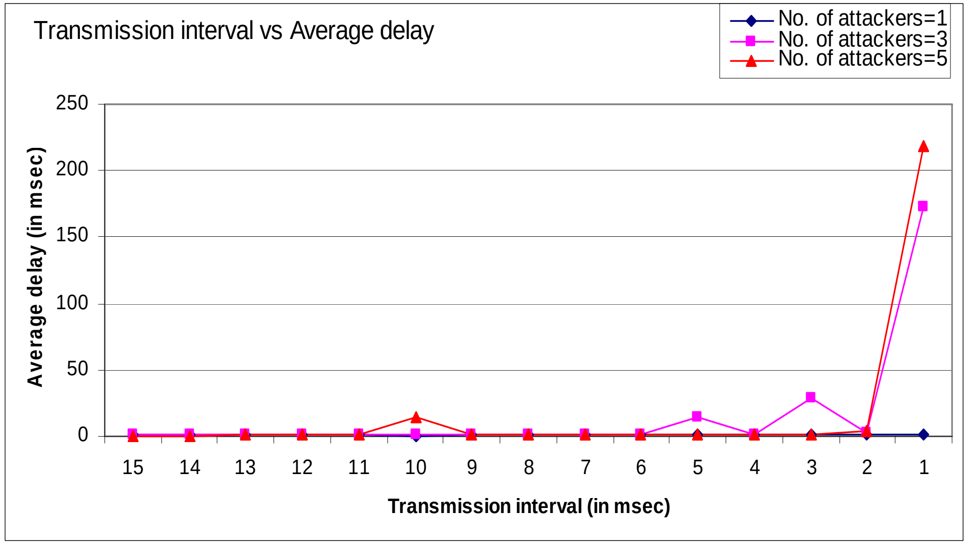




Effects of jamming on network performance (2/3)

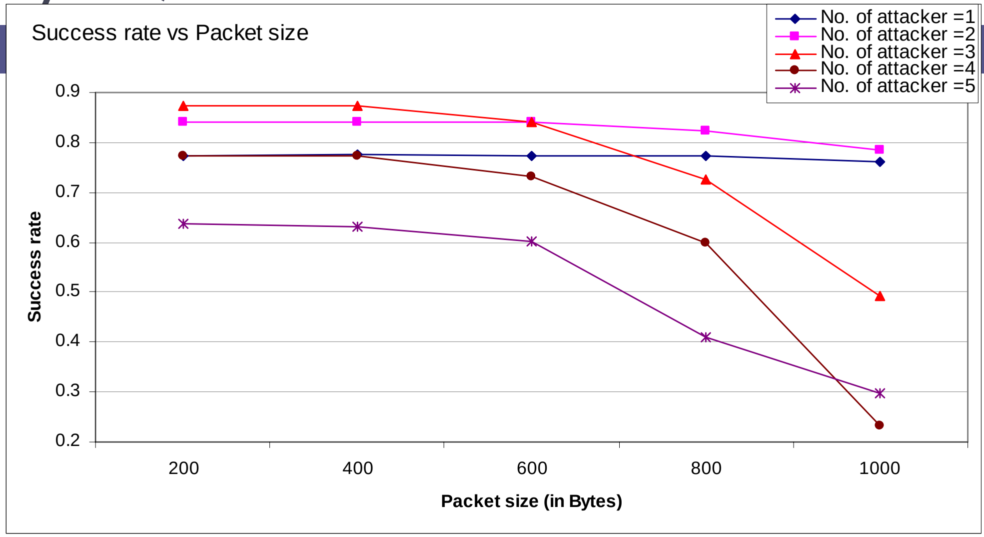
- If an attacker increases the transmission rate, the results are little deviated from usual behavior.
- Graph on top shows the success rate with increasing transmission rate.
- Bottom graph shows the effect of transmission rate on average delay (ms) in packet transmission.
- We can observe that as the transmission rate increases:
  - The success rate increases up to certain point and then starts to decrease gradually.
  - Average delay decreases rapidly up to some point and than becomes stable.

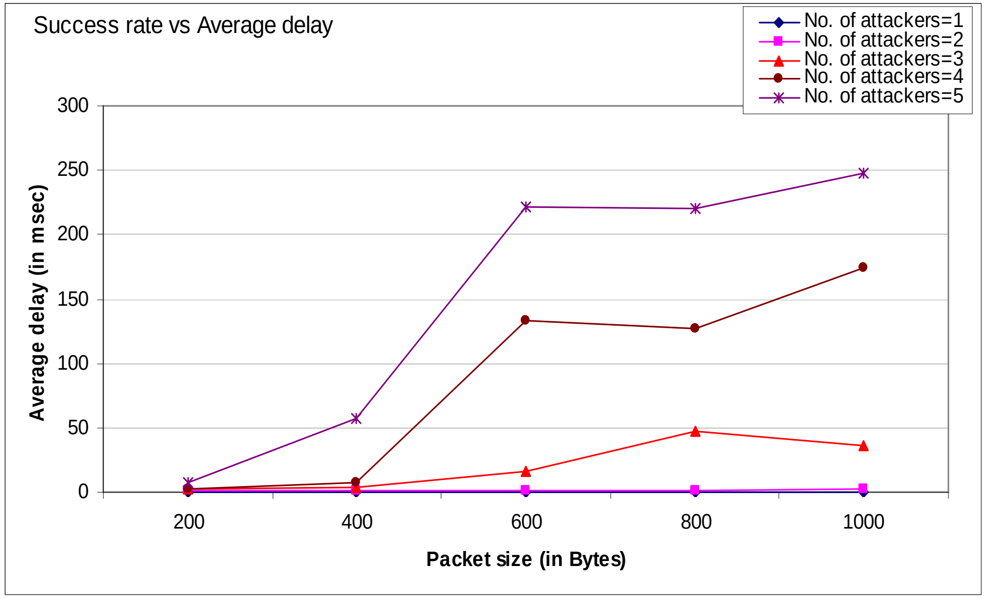




Effects of jamming on network performance (3/3)

- Graph on top shows the success rate as an attacker increases the packet size.
- Bottom graph shows the effect of packet size on average delay (ms) in packet transmission.
- We can observe that
  - As the packet size increases the success rate decreases.
  - Average delay shows some random behavior because of MAC protocol which gives the chance of transmission to other nodes even if there are malicious nodes in the network.





Lightweight Intrusion Detection for USN

Detection Strategy

- To detect the jamming attack we propose a collaborative approach of intrusion detection.
- 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 will generate an alarm to the base-station.
- The alarm will contain 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.

Application Layer Flooding

- 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.

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

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

- Our scheme is not resource hungry as instead of calculating average of whole block we only take new values in account.

Application Layer Flooding

- Each node listens the packet in promiscuous mode and calculates the mean of packet inter-arrival time for the first 2,000 packets.
- For the rest of the packets we use EWMA for calculation.
- After calculating mean, our study is focusing on deriving the threshold value, after which an attack signal should be raised.
- To perform this we derive a normal distribution of the readings gathered from all of the nodes. Which is given by:

$$z = \frac{x - \mu}{\sigma}$$

where

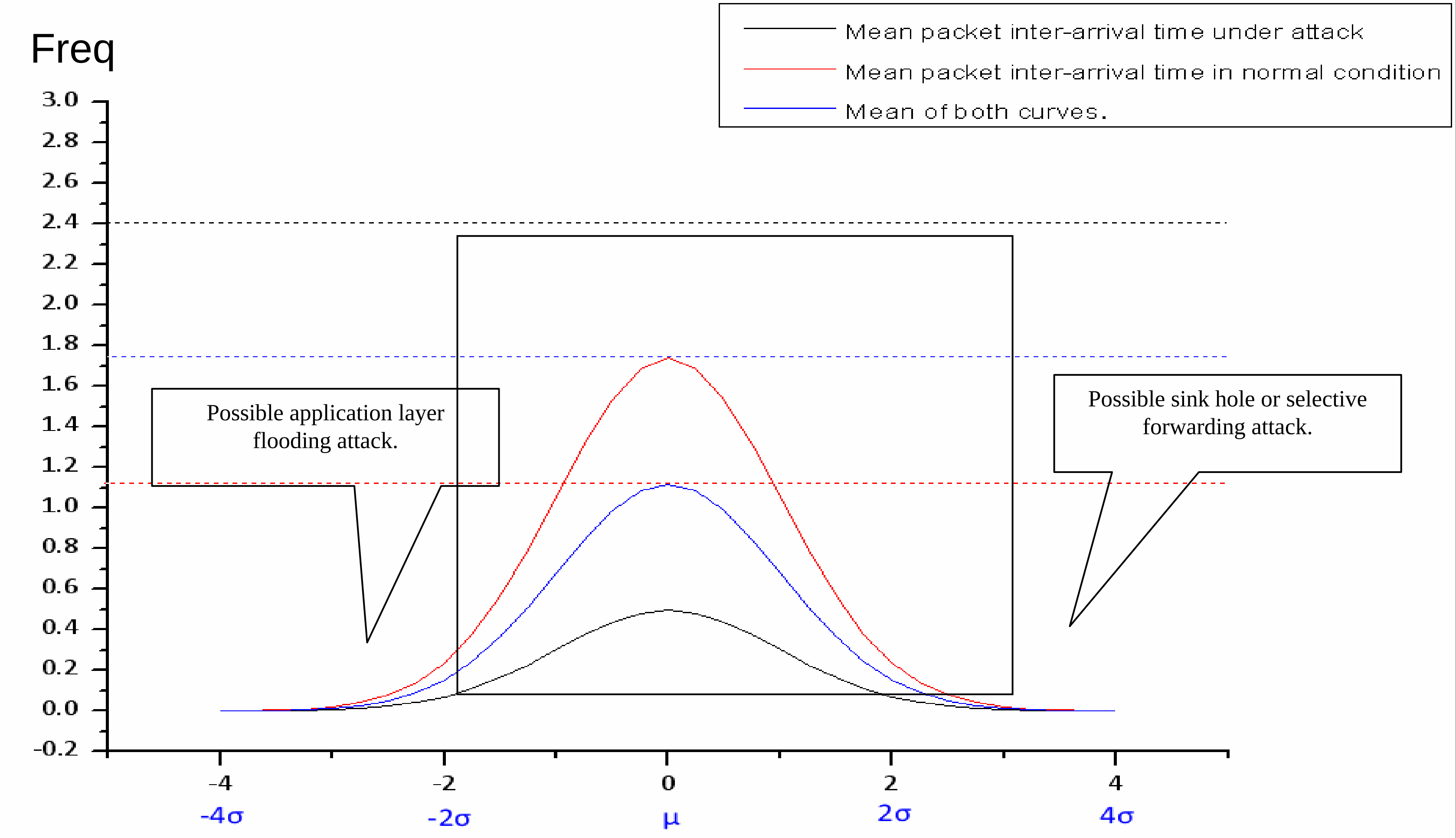
$z =$ Standard Random Variable

x= Random variable (in our case packet inter arrival time)

μ=Mean

σ=Standard Deviation

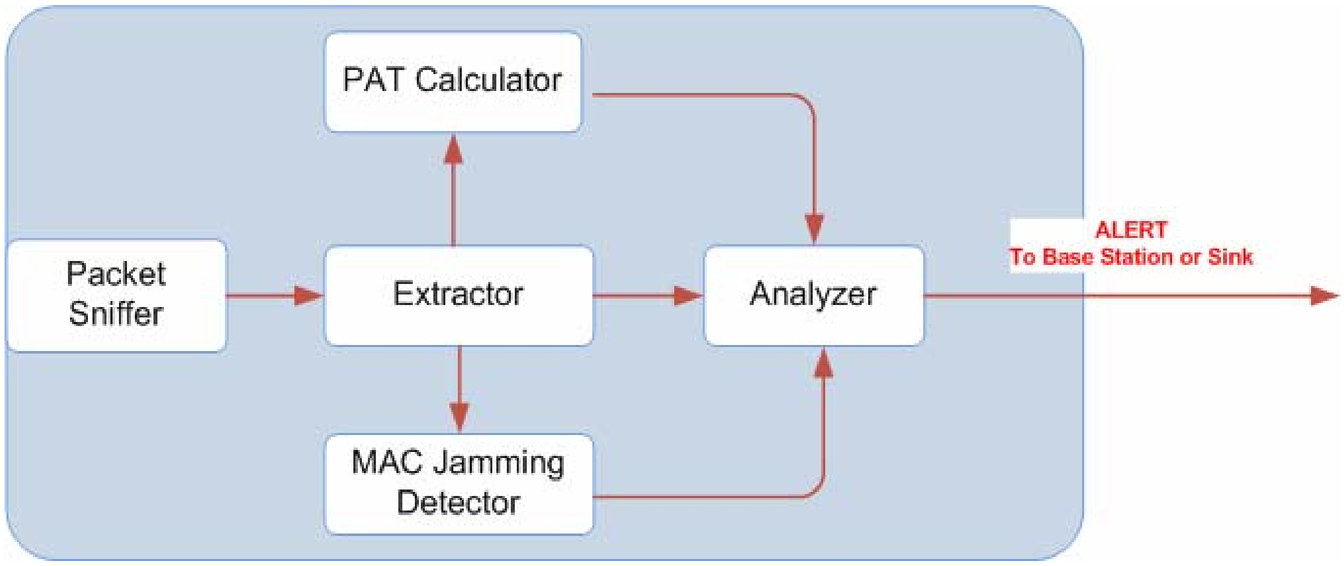
Normal Distribution



Detecting MAC Layer Jamming

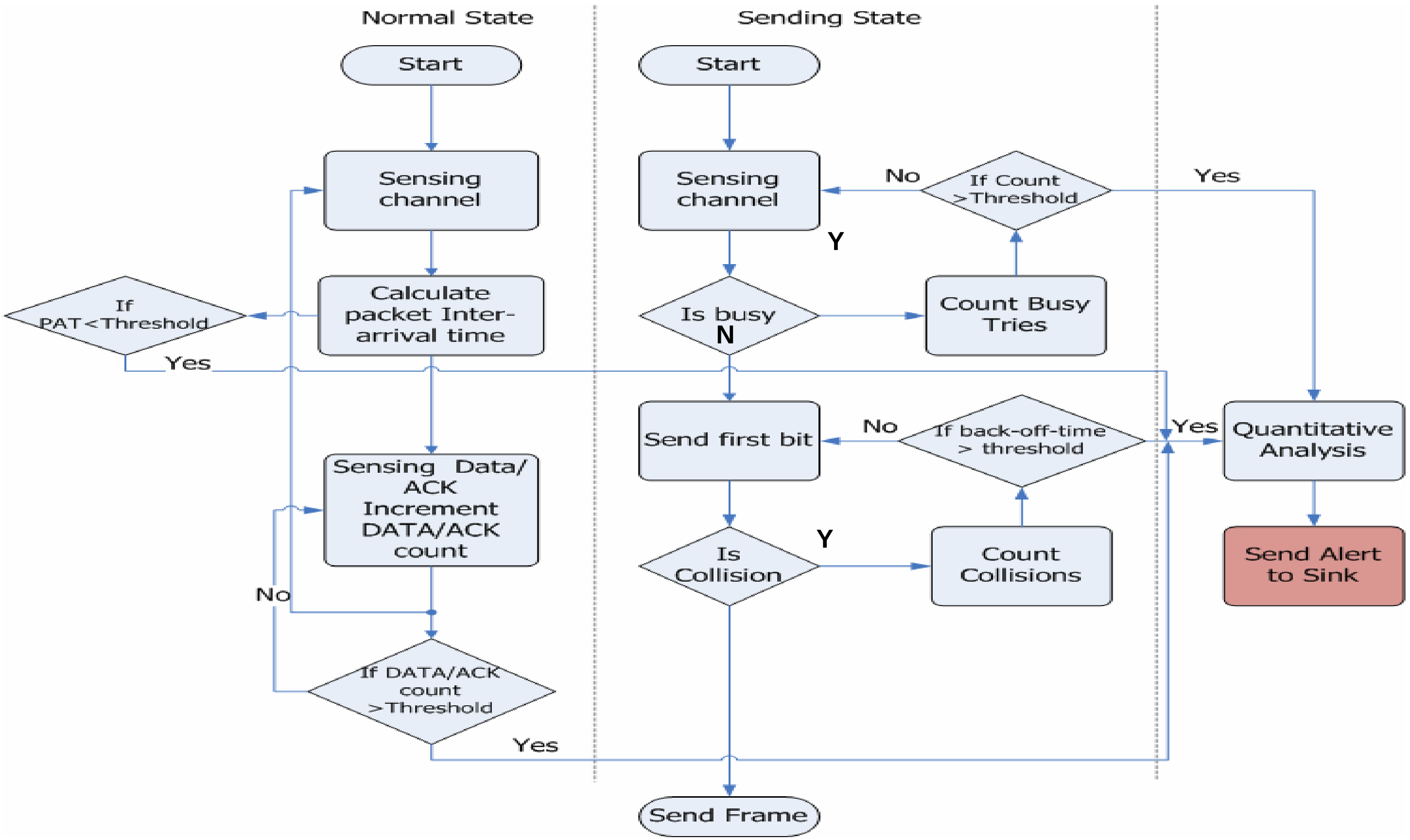
- Few of the abnormalities are discussed as follows:
  - **Increased channel busy time:** A node may observe frequent busy time and consequent transition from back-off state to defer stage which is an indication of heavy traffic.
  - **Increased frames:** As attack packets are increased, the number of data frames and ACK are increased. In addition, to access channel, the number of RTS and CTS frames are also increased.
  - **Increased number of collisions:**
    - Increased retry count due to lack of ACK or CTS.
    - Large contention window (CW) which depends upon retry count.
    - Long lifetime of fragments.

Major Components of USN IDS



Detection Algorithm

(Contention State)



Approaches for Intrusion Response in IP-USN

- Traceback
  - An integrated traceback scheme is required which can work on IP as well as on sensor networks.
  - Logging:
    - Sensor networks are resource constrained networks
    - Having very limited storage capabilities
    - Therefore, logging packet information doesn't seem as a good option.
  - Messaging:
    - Due to broadcast nature of sensor networks seems nice, so that single transmission can disseminate the packet information to multiple nodes.
    - However, we know that sensor consumes more energy in transmission than processing.
    - Therefore messaging should be occasional.
  - Packet Marking:
    - This approach inherits drawbacks of traditional packet marking traceback schemes and symmetric cryptography such as increased packet size and key management issues.
    - Therefore, not tempting for sensor networks.
- We believe that in sensor networks, intrusion detection can support traceback operations, with the help of messaging architecture.

Future Work

- Working on scheduling framework so that instead of all nodes few candidate nodes runs the detection algorithm.
- Implementing other proposal for comparison.
- Have to see the effects of other routing protocols, such as DSR

References

[1] Byunghak Song, Joon Heo and Choong Seon Hong, “Collaborative Defense Mechanism Using Statistical Detection Method against DDoS Attacks”, to be published (Oct. 2007) in IEICE Transaction on Communications.

[2] Syed Obaid Amin, Choong Seon Hong, Ki Young Kim, "Tracing the True Source of an IPv6 Datagram Using Policy Based Management System", LNCS 4238(APNOMS 2006), pp.263-272, September 2006.

[3] Karlof, C. and Wagner, D., “Secure Routing in Sensor Networks: Attacks and Countermeasures”, Ad Hoc Networks, Vol. 1, issues 2-3 (Special Issue on Sensor Network Applications and Protocols), pp. 293-315, Elsevier, 2003

Thank you!