A New Method for Intrusion Detection on Hierarchical Wireless Sensor Networks

Rung-Ching Chen, Chia_Fen Hsieh and Yung-Fa Huang
Chaoyang University Of Technology
Taiwan

Presenter - Bob Kinicki
rek@cs.wpi.edu

***The Third International Conferences on Ubiquitous Information Management and Communication,*(ICUIMC-09) Suwon, S. Korea**
January 15-16, 2009

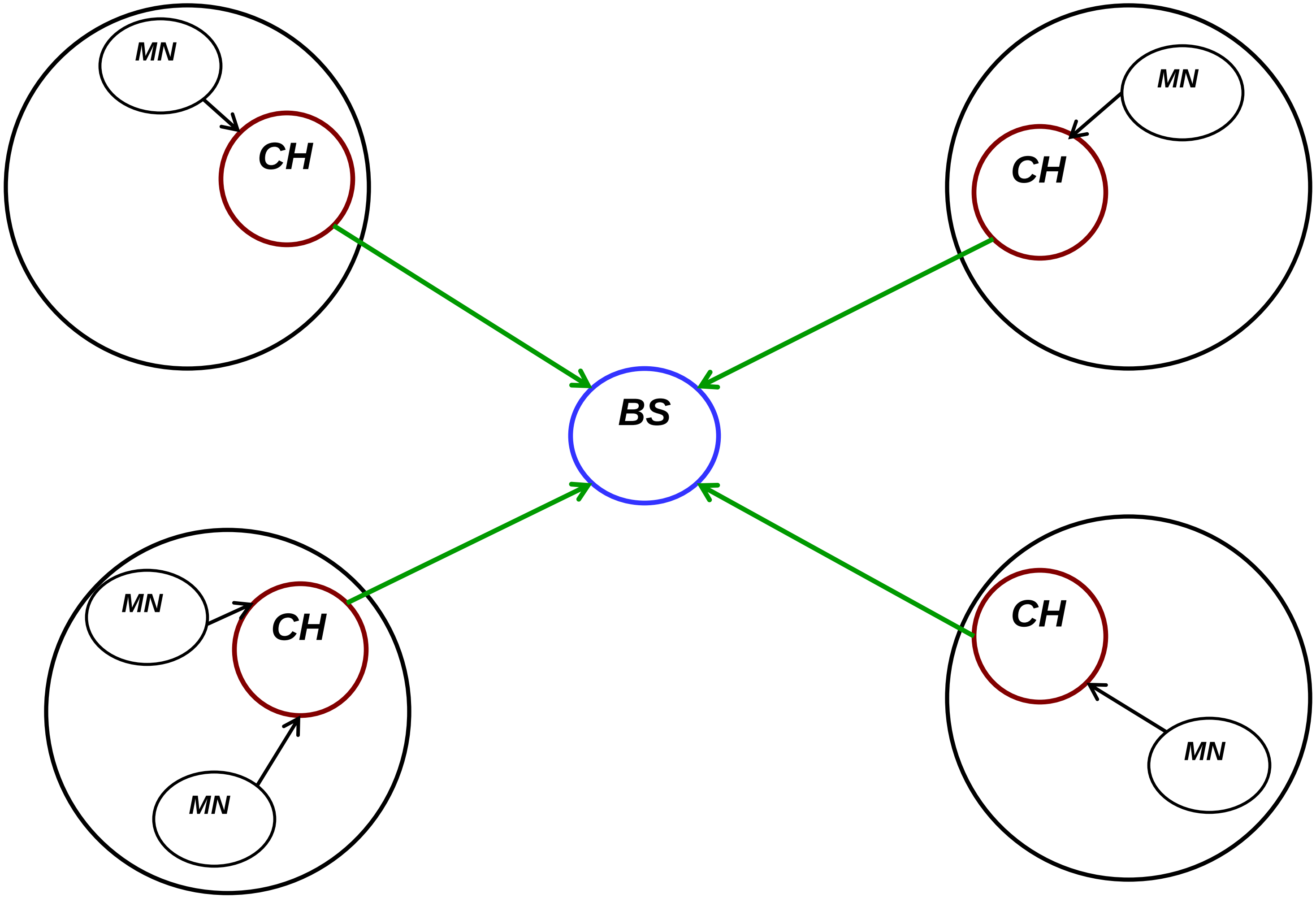
Outline

- *Introduction*
- Intrusion Detection Systems (IDS) for Wireless Sensor Networks
- Collaborated-Based Intrusion Detection
- Routing Table Intrusion Detection
- Isolated Table Intrusion Detection System
- Comparison Experiments
- Conclusions/Criticisms

Introduction

- Energy conservation is the critical performance consideration to extend WSN lifetime.
- This paper adopts cluster-based WSN (CWSN) as their choice to extend network coverage and increase lifetime {They reference the Leach paper [Heinzelman]}.

Cluster Architecture



Cluster Hierarchy

- MN (Member Nodes) deliver sensed data to the BS (Base Station) through their CH (Cluster Head).
- CHs are chosen as center of cluster and data from MN is aggregated before being sent to BS.
- {Note – paper ignores dynamically changing CHs.}

WSN Security

- Authors divide WSN security roles into IDS (Intrusions Detection Systems) and IPS (Intrusion Protection System).
- IPS uses authentication and symmetric keys to defend system from outside attackers (Not part of this paper).
- IDS identifies attackers using a rules database via anomaly data (e.g., signatures).

WSN IDS

- This paper uses term '**anomalies**' and relies on detecting them.
- With WSN, IDS database must be smaller due to limited resources.
- Attack behavior is different in WSN and draining sensor energy and breaking network connectivity are possible attack strategies.

Stated Objectives

1. Use IDS to isolate intruders in WSN.
2. Reduce IDS energy consumption to extend WSN lifetime.
3. Find balance between energy consumption and WSN security.

Outline

- Introduction
- *Intrusion Detection Systems (IDS) for Wireless Sensor Networks*
- Collaborated-Based Intrusion Detection
- Routing Table Intrusion Detection
- Isolated Table Intrusion Detection System
- Comparison Experiments
- Conclusions/Criticisms

IDSs for Wireless Sensor Networks

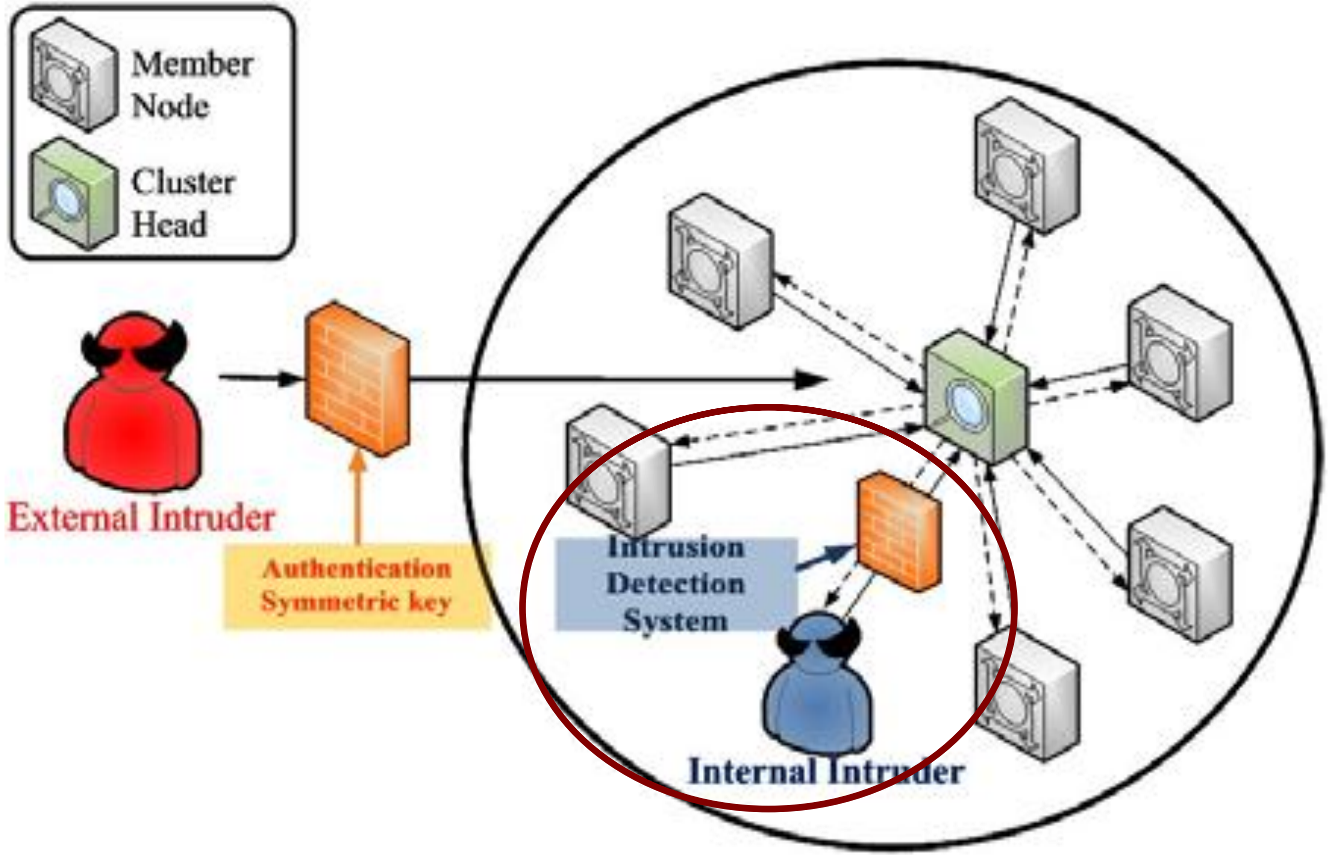


Figure 1.The Secondary Defense of WSNs

Stages of WSN Attack Behaviors

1. **Preparation stage**
   - Probing the communication of the BS and gathering info from the WSN.
   - Intrusion often happens in the connection between the BS and CHs.
2. **Attack and Occupy stage**
   - Uses victim components (spoof, alter or replay routing info and selective forwarding).

Stages of WSN Attack Behaviors

3. Doom Stage

- This paper focuses on these forms of attack to crash WSN:
  - including Hello Flooding, Denial of Service, Denial of Sleep, Sinkholes and Wormholes.
- Goal is to attack CH and need to occupy a sensor (an MN) to intrude CH. Essentially, try to consume CH resources until CH energy exhausted.

Outline

- Introduction
- Intrusion Detection Systems (IDS) for Wireless Sensor Networks
- *Collaborated-Based Intrusion Detection*
- Routing Table Intrusion Detection
- Isolated Table Intrusion Detection System
- Experiments Comparison
- Conclusions/Criticisms

Collaboration-based Intrusion Detection (CID)

- CH runs whole network: controls and monitors MNs and communicates with BS.
- Uses several security levels. Level is determined by thresholds.
- MNs divide into Monitor Groups (MGs) to reduce energy and to monitor CH using authentication methods.
- Structure and alarm thresholds set by an administrator.

Collaboration-based Intrusion Detection (CID)

- CH detects anomaly MNs and isolates them.
- When MNs raise alarms above threshold, they can depose CH.
- CID weaknesses when CH changes:
  - when CH changes, new CH does not obtain old isolation information.
  - new CH consumes extra energy monitoring MNs again for malicious nodes.

Outline

- Introduction
- Intrusion Detection Systems (IDS) for Wireless Sensor Networks
- Collaborated-Based Intrusion Detection
- *Routing Table Intrusion Detection*
- Isolated Table Intrusion Detection System
- Comparison Experiments
- Conclusions/Criticisms

Routing Table Intrusion Detection (RTID)

- WSN routing table used to detect anomaly behaviors.
- Example in Figure 3, static sensors topology uses a spanning tree with hops metric in the IASN table.
- IASN (Information Authentication for Sensor Networks) Table holds information such that arriving sensor data is compared against valid info coming correct path.

Routing Table Intrusion Detection (RTID)

- Both information sent along the wrong path or invalid information deemed anomalous by IASN table.
- Actual routing is DSDV (Destination-Sequenced Distance Vector).
- Problem is each sensor must store DSDV routing table and IASN table.

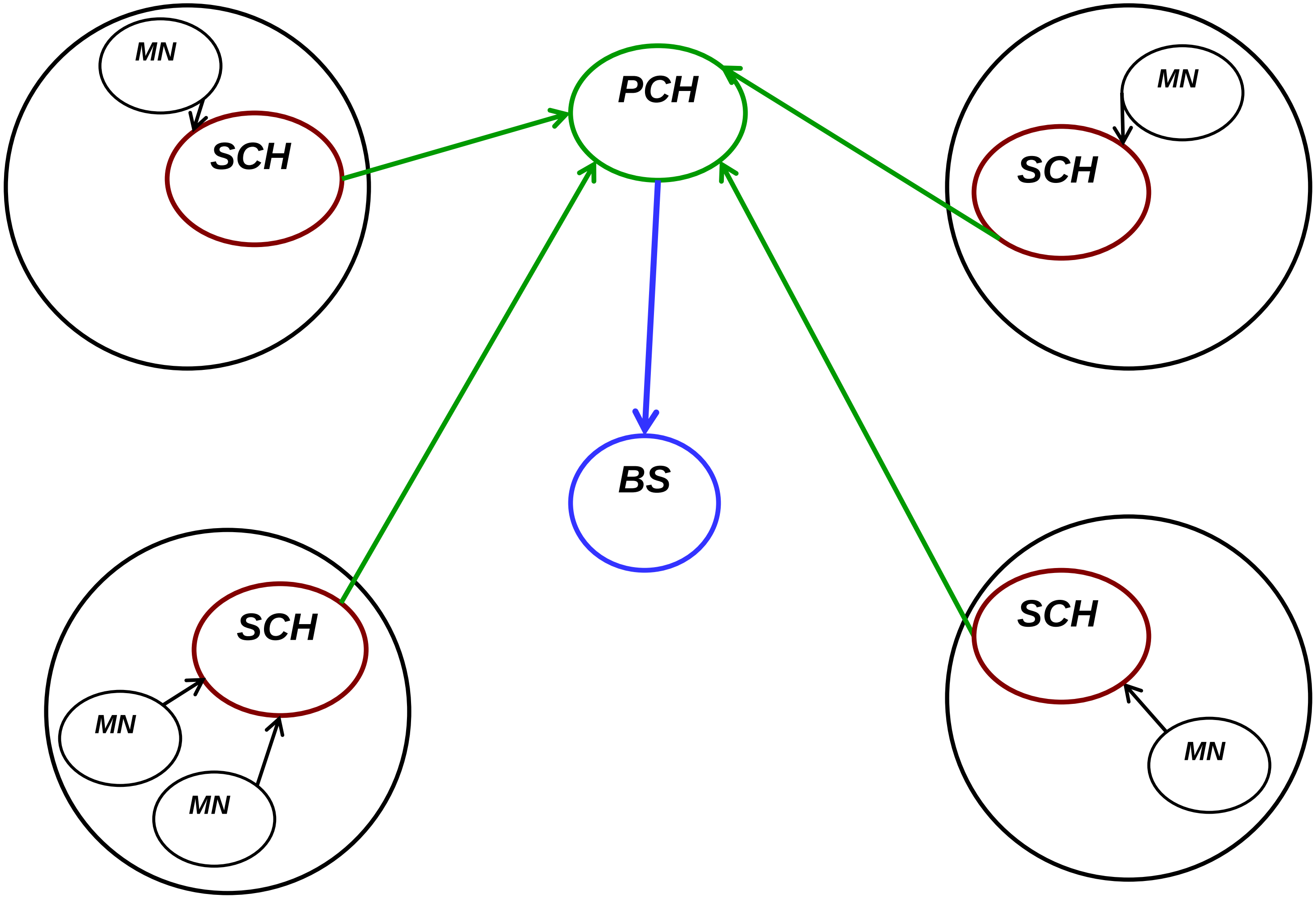
Outline

- Introduction
- Intrusion Detection Systems (IDS) for Wireless Sensor Networks
- Collaborated-Based Intrusion Detection
- Routing Table Intrusion Detection
- *Isolated Table Intrusion Detection System*
- Experiments Comparison
- Conclusions/Criticisms

Isolation Table Intrusion Detection System (ITIDS)

- Authors claim: to save on energy consumption of sensors employ an isolation table for IDS.
- Node types: 1 BS, 1 Primary Cluster Head (PCH), 1 Secondary Cluster Head (SCH) per MG where MNs are assigned to MGs.

Modified Cluster Architecture



ITIDS Architecture

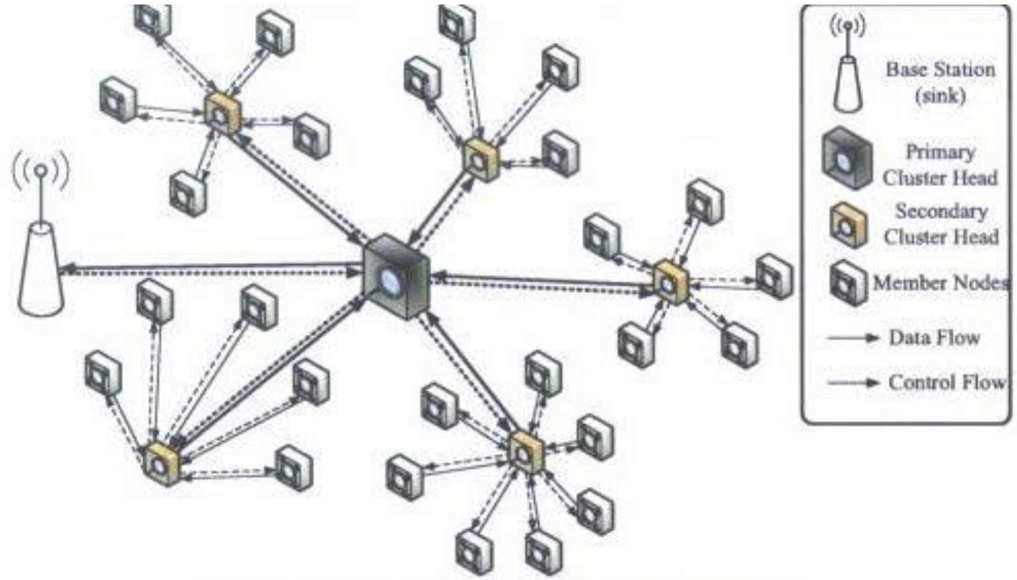


Figure 5. The Architecture of ITIDS.

Table 4. The Routing Table of SCH

N_{id}	G_{id}	N_{INFO}	$E_{fi}(\mu J)$
S406_1	1	$INFO_1$	$7.2*10^6$
S128_2	2	$INFO_1$	$7*10^6$
S564_9	3	$INFO_3$	$7.1*10^6$
S710_7	2	$INFO_2$	$6.5*10^6$
S392_5	5	$INFO_5$	$6.8*10^6$

ITIDS Sensor Roles

- BS - used by administrator to control WSN; receives sensing data and isolation tables.
- PCH – gathers sensing data and isolation table from SCH to BS.
- SCHs – calculate trust value to find malicious MNs and monitors PCH with MNs in its MG.
- MNs – send sensed data to SCH and rotate monitoring PCH.

ITIDS Four Stages

1. System Predefinition of IDS
2. SCHs monitors MNs.
3. SCH and MNs monitor PCH.
4. IDS backups the isolation table in BS.

Predefinition Stage

- Set up and define all the roles.
  - Set sensing types and number of MGs.
  - PCH randomly selects a sensor node in each MG to be SCH.

  * Authors discuss duty-cycle between PCH and SCH {unclear!}.
- Anomaly thresholds set per *MG* {set to 2/3 of N_k}.

Predefinition Stage

- MNs report info (including remaining energy) to SCHs.
- SCHs authenticate info from their Mns and isolate anomalies.
- Anomalies recorded in the SCH isolation table.
- SCH isolation tables integrated by PCH.

Stage 2 -SCHs Monitors MNs

- SCHs authenticate info from MNs.
- Anomalies recorded in the SCH isolation table (transmitted immediately to PCH).
- Possible MN anomalies:
  - Routing info changed by intruder.
  - Record attack behaviors (spoofed, altered, replayed routing info or selective forwarding) in isolation table.

Stage 2 -SCHs Monitors MNs

- Possible MN anomalies (cont.):
  - Remaining energy has increased instead of decreasing (implies sinkhole attack).
- Defense against doom attacks:
  - Measure frequency of MN traffic to SCH during time slot. If too frequent, MN is isolated by SCH.
  - Routing tables record energy information, if energy has increased SCH isolates the MN.

Stage 3 - SCH and MNs monitor PCH

- When enough MNs raise alarm total above threshold, SCH deposes PCH.
- New PCH integrates isolation table from each SCH and sends BS latest isolation table.
- PCH selects new SCHs – one from each MG randomly.
- Duty cycle of PCH divided into SCH duty cycles equally.

Table 5 - Isolation Table

- **Sample attack behaviors:**
  - **Fault information:: deliver info is a fault type from routing table.**
  - **Detection error:: MN raises detection alarm when no attack occurs.**
  - **Redundancy:: the same MN repeatedly sends data to SCH.**
  - **Wrong source:: the data source of the transmission is wrong.**

Outline

- Introduction
- Intrusion Detection Systems (IDS) for Wireless Sensor Networks
- Collaborated-Based Intrusion Detection
- Routing Table Intrusion Detection
- Isolated Table Intrusion Detection System
- *Comparison Experiments*
- Conclusions/Criticisms

Comparison Experiments

- Use NS-2 to compare ITIDS against CID and RTID.
- Only comparisons are Number of Alive Nodes for ITIDS and CID and Transmission Accuracy between ITIDS and RTID.
- Not enough detail to understand details of wireless energy usage.
- No discussion of MAC protocol simulated (assume 802.11).

Comparison Experiments

- No indication of radio (byte or packet)
  - 100 or 200 sensors in 10,000 sq. meters.
  - PCH in center, BS ??
  - 50 meter transmit radius
  - Energy formula: ONLY transmission + detection energy (calculation).
- No mention of routing or multi-hop.
- ONLY simulated doom attacks.

Comparison Experiments

- Remained resources formula used to determine number of alive nodes.
- Again, CHs NOT rotated to balance energy among MNs.

Figure 6 Number of Alive Nodes

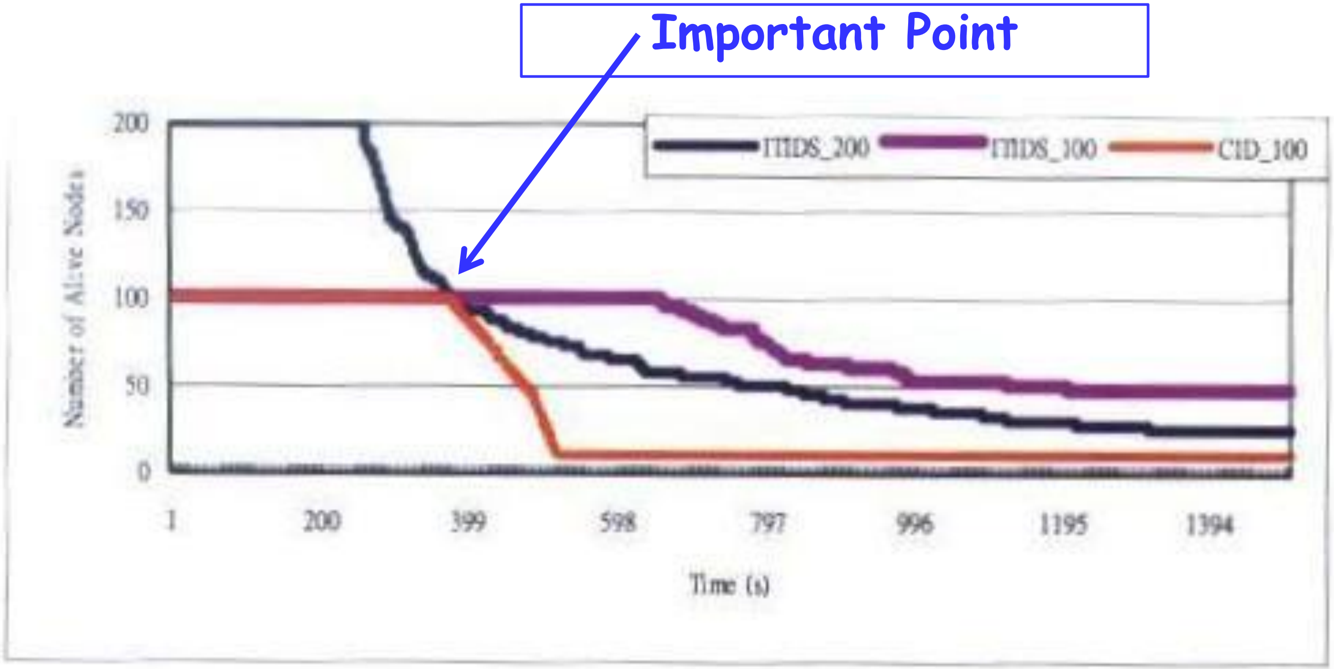


Figure 6. The Comparison of the Number of Alive Nodes Between ITIDS and CID.

Figure 7 Transmission Accuracy

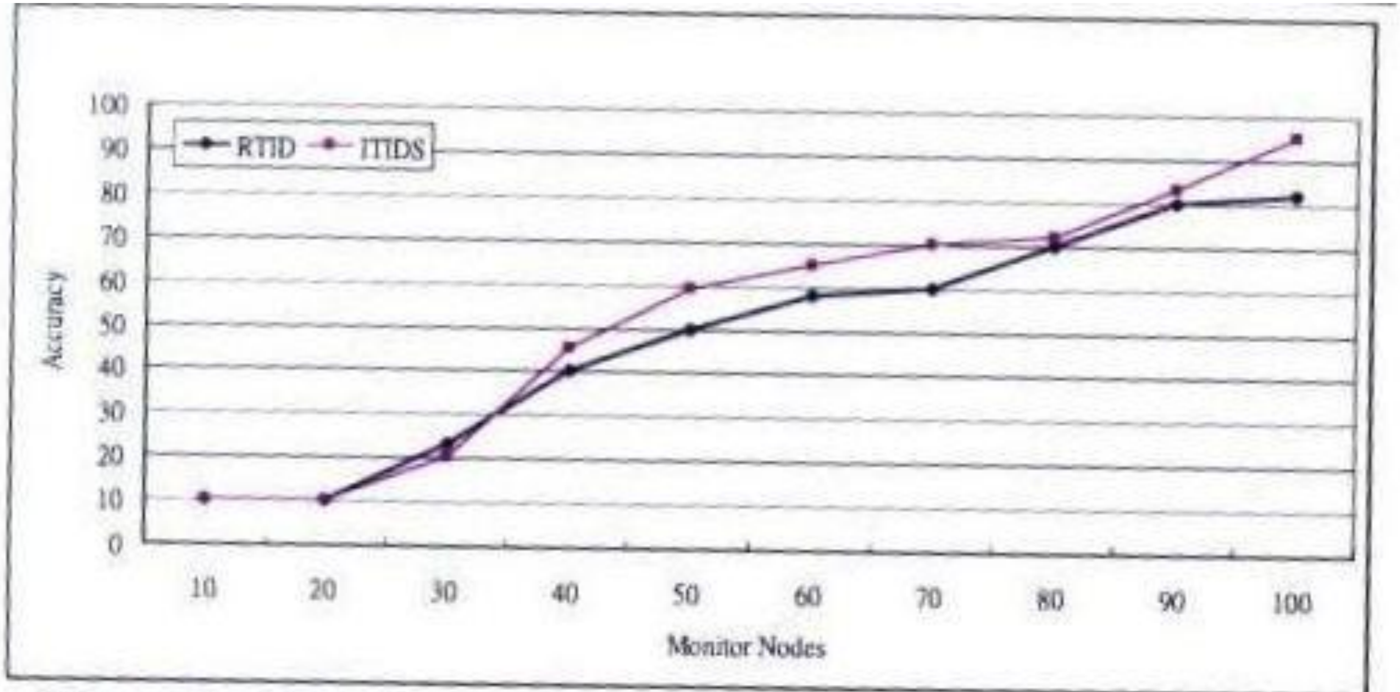


Figure 7. The Comparison of the Transmission Accuracy Between ITIDS and RTID.

Conclusions/Criticisms

- Authors conclude that evidence shows ITIDS can prevent attacks effectively.
  - No info on number of attacks attempted and number prevented.
- Generally, experiments are few weak with too few details to assess or to reproduce.
- Difficult to see cause-and-effect from two graphs presented.

A New Method for Intrusion Detection on Hierarchical Wireless Sensor Networks

Questions ??

Thank You!