Security Issues in Wireless Sensor Networks

Yenumula B Reddy

Grambling State University
Grambling, LA 71245

Security Issues in Wireless Sensor Networks

The tutorial includes 3 parts.

Part 1	Basics Terminology, topology, security threats and applications
Part 2	Threats and Counter measures
Part 3	Research directions

Part 1

Introduction

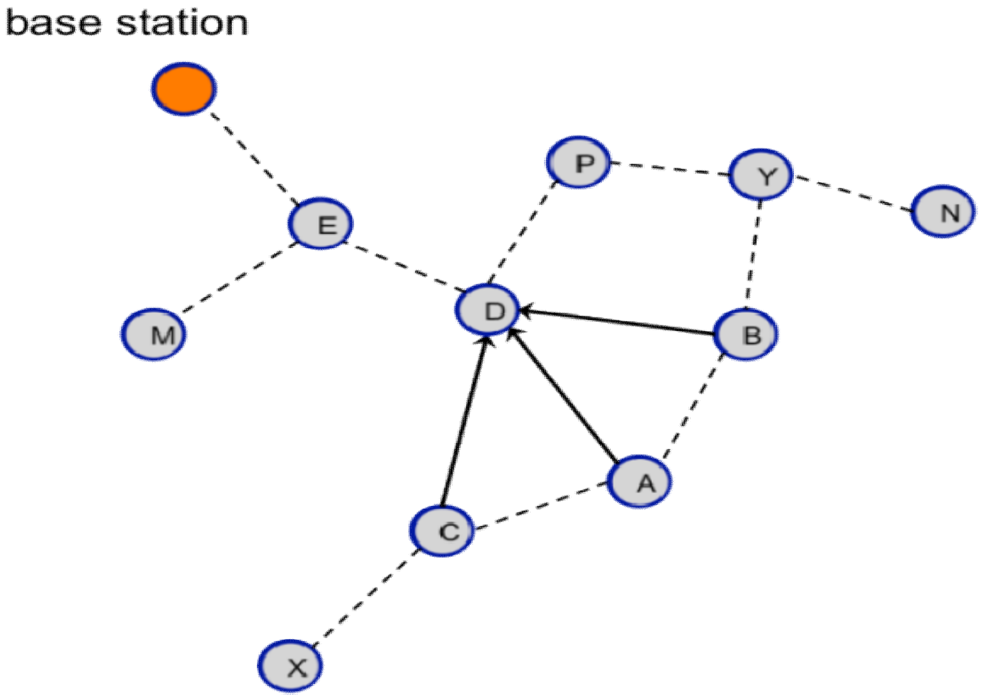
Terminology, topology, security threats and applications

Part 1 Contents

- Overview of Wireless Sensor Networks
    - What is Wireless Sensor Network
    - What are the Characteristics of WSN
    - Standards and specifications
    - Factors influencing sensor network design
    - Measurements for Wireless Sensor Networks
- Topology
- Applications
- Protocols and Routing
- Threats
- Future and Challenges
- Conclusions

What is Wireless Sensor Network

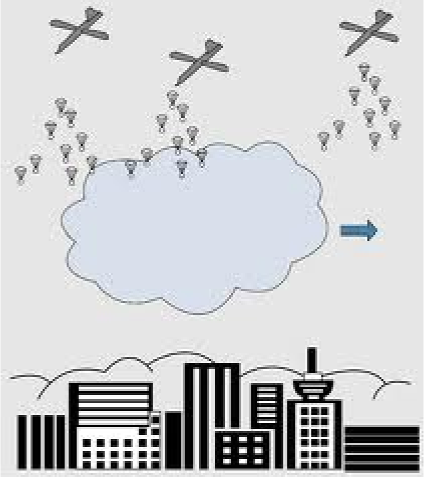
Wireless Sensor Network consists of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants and to cooperatively pass their data through the network to a main location.



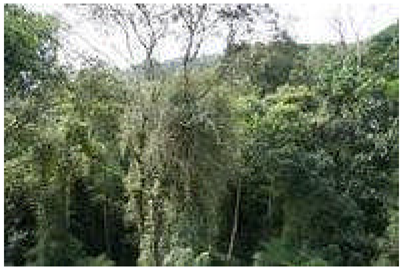
WSN Examples

Monitors Environmental conditions

Energy Efficient Non-Local Phenomenon Awareness



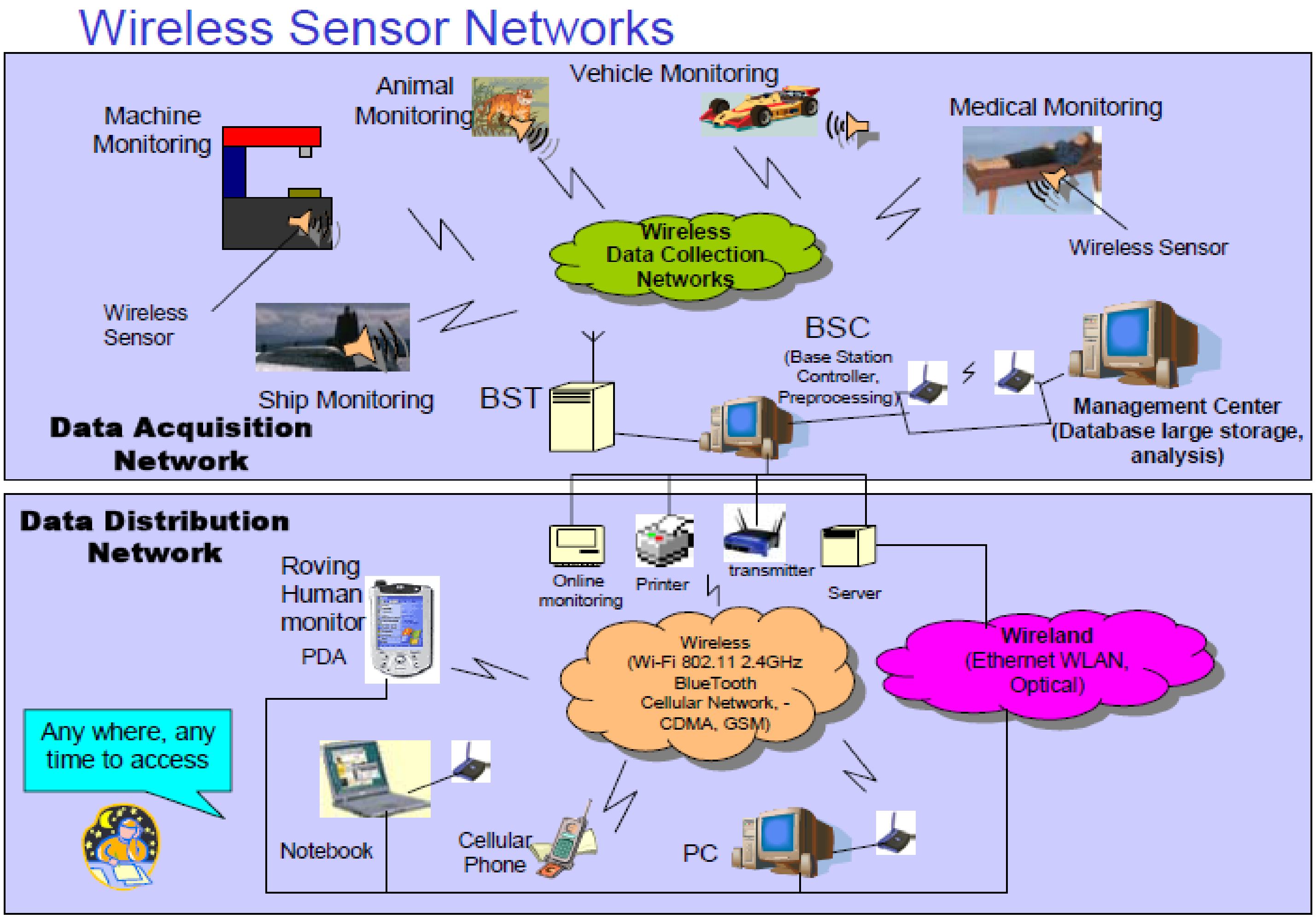
Rainforest Micrometeorology Sensor



Social Sensor Network

WSN Examples

Example Diagram


Wireless Sensor Networks
Machine Monitoring
Animal Monitoring
Vehicle Monitoring
Medical Monitoring
Wireless Data Collection Networks
Wireless Sensor
Wireless Sensor
Ship Monitoring
BST
BSC
(Base Station Controller, Preprocessing)
Management Center (Database large storage, analysis)
Data Acquisition Network
Data Distribution Network
Roving Human monitor
PDA
Online monitoring
Printer
transmitter
Server
Wireless (Wi-Fi 802.11 2.4GHz BlueTooth Cellular Network, - CDMA, GSM)
Wireland (Ethernet WLAN, Optical)
Any where, any time to access
Notebook
Cellular Phone
PC

Parts of Sensor Node

- a radio transceiver with an internal antenna or connection to an external antenna,
- a microcontroller (sometimes abbreviated **µC**, **uC** or **MCU**) is a small computer on a single integrated circuit containing a processor core, memory, and programmable input/output peripherals.
- an electronic circuit for interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting

Characteristics of WSN

The main characteristics of a WSN include

- Power consumption constrains for nodes using batteries or energy harvesting
- Ability to cope with node failures
- Mobility of nodes
- Dynamic network topology
- Communication failures
- Heterogeneity of nodes
- Scalability to large scale of deployment
- Ability to withstand harsh environmental conditions
- Ease of use
- Unattended operation.

Standards and specifications

Predominant standards commonly used in WSN communications include:

- WirelessHART (**The wireless standard for process automation)**
- ISA100 **(WirelessHART and ISA100.11a convered in a recent Control Engineering article, News and comment: Please see in WirelessHART and ISA100 converge?)**
- IEEE 1451 (**IEEE 1451** is a set of Smart transducer interface standards developed by the IEEE Instrumentation and Measurement Society's Sensor Technology Technical Committee that describe a set of open, common, network-independent communication interfaces for connecting transducers (sensors or actuators) to microprocessors, instrumentation systems, and control/field networks.)
- ZigBee / 802.15.4 (IEEE 802.15.4/ZigBee is intended as a specification for low-powered networks for such uses as wireless monitoring and control of lights, security alarms, motion sensors, thermostats and smoke detectors.)
- IEEE 802.11 (IEEE 802.11p-2010 IEEE Standard for Information technology--Telecommunications and information exchange between systems--Local and metropolitan area networks--Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Wireless Access in Vehicular Environments)

The IEEE focuses on the physical and MAC layers;

The Internet Engineering Task Force works on layers 3 and above; In addition to these, bodies such as the International Society of Automation provide vertical solutions, covering all protocol layers.

Challenges and specifications

- Hardware
  - To produce low cost and tiny sensor node
  - Low power method for data acquisition
- Software

Sensors are meant to be deployed in large numbers in various environments, including remote and hostile regions, with ad-hoc communications as key. For this reason, algorithms and protocols need to address the following issues:

- Lifetime maximization
- Robustness and fault tolerance
- Self-configuration

Challenges and specifications

Some of the important topics in WSN software research are:

- Operating systems
- Security Issues
- Mobility
- Usability – human interface for deployment and management, debugging and end-user control
- Middleware – the design of middle-level primitives between high level software and the systems

WSN Operating Systems

WSNs are less complex, particularly deployed specific application, have low-power microcontrollers, and virtual memory is expensive to implement.

It is therefore possible to use embedded operating systems such as eCos or uC/OS for sensor networks. However, such operating systems are often designed with real-time properties.

- TinyOS is perhaps the first operating system specifically designed for wireless sensor networks. TinyOS is based on an event-driven programming model instead of multithreading. TinyOS programs are composed into *event handlers* and *tasks* with run to completion-semantics. When an external event occurs, such as an incoming data packet or a sensor reading, TinyOS signals the appropriate event handler to handle the event. Event handlers can post tasks that are scheduled by the TinyOS kernel some time later.
- LiteOS is a newly developed OS for wireless sensor networks, which provides UNIX like abstraction and support for C programming language. Contiki is an OS which uses a simpler programming style in C while providing advances such as 6LoWPAN and proto-threads.

WSN Security Issues

Important security issues include

- key establishment
- secrecy
- authentication
- privacy
- denial-of-service attacks → More info in a later set of slides
- secure routing → More info in a later set of slides
- node capture

The above security models are expensive;

We need special security models in WSN;

Developing low: (a)power, (b) processing, and fast models is an open problem

WSN Mobility

Mobility of sinks, mobility of sensors and actuators as well as mobility of code (i.e. applications) opens a new research topic.

Mobility models include:

- Sink mobility
- Code mobility
- Mobile agent-based data aggregation
- Localization techniques
- Mobility issues in underwater Wireless Sensor Networks
- Connectivity maintenance in Wireless Sensor Networks with mobile elements
- Mobility for maximizing network lifetime in Wireless Sensor Networks
- Mobility models for sinks and actuators in Wireless Sensor Networks
- Routing protocols for handling mobility
- Distributed algorithms and reasoning in Wireless Sensor Networks with mobile elements
- Data fusion techniques in Wireless Sensor Networks with mobile elements - Mobile GeoSensor Networks

WSN Usability

Human interface for

- deployment and management,
- debugging and end-user control

WSN Middleware

The design of middle-level primitives between high level software and the systems

WSN - Factors influencing sensor network design

Fault Tolerance

- Fault tolerance is the ability to sustain sensor network functionalities without any interruption due to sensor node failure
- The fault tolerance level depends on the application of the sensor network

Scalability - Scalability measures the density of the sensor nodes

Hardware Constrains

- The cost of single node to justify overall cost, hardware, and limitations

Sensor Network Topology

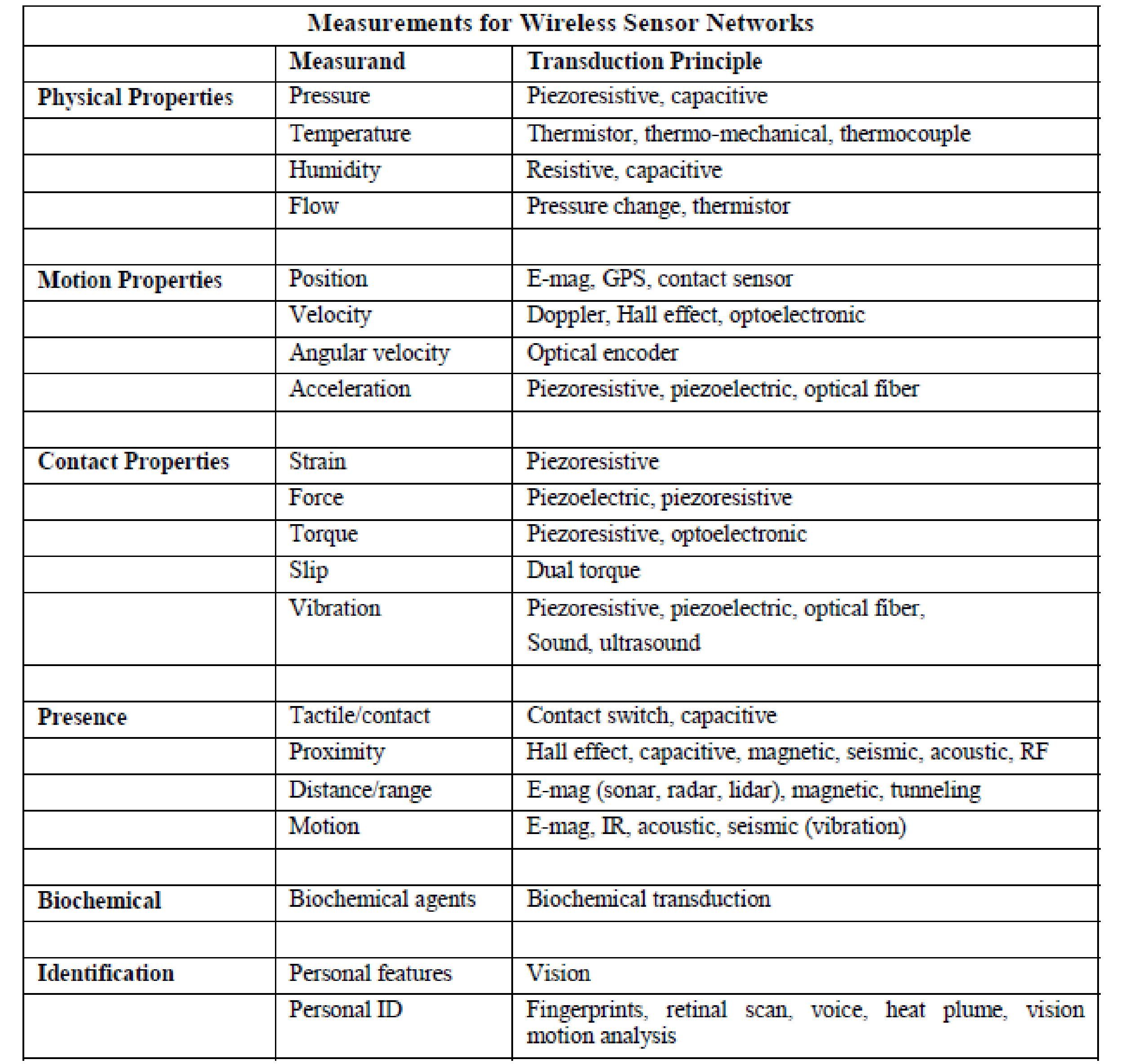
- Deployment: Pre, current, post, and redeployment phases

Environment - Busy intersections, interior of large machinery, bottom of an ocean, surface of an ocean during a tornado, biologically or chemically contaminated field, battlefield beyond the enemy lines, home or large building, large warehouse, animals, fast moving vehicles, drain or river (moving with current)

Transmission Media – Radio, infrared, optical media (in a multihop sensor network, communicating nodes are linked by a wireless medium to enable global operation)

Power Consumption – sensing, communication, data processing

WSN Measurements



Measurements for Wireless Sensor Networks		
	Measurand	**Transduction Principle**
Physical Properties	Pressure	Piezoresistive, capacitive
	Temperature	Thermistor, thermo-mechanical, thermocouple
	Humidity	Resistive, capacitive
	Flow	Pressure change, thermistor
Motion Properties	Position	E-mag, GPS, contact sensor
	Velocity	Doppler, Hall effect, optoelectronic
	Angular velocity	Optical encoder
	Acceleration	Piezoresistive, piezoelectric, optical fiber
Contact Properties	Strain	Piezoresistive
	Force	Piezoelectric, piezoresistive
	Torque	Piezoresistive, optoelectronic
	Slip	Dual torque
	Vibration	Piezoresistive, piezoelectric, optical fiber, Sound, ultrasound
Presence	Tactile/contact	Contact switch, capacitive
	Proximity	Hall effect, capacitive, magnetic, seismic, acoustic, RF
	Distance/range	E-mag (sonar, radar, lidar), magnetic, tunneling
	Motion	E-mag, IR, acoustic, seismic (vibration)
Biochemical	Biochemical agents	Biochemical transduction
Identification	Personal features	Vision
	Personal ID	Fingerprints, retinal scan, voice, heat plume, vision motion analysis

WSN Other Concepts

Distributed sensor network

Reliability increases using distributed property with the following reasons.

- Sensor nodes are prone to failure,
- For better collection of data
- To provide nodes with backup in case of failure of the central node

It is important to take care of nodes sensing redundant information and forwarding the data that is of no use. There is also no centralized body to allocate the resources and they have to be self organized.

Data visualization

The data gathered from wireless sensor networks is usually saved in the form of numerical data in a central base station. Additionally, the Open Geospatial Consortium (OGC) is specifying standards for interoperability interfaces and metadata encodings that enable real time integration of heterogeneous sensor webs into the Internet, allowing any individual to monitor or control Wireless Sensor Networks through a Web Browser.

WSN Other Concepts

Information fusion

- In wireless sensor networks, information fusion, also called data fusion, has been developed for processing sensor data by filtering, aggregating, and making inferences about the gathered data. Information fusion deals with the combination of multiple sources to obtain improved information: cheaper, greater quality or greater relevance. Within the wireless sensor networks domain, simple aggregation techniques such as maximum, minimum, and average, have been developed for reducing the overall data traffic to save energy

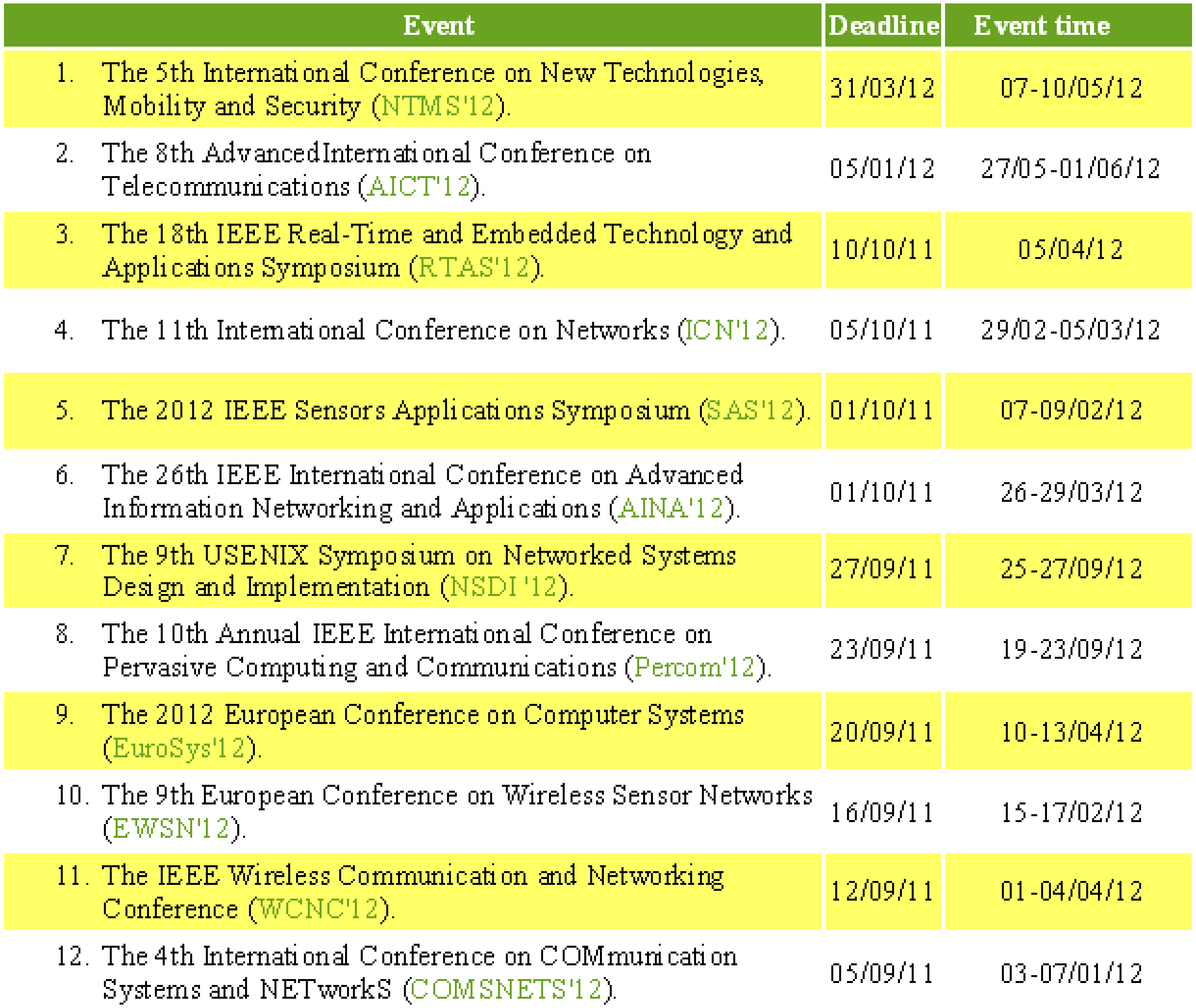
Factors influencing WSN design

- **Fault tolerance:** ability to sustain sensor network functionalities - without any interruption due to sensor node failures;
- **WSN topology** and topology maintenance, a challenging task;
- **Successful operation of WSN** - relying on reliable communication between nodes in a network;
- **Complementary metal oxi**de semiconductor (CMOS) technology - and cost and size limitations;
- **Energy-efficient communication protocols**;
- **Energy consumption for communication** - factors such as hardware profile, packet size, transmit power level and distance

WSN Conferences
http://www.wsn-security.info/CFP.htm

You will find 187 conferences; some of them are:

- Symposium on Networking and wireless Communications in connection with ITNG 2012
- SENSORCOMM 2011 (IARIA)



Event	Deadline	Event time
1. The 5th International Conference on New Technologies, Mobility and Security (NTMS'12).	31/03/12	07-10/05/12
2. The 8th AdvancedInternational Conference on Telecommunications (AICT'12).	05/01/12	27/05-01/06/12
3. The 18th IEEE Real-Time and Embedded Technology and Applications Symposium (RTAS'12).	10/10/11	05/04/12
4. The 11th International Conference on Networks (ICN'12).	05/10/11	29/02-05/03/12
5. The 2012 IEEE Sensors Applications Symposium (SAS'12).	01/10/11	07-09/02/12
6. The 26th IEEE International Conference on Advanced Information Networking and Applications (AINA'12).	01/10/11	26-29/03/12
7. The 9th USENIX Symposium on Networked Systems Design and Implementation (NSDI '12).	27/09/11	25-27/09/12
8. The 10th Annual IEEE International Conference on Pervasive Computing and Communications (Percom'12).	23/09/11	19-23/09/12
9. The 2012 European Conference on Computer Systems (EuroSys'12).	20/09/11	10-13/04/12
10. The 9th European Conference on Wireless Sensor Networks (EWSN'12).	16/09/11	15-17/02/12
11. The IEEE Wireless Communication and Networking Conference (WCNC'12).	12/09/11	01-04/04/12
12. The 4th International Conference on COMmunication Systems and NETworkS (COMSNETS'12).	05/09/11	03-07/01/12

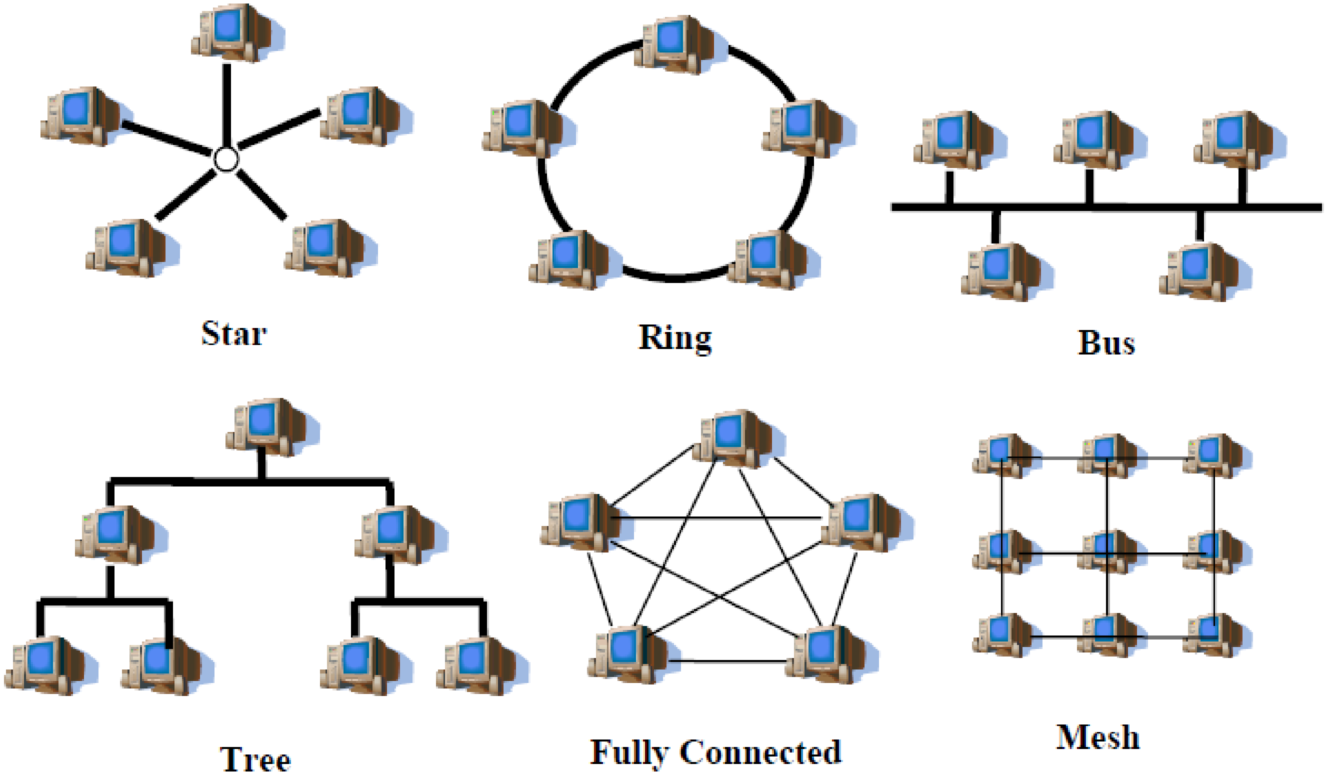
Topology

WSN Topology

Topology

The WSN topologies are shown in the figure and include:

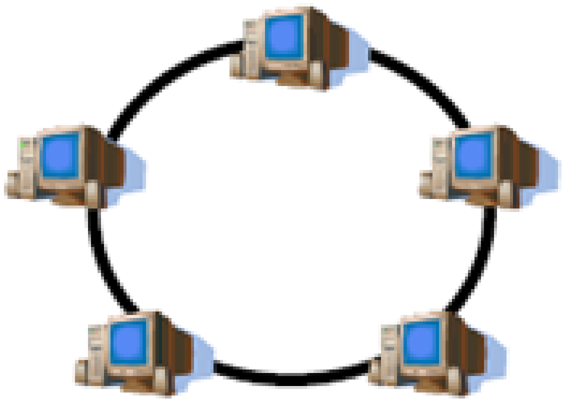
- fully connected
- Mesh
- Star
- ring
- tree
- bus.



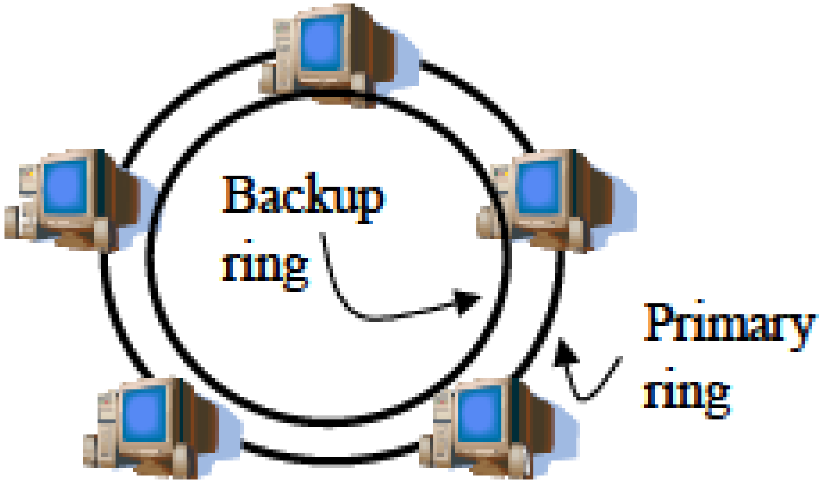
A single network may consist of several interconnected subnets of different topologies.

Topology - Ring

In the ring topology all nodes perform the same function and there is no leader node. Messages generally travel around the ring in a single direction. However, if the ring is cut, all communications are lost. The self-healing ring network (SHR) shown below that has two rings and is more fault tolerant.



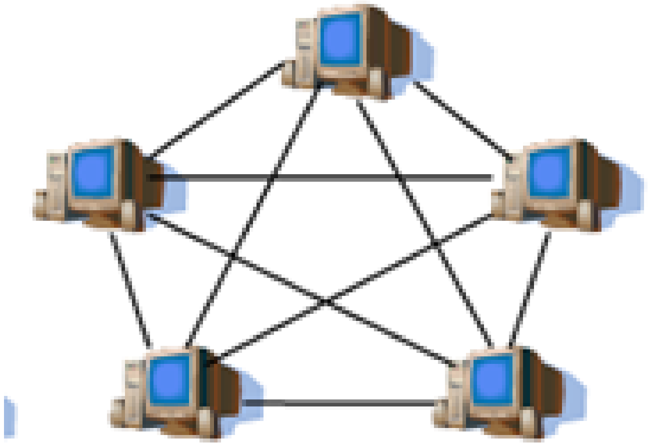
Ring



Self-Healing Ring

Topology – Fully Connected

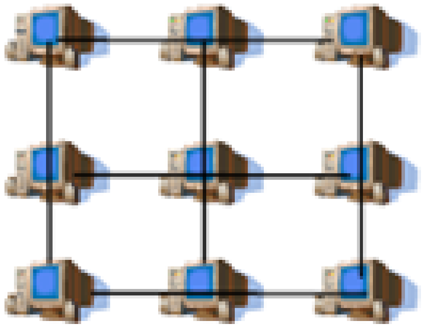
Fully connected networks suffer from problems of NP-complexity; as additional nodes are added, the number of links increases exponentially. Therefore, for large networks, the routing problem is computationally intractable even with the availability of large amounts of computing power



Fully Connected

Topology - Mesh

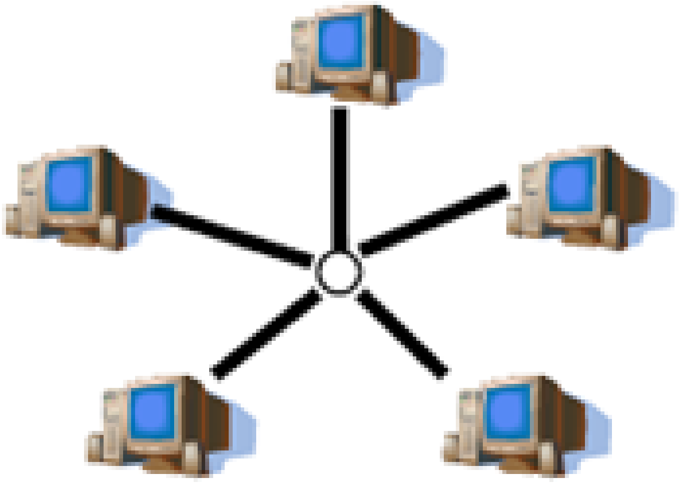
Mesh networks are regularly distributed networks that generally allow transmission only to a node’s nearest neighbors. The nodes in these networks are generally identical, so that mesh nets are also referred to as peer-to-peer (see below) nets. Mesh nets can be good models for large-scale networks of wireless sensors that are distributed over a geographic region, e.g. personnel or vehicle security surveillance systems. Note that the regular structure reflects the communications topology; the actual geographic distribution of the nodes need not be a regular mesh. Since there are generally multiple routing paths between nodes, these nets are robust to failure of individual nodes or links. An advantage of mesh nets is that, although all nodes may be identical and have the same computing and transmission capabilities, certain nodes can be designated as ‘group leaders’ that take on additional functions. If a group leader is disabled, another node can then take over these duties.



Mesh

Topology - Star

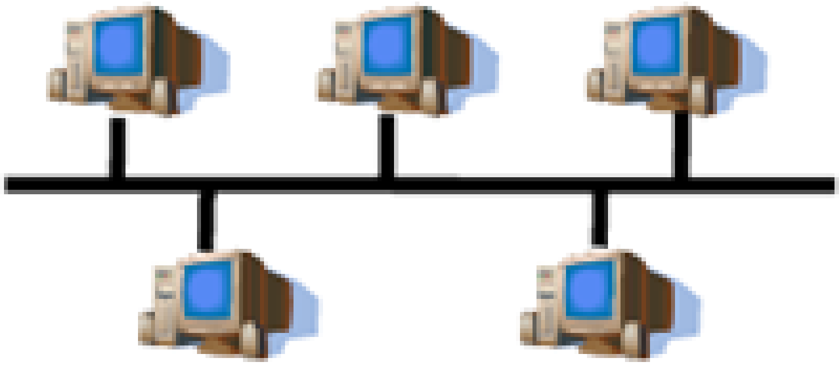
In Star topology all nodes are connected to a single hub node. The hub requires greater message handling, routing, and decision-making capabilities than the other nodes. If a communication link is cut, it only affects one node. However, if the hub is incapacitated the network is destroyed.



Star

Topology - Bus

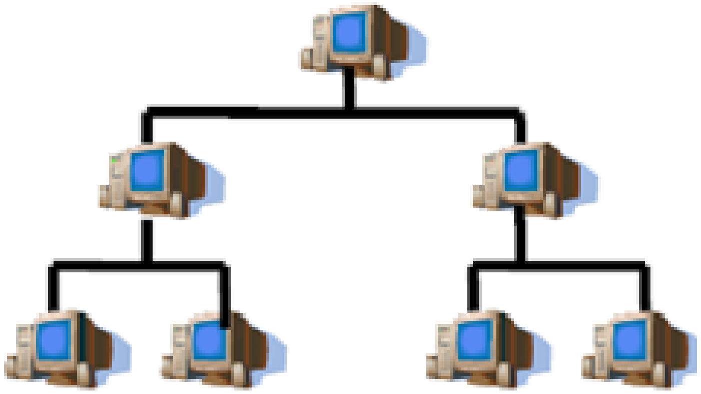
In the bus topology, messages are broadcast on the bus to all nodes. Each node checks the destination address in the message header, and processes the messages addressed to it. The bus topology is passive in that each node simply listens for messages and is not responsible for retransmitting any messages.



Bus

Topology - Tree

In tree network, if a node is disconnected only the descendents are disconnected.



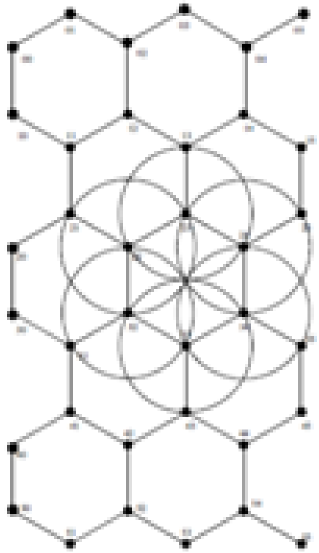
Tree

Note: Any network can be designed as a hybrid network

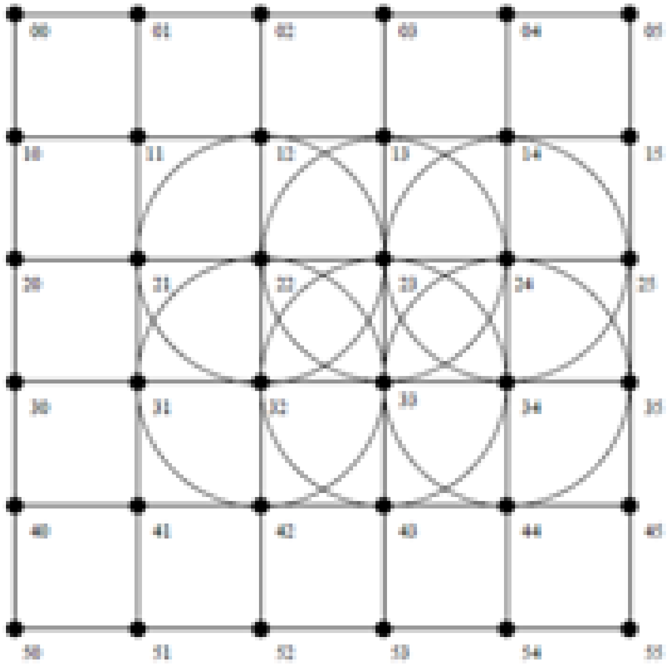
Topology - Other

Example -1: Topology up to

3 neighbors



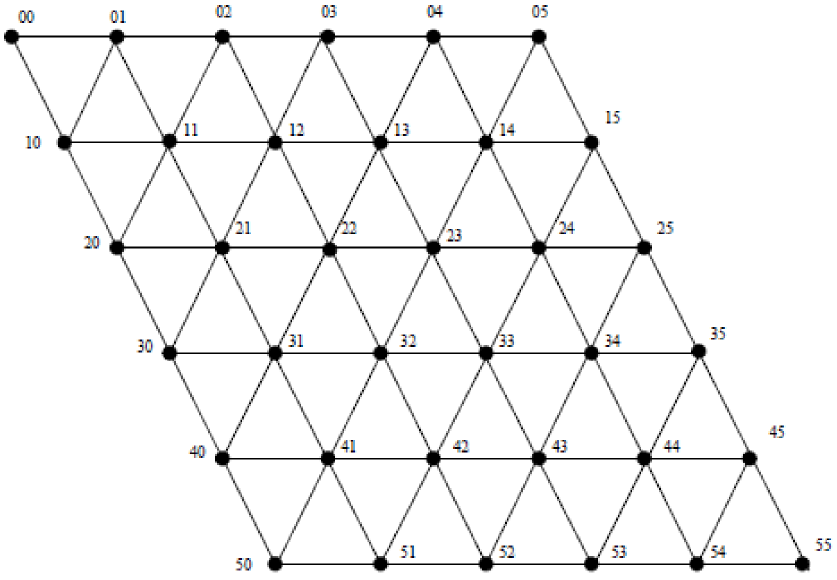
4 neighbors



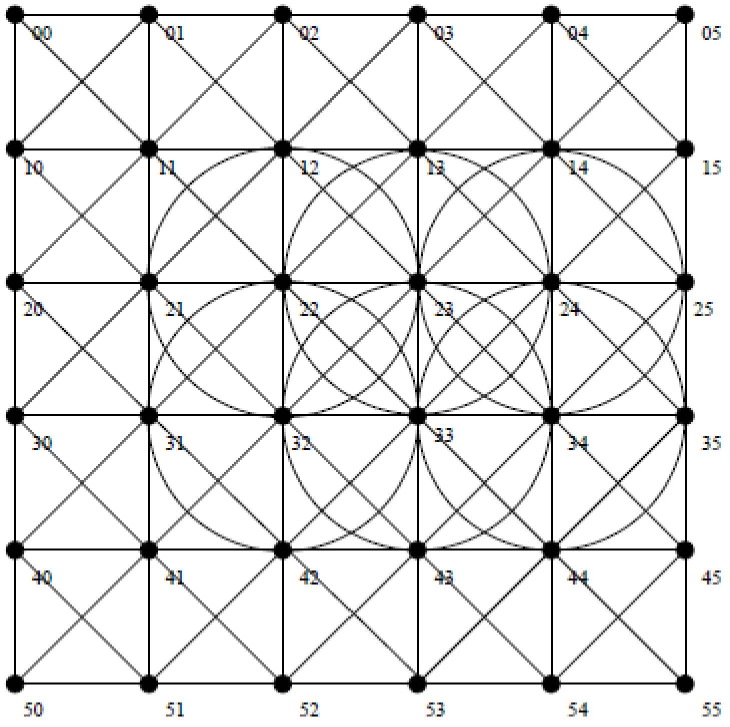
Topology – Example 2

Example -2: Topology up to

6 neighbors



8 neighbors



Wireless Sensor Networks

Applications

Wireless Sensor Networks

Applications are divided into following categories:

- **Military Applications**
- **Environmental Applications**
- **Health applications**
- **Home and other commercial applications**

Military Applications

- ➢ Monitoring friendly forces, equipment, and ammunition
- ➢ Reconnaissance of opposing and terrain
- ➢ Battle Field surveillance and Battle damage assessment
- ➢ Nuclear, Biological and chemical attack detection

Environmental Applications

- ➢ Forest fire detection
- ➢ Bio-complexity mapping of the environment
- ➢ Flood detection
- ➢ Precision agriculture

Wireless Sensor Networks

- **Health applications**
  - Tele-monitoring of human physiological data
  - Tracking and monitoring patients and doctors inside a hospital
  - Drug administration in hospitals

- **Home and other commercial applications**
  - Home Automation and smart environment
  - Interactive museums
  - Managing Inventory control
  - Vehicle tracking and detection
  - Detecting and Monitoring car thefts

WSN Applications
Explanation of some applications

Area monitoring: WSN is deployed over a region where some phenomenon is to be monitored. A military example is the use of sensors to detect enemy intrusion; a civilian example is the geo-fencing of gas or oil pipelines.

Air pollution monitoring: WSNs have been deployed in several cities (Stockholm, London or Brisbane) to monitor the concentration of dangerous gases for citizens.

Forest fires detection: A network of Sensor Nodes can be installed in a forest to control when a fire has started. The sensor nodes will be equipped with sensors to control temperature, humidity and gases which are produced by fire in the trees or vegetation. The early detection is crucial for a successful action of the firefighters; thanks to Wireless Sensor Networks, the fire brigade will be able to know when a fire is started and how it is spreading.

WSN Applications

Greenhouse monitoring: WSNs are used to control the temperature and humidity levels inside commercial greenhouses. When the temperature and humidity drops below specific levels, the greenhouse manager must be notified via e-mail or cell phone text message, or host systems can trigger misting systems, open vents, turn on fans, or control a wide variety of system responses.

Landslide detection: A landslide detection system makes use of a WSN to detect the slight movements of soil and changes in various parameters that may occur before or during a landslide and is possible to know the occurrence of landslides long before it actually happens.

Industrial monitoring: WSNs have been developed for machinery condition-based maintenance (CBM) as they offer significant cost savings and enable new functionalities. In wired systems, the installation of enough sensors is often limited by the cost of wiring. Previously inaccessible locations, rotating machinery, hazardous or restricted areas, and mobile assets can now be reached with wireless sensors.

WSN Applications

Water/wastewater monitoring: Facilities not wired for power or data transmission can be monitored using industrial wireless I/O devices and sensors powered using solar panels or battery packs.

Agriculture: WSN frees the farmer from the maintenance of wiring in a difficult environment. Gravity feed water systems can be monitored using pressure transmitters to monitor water tank levels, pumps can be controlled using wireless I/O devices and water use can be measured and wirelessly transmitted back to a central control center for billing. Irrigation automation enables more efficient water use and reduces waste.

Structural monitoring: Wireless sensors can be used to monitor the movement within buildings and infrastructure such as bridges, flyovers, embankments, tunnels etc... enabling Engineering practices to monitor assets remotely without the need for costly site visits, as well as having the advantage of daily data, whereas traditionally this data was collected weekly or monthly, using physical site visits, involving either road or rail closure in some cases.

Volcano monitoring: The low cost, size, and power requirements of wireless sensor networks have a tremendous advantage over existing instrumentation used in volcanic field studies. This technology will permit sensor arrays with greater spatial resolution and larger apertures than existing wired monitoring stations.

WSN Some Interesting Applications

iButton: is a computer chip enclosed in a 16mm thick stainless steel can. Provides up-to-date information can travel with a person or object anywhere they go. The steel iButton can be mounted virtually anywhere because it is rugged enough to withstand harsh environments, indoors or outdoors. It is small and portable enough to attach to a key fob, ring, watch, or other personal items, and be used daily for applications such as access control to buildings and computers, asset management, and various data logging tasks

How Durable Is the iButton?

The silicon chip within the iButton is protected by the ultimate durable material: stainless steel. You can drop an iButton, step on it, or scratch it. The iButton is wear-tested for 10-year durability

Each **iButton** is identified by **a unique address**.

Since it travels with the object, detection of lost object is easy.

Applications: Access Control, Asset management, eCash, Gaming systems, Guard tour, Thermochron application (tracking food quality), Time & attendance (track of employees)

WSN Some Interesting Applications

Proximity sensor - detect the presence of nearby objects without any physical contact.

A proximity sensor often emits an electromagnetic or electrostatic field, or a beam of electromagnetic radiation (infrared, for instance), and looks for changes in the field or return signal. The object being sensed is often referred to as the proximity sensor's target. Different proximity sensor targets demand different sensors.

Applications

- Parktronic, car bumpers that sense distance to nearby cars for parking
- Ground proximity warning system for aviation safety
- Vibration measurements of rotating shafts in machinery [1]
- Top dead centre (TDC)/camshaft sensor in reciprocating engines.
- Sheet break sensing in paper machine.
- Anti-aircraft warfare
- Mobile phones
- Roller Coasters
- Conveyor systems

Manufacturers

- AutomationDirect
- c3controls
- Pepperl+Fuchs
- Turck
- Rockwell Automation

WSN Some Interesting Applications

Other applications – Refer Internet (Google)

proximity sensor applications Explained

pressure sensor applications

biosensor applications

sensor **jobs**

ultrasonic sensor applications

hall effect sensor applications

dependent resistors for sensor applications

Wireless Sensor Networks

Protocols

WSN Protocols

Protocols are the communications standards and the set of rules that source and destination computers must abide by and follow in order to communicate with each other. They determine that how data will be transmitted between two computer compute.

They also define the data packet size, authentication, signaling, data compression, error checking and retransmission of the packets. They also define that how the packet information will be organized while traveling over the network.

There are several types of the communication protocols and the most common network protocols are TCP/IP, POP, SMTP, SLIP, LDAP, FTP, SNMP, HTTP, PPP, PPTP, UDP, RIP, OSPF, RIP, DHCP, NNTP, ICMP and BOOTP.

Protocols are sometimes grouped into the lower level, upper level and the application protocols. On the internet and the LAN/WAN communication networks, TCP/IP is the most common protocol.

WSN Protocols

TCP/IP stands for **Transmission Control Protocol and the Internet Protocol**. TCP/IP in fact is a suite of protocols that consists of more than 65,000 protocols. Each of the protocols in the TCP/IP stack performs different functionalities.

In the Ethernet based networks and the on the internet, the data is divided into the small packets to make the transmission process speedy and reduce the errors. These packets then reunite at the destination computer till all the packets are transmitted. In the OSI (**Open System Interconnectivity**) model, each protocol works at different layer of the OSI layers model.

WSN Protocols

Layer 1 (Physical Layer):	Sonet, ISDN, SDH
Layer 2 (Data Link Layer):	Frame Relay, FDDI, Ethernet
Layer 3 (Network Layer):	RIP, OSPF, EGP, IPX, IPV6, ARP
Layer 4 (Transport Layer):	TCP, UDP, SPX
Layer 5 (Session Layer):	NFS, NCP, SMB
Layer 6 (Presentation Layer):	
Layer 7 (Application Layer):	

BOOTP, DHCP, DNS, HTTP, POP3, SSH, Telnet

WSN Protocols

Classifications of the Protocols

Protocols are classified into the following major categories.

TCP/IP	IP, TCP, UDP, SMTP, POP3, RIP, FTP, DHCP
Cellular	GPRS, GSM, WAP and CDMA
VOIP	SIP, RTP, Megaco, MGCP and H.323
General	Frame Relay, ATM, X.25, PPP,

WSN Threats

WSN Threats

WSN Threats

Many sensor network routing protocols are Quite simple. Due to this reason attacks on routing in ad-hoc networks are susceptible. Most **network layer attacks** against sensor networks fall into one of the following categories:

- Spoofed, altered, or replayed routing Information
- Selective forwarding
- Sinkhole attacks
- Sybil attacks
- Wormholes
- HELLO flood attacks

WSN Threats

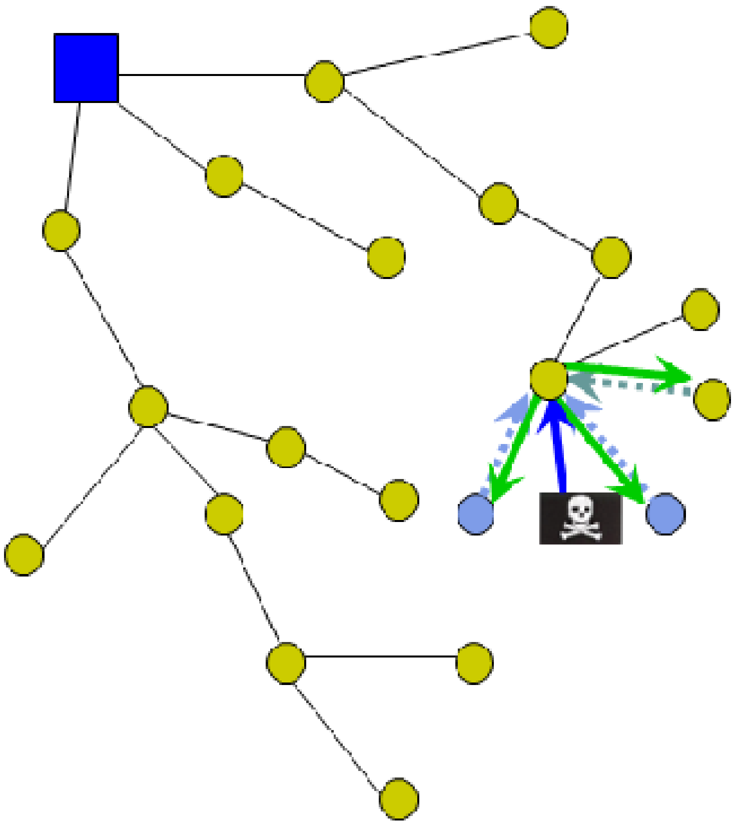
Spoofed, altered, or replayed routing Information

The most direct attack against a routing protocol is to target the routing information exchanged between nodes.

By spoofing, altering, or replaying routing information, adversaries may be able to create routing loops, attract or repel network traffic, extend or shorten source routes, generate false error messages, partition the network, increase end-to-end latency, etc.

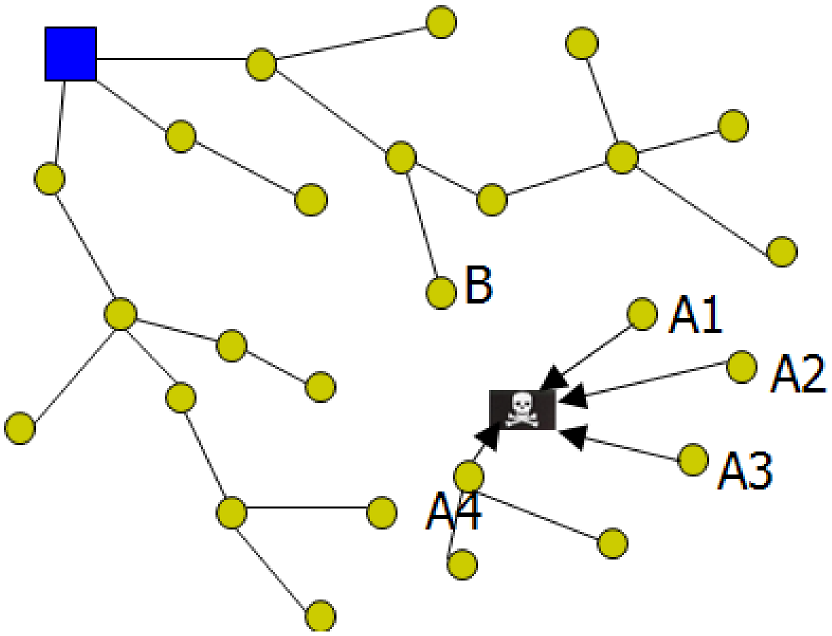
WSN Threats - Acknowledgment spoofing

- Some routing protocols use link layer acknowledgments
- Attacker may spoof acks
- Goals: convince that weak link is strong or that dead node is alive.
- Consequently weak link may be selected for routing; packets send trough that link may be lost or corrupted



WSN Threats – false routing

- Injecting fake routing control packets into the network, examples: attract / repeal traffic, generate false error messages
- Consequences: routing loops, increased latency, decreased lifetime of the network, low reliability



Example: captured node attracts traffic by advertising shortest path to sink, high battery power, etc

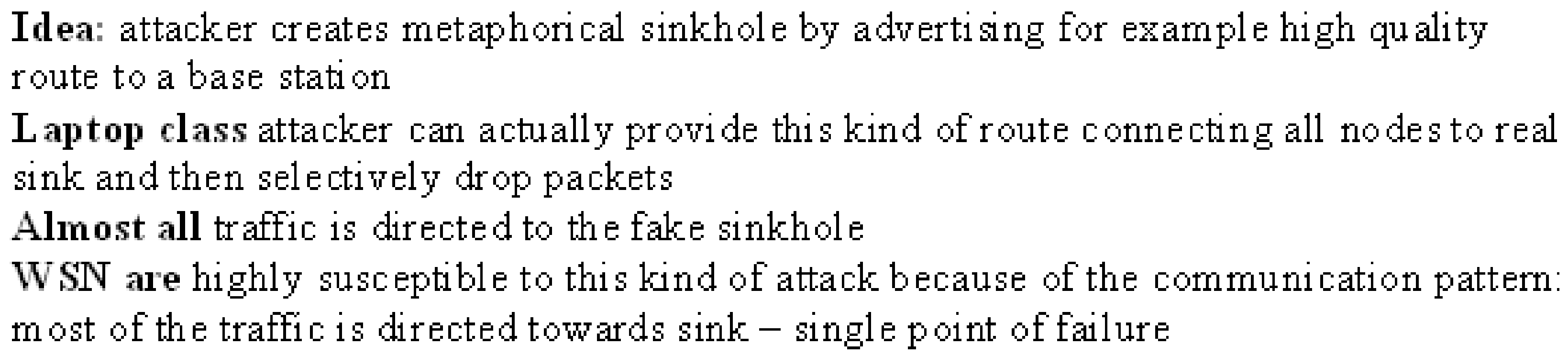
WSN Threats - Selective forwarding

In a selective forwarding attack, malicious nodes may refuse to forward certain messages and simply drop them, ensuring that they are not propagated any further.

- Multi hop paradigm is prevalent in WSN
- It is assumed that nodes faithfully forward received messages
- Compromised node might refuse to forward packets, however neighbors might start using another route
- More dangerous: compromised node forwards selected packets

A simple form of this attack is when a malicious node behaves like a black hole and refuses to forward every packet it sees. However, such an attacker runs the risk that neighboring nodes will conclude that the node has failed and decides to seek another route. A more subtle form of this attack is when an adversary selectively forwards packets. An adversary interested in suppressing or modifying packets originating from a select few nodes can reliably forward the remaining traffic and limit suspicion of her wrongdoing. Selective forwarding attacks are typically most effective when the attacker is explicitly included on the path of a data flow. However, it is conceivable an adversary overhearing a flow passing through neighboring nodes might be able to emulate selective forwarding by jamming or causing a collision on each forwarded packet of interest.

WSN Threats - Sinkhole attacks



Idea: attacker creates metaphorical sinkhole by advertising for example high quality route to a base station

Laptop class attacker can actually provide this kind of route connecting all nodes to real sink and then selectively drop packets

Almost all traffic is directed to the fake sinkhole

WSN are highly susceptible to this kind of attack because of the communication pattern: most of the traffic is directed towards sink – single point of failure

WSN Threats - Sybil attack

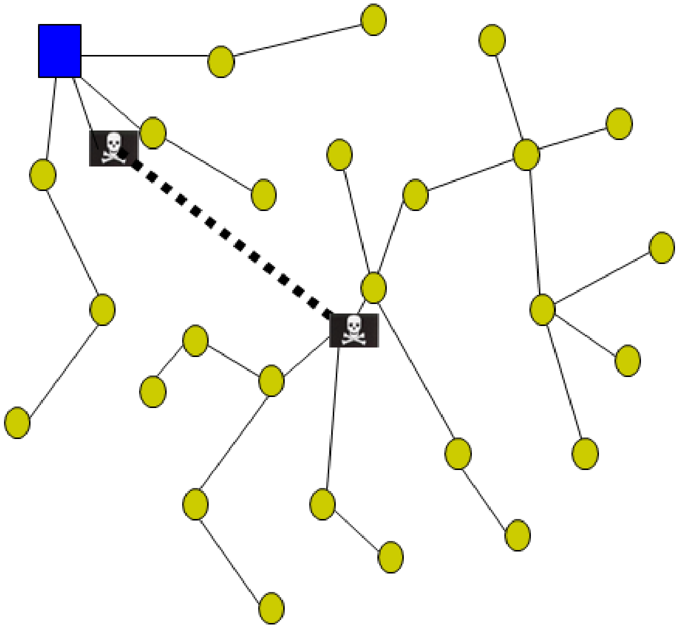
Idea: a single node pretends to be present in different parts of the network.

Mostly affects geographical routing protocols

- a single node presents multiple identities to other nodes in the network. The Sybil attack can significantly reduce the effectiveness of fault-tolerant schemes such as distributed storage, disparity and multipath routing, and topology maintenance Replicas, storage partitions, or routes believed to be using disjoint nodes could in actuality be using a single adversary presenting multiple identities.
- Sybil attacks also pose a significant threat to geographic routing protocols. Location aware routing often requires nodes to exchange coordinate information with their neighbors to efficiently route geographically addressed packets. It is only reasonable to expect a node to accept but a single set of coordinates from each of its neighbors, but by using the Sybil attack an adversary can ‘‘be in more than one place at once’’.

WSN Threats - Wormholes

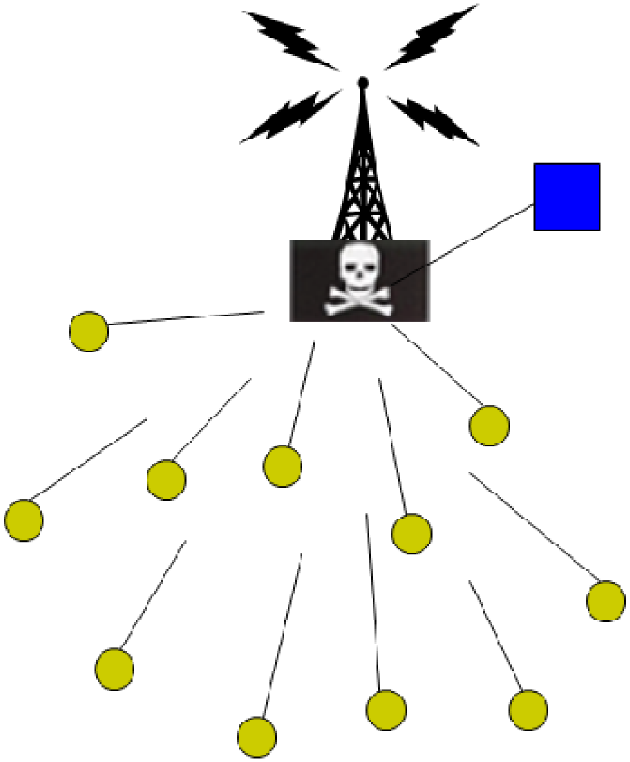
- Idea: tunnel packets received on one part of the network to another
- Well placed wormhole can completely disorder routing
- Wormholes may convince distant nodes that they are close to sink. This may lead to sinkhole if node on the other end advertises high-quality route to sink



- Wormholes can exploit routing race conditions which happens when node takes routing decisions based on the first route advertisement
- Attacker may influence network topology by delivering routing information to the nodes before it would really reach them by multi hop routing
- Even encryption can not prevent this attack
- Wormholes may convince two nodes that they are neighbors when on fact they are far away from each other
- Wormholes may be used in conjunction with Sybil attack

WSN Threats - HELLO flood attacks

- Many WSN routing protocols require nodes to broadcast HELLO packets after deployment, which is a sort of neighbor discovery based on radio range of the node
- Laptop class attacker can broadcast HELLO message to nodes and then advertises high-quality route to sink



WSN Threats - Spoofed routing information

Spoofed routing information: the most direct attack against a routing protocol is to target the routing information in the network. An attacker may spoof, alter, or replay routing information to disrupt traffic in the network. These disruptions include creation of routing loops, attracting or repelling network traffic from selected nodes, extending or shortening source routes, generating fake error messages, causing network partitioning, and increasing end-to-end latency.

WSN Threats - Acknowledgment spoofing

Acknowledgment spoofing: some routing algorithms for WSNs require transmission of acknowledgment packets. An attacking node may overhear packet transmissions from its neighboring nodes and spoof the acknowledgments thereby providing false information to the nodes. In this way, the attacker is able to disseminate wrong information about the status of the nodes.

WSN Threats – Denial of Service (DoS)

Denial of Service (DoS)

It occurs by the unintentional failure of nodes or malicious action. The simplest DoS attack tries to exhaust the resources available to the victim node, by sending extra unnecessary packets and thus prevents legitimate network users from accessing services or resources to which they are entitled. DoS attack is meant not only for the adversary’s attempt to subvert, disrupt, or destroy a network, but also for any event that diminishes a network’s capability to provide a service. In wireless sensor networks, several types of DoS attacks in different layers might be performed.

At physical layer the DoS attacks could be jamming and tampering, **at link layer**, collision, exhaustion, unfairness, **at network layer**, neglect and greed, homing, misdirection, black holes and **at transport layer** this attack could be performed by malicious flooding and desynchronization.

WSN Threats – Other attacks

Passive Information Gathering

An intruder with an appropriately powerful receiver and well designed antenna can easily pick off the data stream. Interception of the messages containing the physical locations of sensor nodes allows an attacker to locate the nodes and destroy them. Besides the locations of sensor nodes, an adversary can observe the application specific content of messages including message IDs, timestamps and other fields.

Node Capturing

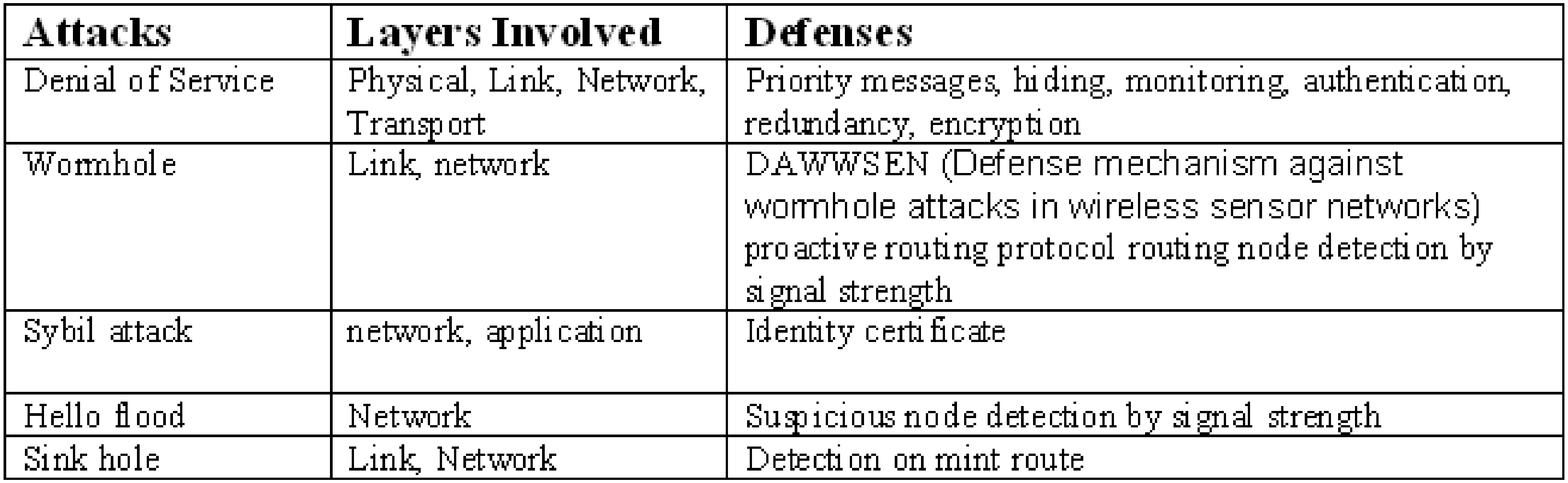
A particular sensor might be captured, and information stored on it might be obtained by an adversary.

False or Malicious Node

Most of the attacks against security in wireless sensor networks are caused by the insertion of false information by the compromised nodes within the network.

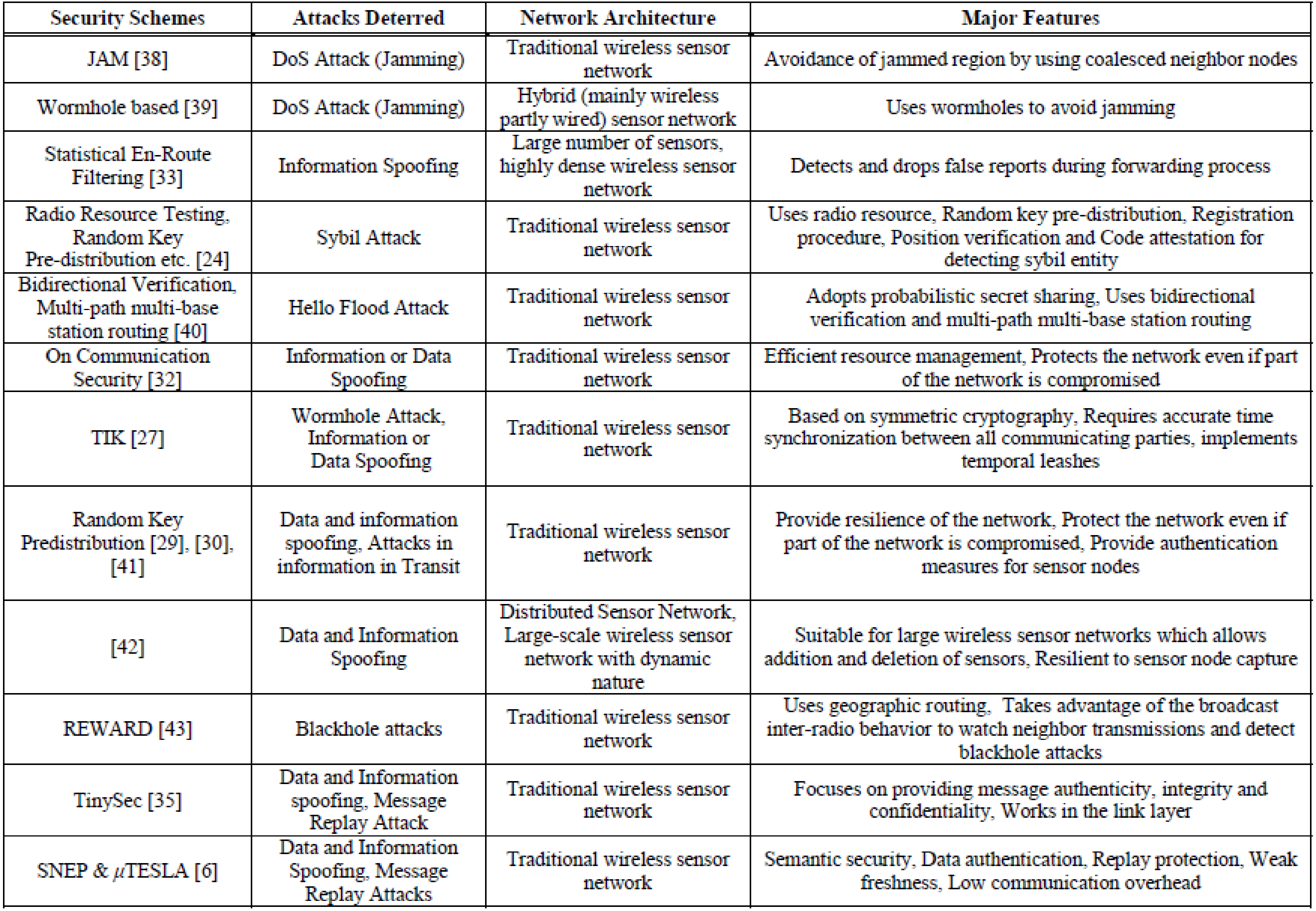
WSN attacks in layers and defense mechanisms

Some attacks and defense mechanisms are provided below:



Attacks	Layers Involved	Defenses
Denial of Service	Physical, Link, Network, Transport	Priority messages, hiding, monitoring, authentication, redundancy, encryption
Wormhole	Link, network	DAWWSEN (Defense mechanism against wormhole attacks in wireless sensor networks) proactive routing protocol routing node detection by signal strength
Sybil attack	network, application	Identity certificate
Hello flood	Network	Suspicious node detection by signal strength
Sink hole	Link, Network	Detection on mint route

WSN Security Schemes and attacks



Security Schemes	Attacks Deterred	Network Architecture	Major Features
JAM [38]	DoS Attack (Jamming)	Traditional wireless sensor network	Avoidance of jammed region by using coalesced neighbor nodes
Wormhole based [39]	DoS Attack (Jamming)	Hybrid (mainly wireless partly wired) sensor network	Uses wormholes to avoid jamming
Statistical En-Route Filtering [33]	Information Spoofing	Large number of sensors, highly dense wireless sensor network	Detects and drops false reports during forwarding process
Radio Resource Testing, Random Key Pre-distribution etc. [24]	Sybil Attack	Traditional wireless sensor network	Uses radio resource, Random key pre-distribution, Registration procedure, Position verification and Code attestation for detecting sybil entity
Bidirectional Verification, Multi-path multi-base station routing [40]	Hello Flood Attack	Traditional wireless sensor network	Adopts probabilistic secret sharing, Uses bidirectional verification and multi-path multi-base station routing
On Communication Security [32]	Information or Data Spoofing	Traditional wireless sensor network	Efficient resource management, Protects the network even if part of the network is compromised
TIK [27]	Wormhole Attack, Information or Data Spoofing	Traditional wireless sensor network	Based on symmetric cryptography, Requires accurate time synchronization between all communicating parties, implements temporal leashes
Random Key Predistribution [29], [30], [41]	Data and information spoofing, Attacks in information in Transit	Traditional wireless sensor network	Provide resilience of the network, Protect the network even if part of the network is compromised, Provide authentication measures for sensor nodes
[42]	Data and Information Spoofing	Distributed Sensor Network, Large-scale wireless sensor network with dynamic nature	Suitable for large wireless sensor networks which allows addition and deletion of sensors, Resilient to sensor node capture
REWARD [43]	Blackhole attacks	Traditional wireless sensor network	Uses geographic routing, Takes advantage of the broadcast inter-radio behavior to watch neighbor transmissions and detect blackhole attacks
TinySec [35]	Data and Information spoofing, Message Replay Attack	Traditional wireless sensor network	Focuses on providing message authenticity, integrity and confidentiality, Works in the link layer
SNEP & μTESLA [6]	Data and Information Spoofing, Message Replay Attacks	Traditional wireless sensor network	Semantic security, Data authentication, Replay protection, Weak freshness, Low communication overhead

WSN Future and Challenges

Ultimate limitations of secure multihop routing

An ultimate limitation of building a multi hop routing topology around a fixed set of base stations is that those nodes within one or two hops of the base stations are particularly attractive for compromise. After a significant number of these nodes have been compromised, all is lost. This indicates that clustering protocols like LEACH where cluster-heads communicate directly with a base station may ultimately yield the most secure solutions against node compromise and insider attacks.

Another option may be to have a randomly rotating set of ‘‘virtual’’ base stations to create an overlay network. After a set of virtual base stations have been selected, a multi hop topology is constructed using them. The virtual base stations then communicate directly with the real base stations. The set of virtual base stations should be changed frequently enough to make it difficult for adversaries to choose the ‘‘right’’ nodes to compromise

Challenge: Build an automatic adaptable trust-based security model to transfer the information with minimum overheads

Conclusions

- **Presented the overview of the WSN. The overview includes the introduction, characteristics, specifications and facors influencing the WSN design**
- Topology – several models of implementing the sensor network (fully connected, Mesh, Star, ring, tree. bus)
- Applications – includes health care to defense applications
- Protocols and Routing – discussed various communication protocols
- Threats – threats includes sinkhole attacks, wormholes, selective forwarding, and HELLO flood attacks.
- Future and Challenges – The current status and future challenges are presented in theis part.

References

- Sophia Kaplantzis, “Security Models for Wireless Sensor Networks”, March 2006
- John Paul Walters, Zhengqiang Liang, Weisong Shi, and Vipin Chaudhary, “Wireless Sensor Network Security, A survey. Chapter 17, Security in Distributed Grid, and Pervasive Computing (Yang Xiao editors), 2006 CRC press
- Jaydip Sen, “A survey on Wireless Sensor Network Security”, Int. Jr. of Communication Networks and Information Security (IJCNIS), Vol 1, No.2 , Aug 2009
- Vasyl A. Radzevych and Sunu Mathew, “Security in Wireless Sensor Networks: Key Management Approaches (Power point presentation, available on Internet)
- Joshua Backfield, “Network Security Model”, SANS Institute 2008
- J. Hill, R. Szewczyk, A. Woo, S. Hollar, D.E. Culler, and K. Pister, “System architecture directions for networked sensors”, In Proceedings of the 9th International Conference on Architectural Support for Programming Languages and Operating Systems, New York, ACM Press, 2000, pp. 93-104.
- G. Gaubatz, J.P. Kaps, and B. Sunar, “Public key cryptography in sensor networks-Revisited”, In Proceedings1st European Workshop on Security in Ad-Hoc and Sensor Networks (ESAS ‘04), 2004.
- D.J. Malan, M. Welsh, and M.D. Smith, “A public-key infrastructure for key distribution in TinyOS based on elliptic curve cryptography”, In Proceedings of the 1st IEEE International Conference on Sensor and Ad Hoc Communications and Networks, Santa Clara, California, October, 2004
- R. Watro, D. Kong, S. Cuti, C. Gardiner, C. Lynn, and P. Kruus, “TinyPK: Securing sensor networks with public key technology”, In Proceedings of the 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN’04), pp. 59-64, New York, USA, 2004, ACM Press.
- Karlof, N. Sastry, and D. Wagner, “TinySec: a link layer security architecture for wireless sensor networks”, In 2nd ACM Conference on Embedded Networked Sensor Systems (SensSys’04), Baltimore, MD, November 2004, pp. 162-175
- Liu and P. Ning, “TinyECC: Elliptic Curve Cryptography for Sensor Networks (version 0.1), September 2005, [online], available at http://discovery.csc.ncsu.edu/software/TinyECC/.

Security Issues and Approaches to solve

Security Issues

Security Issues and Approaches to solve

Main security threats in WSN are:

Radio links are insecure – eavesdropping / injecting faulty information is possible

Sensor nodes are not temper resistant – if it is compromised attacker obtains all security information

Attacker's target:

- **Nodes** (Mote-class): attacker has access to some number of nodes with similar characteristics
- **Base Station** (laptop-class): attacker has access to more powerful devices
- **Outside** (Radio links)
- **Network** (inside): attacker compromised some number of nodes in the network
- **Other (software)**

Security Issues and Approaches to solve

Main types of attacks on WSN are (discussed before):

- Spoofed, altered, or replayed routing information
- Selective forwarding
- Sinkhole attack
- Sybil attack
- Wormholes
- HELLO flood attacks
- Acknowledgment spoofing

Security Issues and Approaches to solve
Constraints on WSN security

- **Energy constraints** – energy requires to convert input energy to output, communication among the sensor nodes, and computation. Security costs significantly particularly cryptography. WSN could be divided into different security levels depending upon energy costs.
- **Memory Limitations -** Sensors nodes require simple algorithms since they do not have enough space to store and execute complicated algorithms. For example, TelosB- has a 16-bit, 8 MHz RISC CPU with only 10K RAM, 48K program memory, and 1024K flash storage.
- **Unreliable Communication -** The packets are get damaged or corrupted while transferring using connectionless protocols. Many times the packets may need to retransmit due to collision or unreliable communication.
- **Unattended operation of networks -** In most cases, the nodes in a WSN are deployed in remote regions and are left unattended. The likelihood that a sensor encounters a physical attack in such an environment is therefore, very high. Remote management of a WSN makes it virtually impossible to detect physical tampering. This makes security in WSNs a particularly difficult task.
- **Higher latency in communication**: In WSN synchronization is very difficult particularly in multi-hop routing and cryptography key distribution. Higher latency is possible.

Security Issues and Approaches to solves Security Requirements

- **Data confidentiality** – authorized nodes to read message, key distribution mechanisms must be robust; sensor identification and protect against traffic analysis required.
- **Data integrity** – no message can be altered by an entity while traversing from one node to other
- **Availability** – services must be available even in presence of internal or external attacks
- **Data freshness –** ensure no adversary can reply old messages. Reply attack with old keys must not be allowed.
- **Self-organization –** security poses great challenge while WSN is in self-organizing or self-healing. Number of mechanisms were proposed but public key cryptographic technique is an efficient mechanism for key distribution.
- **Secure localization** – accurately and automatically locate the sensor node in WSN poses a challenge. The locators are trusted and cannot be compromised by any attacker.
- **Time synchronization** – proposed security mechanisms for WSN should be time synchronized and collaborative WSN synchronize among group of sensors
- **Authentication** – many authentication sachems are proposed for secure routing and reliable packet transfer. Authentication can also be achieved through message authentication code.

Security Issues and Approaches to solve Security Vulnerabilities in WSNs

The security models will be one of the categories.

The attacks on WSN are divided into three types

- **Attacks on secrecy and authentication** - standard cryptographic techniques can protect the secrecy and authenticity of communication channels from outsider attacks such as eavesdropping, packet replay attacks, and modification or spoofing of packets.
- **Attacks on network availability** - attacks on availability of WSN are often referred to as denial-of-service (DoS) attacks.
- **Stealthy attack against service integrity** - in a stealthy attack, the goal of the attacker is to make the network accept a false data value.

  For example, an attacker compromises a sensor node and injects a false data value through that sensor node. In these attacks, keeping the sensor network available for its intended use is essential.

  DoS attacks against WSNs may permit real-world damage to the health and safety of people. The DoS attack usually refers to an adversary's attempt to disrupt, subvert, or destroy a network. However, a DoS attack can be any event that diminishes or eliminates a network's capacity to perform its expected functions.

Security Issues and Approaches to solve
Attacks on Network Layers

Physical layer attacks

- Jamming
- Tampering

Link layer attacks (responsible for data streams, data frame detection, medium access control, and error control)

- Purposefully created collisions
- Resource exhaustion
- Unfairness in allocation of resources

Network layer attacks

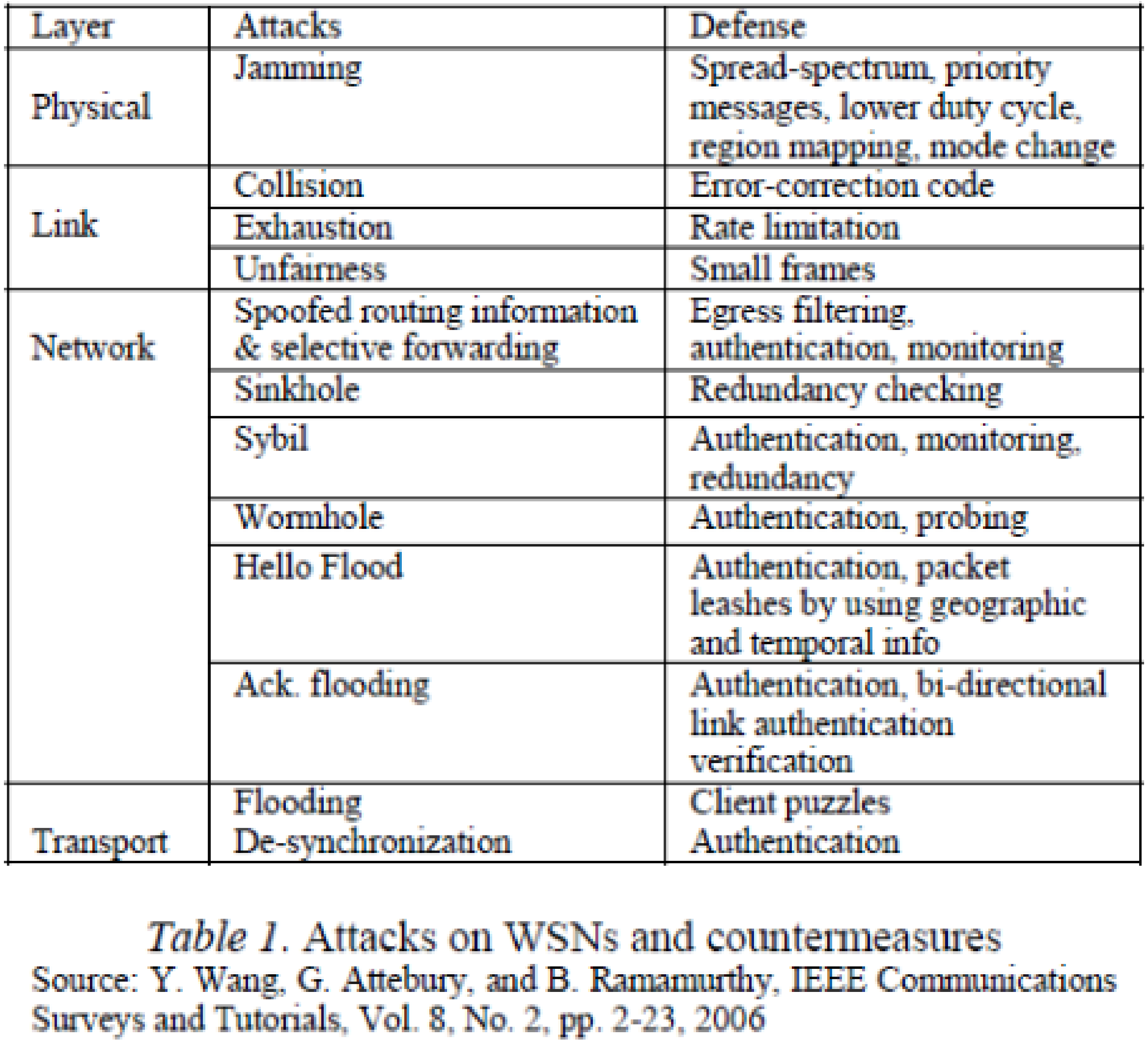
- Spoofed routing information
- Selective forwarding
- Sinkhole
- Sybil attack
- Wormhole
- Hello flood
- Acknowledgment spoofing

Transport layer attacks

- Flooding
- De-synchronization

Security Issues and Approaches to solve
Summary of Attacks on Network Layers

rs



Layer	Attacks	Defense
Physical	Jamming	Spread-spectrum, priority messages, lower duty cycle, region mapping, mode change
Link	Collision	Error-correction code
	Exhaustion	Rate limitation
	Unfairness	Small frames
Network	Spoofed routing information & selective forwarding	Egress filtering, authentication, monitoring
	Sinkhole	Redundancy checking
	Sybil	Authentication, monitoring, redundancy
	Wormhole	Authentication, probing
	Hello Flood	Authentication, packet leashes by using geographic and temporal info
	Ack. flooding	Authentication, bi-directional link authentication verification
Transport	Flooding De-synchronization	Client puzzles Authentication

Table 1. Attacks on WSNs and countermeasures

Source: Y. Wang, G. Attebury, and B. Ramamurthy, IEEE Communications Surveys and Tutorials, Vol. 8, No. 2, pp. 2-23, 2006

Security Issues and Approaches to solve

Approaches to solve

Security Issues and Approaches to solve

Why conventional methods are difficult to implement in WSN?

- A wireless sensor network consists of large number of small size sensor nodes with limited resource capabilities of battery power, processing, storage, and bandwidth. Due to these limitations, it is difficult to employ the conventional security mechanisms in WSN.
- Need to modify conventional methods

Security Issues and Approaches to solve

Encryption at Link-layer prevents majority of attacks but deployment of **key management** architecture is suggested

Reasons

- Avoids bogus routing information, Sybil attack, acknowledge spoofing, etc.
- Cannot avoid Wormhole attack, HELLO flood attacks
- Multi-path routing, bidirectional link verification can be used to avoid "selective forwarding and HELLO flood" attacks

Goals

- The protocol must establish a key between all sensor nodes that must exchange data securely
- Node addition / deletion should be supported
- It should work in undefined deployment environment
- Unauthorized nodes should not be allowed to establish communication with network nodes

Security Issues and Approaches to solve

Key management Constraints

- **Sensor node constraints:**
  - Battery power
    - Computational energy consumption
    - Communication energy consumption
  - Transmission range
  - Memory
  - Temper protection
  - Sleep pattern
- **Network constraints:**
  - Ad-hoc network nature
  - Packet size

Security Issues and Approaches to solve

Key management: evaluation/comparison metrics

- **Resilience against node capture**: how many node are to be compromised in order to affect traffic of not compromised nodes?
- **Addition:** how complicated is dynamic node addition?
- **Revocation**: how complicated is dynamically node revocation?
- **Supported network size**: what is the maximum possible size of the network?

- **Note:** since WSN can be used in a lot of different ways it is not reasonable to look for one key management approach to suite all needs: 20 000 node network deployed from the airplane over a battle field has quite different requirements from 10 node network installed to guard the perimeter of the house

Approaches to solve the threats

- Pre-deployed keying:
  - Key pre-deployment
    - ➢ Straightforward approaches
    - ➢ Eschenauer / Gligor random key pre-deployment
    - ➢ Chan / Perrig q-composite approach (Chan, H., Perrig, A., and Song, D. 2003. Random key predistribution schemes for sensor networks.)
    - ➢ Zhu / Xu approach (Zhu, S., Xu, S., Setia, S., and Jajodia, S: Establishing pairwise keys for secure communication in ad hoc networks: A probabilistic approach, 2003)
    - ➢ DiPietro smart attacker model and PRK protocol (**Efficient and Resilient Key Discovery based on Pseudo-Random Key Pre-Deployment)**
  - Key derivation information pre-deployment
    - ➢ Liu / Ning polynomial pre-deployment (Liu, D. and Ning: Establishing pairwise keys in distributed sensor networks (2003).
- Self-enforcing autonomous approaches
  - Pair-wise asymmetric (public key)
- Arbitrated protocols
    - ➢ Identity based hierarchical keying

Approaches to solve the threats

Straight forward approaches

- Single mission key is obviously unacceptable
- Pair-wise private key sharing between every two nodes is impractical because of the following reasons:
  - it requires pre-distribution and storage of n-1 keys in each node which is n(n-1)/2 per WSN.
  - most of the keys would be unusable since direct communication is possible only in the nodes neighborhood
  - addition / deletion of the node and re-keying are

Approaches to solve the threats

Intrusion Detection, Game Models, Trust-based models

References

Intrusion Detection

- YuanYuan Li and Lynne E. Parker; Intruder detection using a wireless sensor network with an intelligent mobile robot response
- Ana Paula R. da Silva, Antonio A.F. Loureiro, Marcelo H.T. Martins, Linnyer B. Ruiz , Bruno P.S. Rocha, Hao Chi Wong; Decentralized Intrusion Detection in Wireless Sensor Networks
- Vijay Bhuse, Ajay Gupta, Anomaly Intrusion Detection in Wireless Sensor Networks
- Olivier Dousse, Christina Tavoularis, Patrick Thiran; Delay of Intrusion Detection in Wireless Sensor Networks

Game Models

- Y. B. Reddy., Jan Durand, and Sanjeev Kafle., “Detection of Packet Dropping in Wireless Sensor Networks”, ITNG 2010
- Y. B. Reddy., “Potential Game Model to Detect Holes in Sensor Networks”, IFIP/NTMS 2009
- Y. B. Reddy, “Detecting Sinkhole Attack by Observing the Quality of Link in Wireless Sensor Networks”, ICWN’09 - The 2009 International Conference on Wireless Networks, July 13-16, Las Vegas.
- Y. B. Reddy, “A Game Theory Approach to Detect Malicious Nodes in Wireless Sensor Networks”, SENSORCOM09, Athens, Greece.

Trust based models

- Y. B. Reddy and Rastko Selmic., “Agent-based Trust calculation in Wireless Sensor Networks” SENSORCOMM 2011, August 21-27, 2011.
- Y. B. Reddy and Rastko Selmic., “Cooperative and Collaborative Approach for Secure Packet Transfer in Wireless Sensor Networks” SENSORCOMM 2011, August 21-27, 2011.
- Y. B. Reddy and Rastko Selmic., “Secure Packet Transfer in Wireless Sensor Networks – A Trust-based Approach”, IARIA- ICN 2011, January 23-28, 2011 - St. Maarten.
- Y. B. Reddy and Rastko Selmic., “Trust-based Packet Transfer in Wireless Sensor Networks”, Communications and Information Security (CIS2010), IASTED, Nov 8-10, 2010,USA

WSN Approaches

Intrusion Detection (ID)

What is intrusion detection?

- Intrusion detection is the process of discovering, analyzing, and reporting unauthorized or damaging network or computer activities
- Intrusion detection discovers violations of confidentiality, integrity, and availability of information and resources.

Intrusion detection demands

- Try to store all possible information
- Interpret traffic and computer process
- Constant improvement of technologies to pace the current demands

How Useful is ID?

- Provide useful information to protect the network
- Improve the management and customer understanding
- Helps to understand the functionalities of network at operating systems and protocol levels

Security Issues and models

ID models

Falls into following categories

- Normal
- Abnormal but not malicious
- Malicious

Models

- Network-based ID – monitors network traffic for signs of misuse
- Host-based ID – monitors computer process for signs and misuse
- Hybrid – monitors all

Paradigms

- Anomaly detection – the AI approach
- Misuse detection – simple and easy
- Burglar alarms – policy based detection
- Honey Pots – Lure and hackers in
- Hybrid - combination

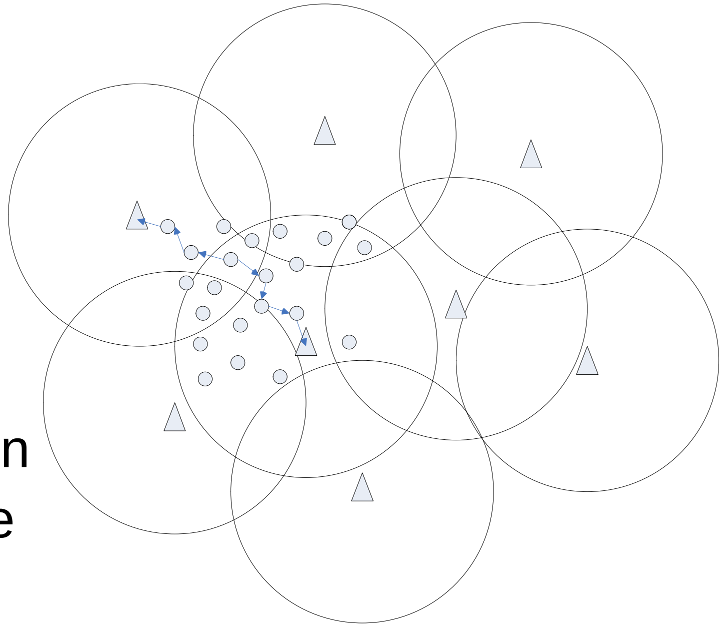
Security Issues and models - ID models

Anomaly detection goals

- Analyze the network flow and infer the status
- Apply statistical or heuristic measures to determine the status
- If the events are not normal generate alert

Misuse detection goals

- Detect the attack using database
- Update database



ID Model

- BS_j: base station at location (X_j, Y_j)
- S_i: sensor node at location (x_i, y_i)
- R: transmission range of the base station
- r: transmission range of the sensor node
- k-coverage: a node covers by k BSs

Develop the required model to detect malicious node and avoid the traffic (probability models, game models, or other)

Security Issues and models

Application of ID to WSN

Proposed IDS models and problems

Intrusion detection based on AODV (Ad hoc On-Demand Distance Vector Routing Protocol)

Pros

- Sophisticated algorithm for detecting and reacting to a great variety of potential wireless network attacks using an anomaly detection pattern
- Works well for ad-hoc wireless networks

Cons

- Computationally expensive

Reference: Wireless Sensor Networks for Intrusion Detection: Packet Traffic Modeling

IEEE Communications Letters, Jan 2006

Security Issues and models

Effective Intrusion Detection using Multiple Sensors in Wireless Ad Hoc Networks

- Pros
  - Mobile agent based intrusion detection
  - Intelligent routing of intrusion data throughout the network
  - Lightweight implementation
- Cons
  - Agent only deployed on a fraction of the network nodes
  - Not deployed on completely wireless sensor networks

Reference: Effective Intrusion Detection Using Multiple Sensors in Wireless Ad Hoc Networks Oleg Kachirski; In Proceedings of the 36th Annual Hawaii International Conference on System Sciences, 2003

Security Issues and models

INSENS (Intrusion Tolerant Routing Protocol for Wireless Sensor Networks)

Pros

Allows an alternative network route to be established between non-malicious nodes

Cons

Does not provide intrusion detection, but rather intrusion tolerance

Still requires the sacrifice of a small number of wireless sensor nodes

Reference: INSENS: Intrusion-Tolerant Routing in Wireless Sensor Networks
Jing Deng*, Richard Han, Shivakant Mishra, Computer Communications, 2005

Security Issues and models

Example 1

Selective Forwarding Attack

- A malicious node selectively neglects to forward messages to the Base Station.

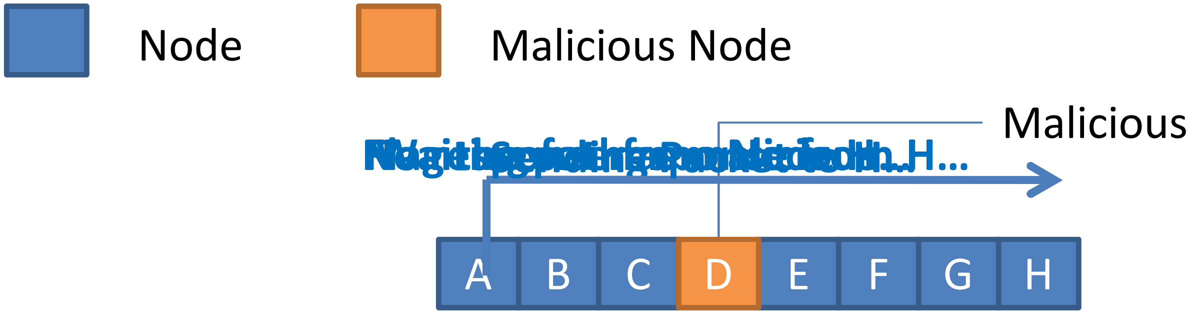
- Can prevent vital information from reaching the base station.
  - E.g. Military applications
- Can be combined with other attacks, such as sinkhole attacks, that try to draw in traffic.

Detecting Selective Forwarding

- Two algorithms to detect selective forwarding:
  - Binary Search Algorithm:
  - Forward Search Algorithm:

Detecting Selective Forwarding (Binary Search)

- Binary Search:
  - In sending a packet from node A to the H (base station), if no acknowledgement is received from H then this raises a flag and the path [node A…H] is tested using the Binary Search method.
  - Halves the list of suspects each iteration until the malicious node is found.

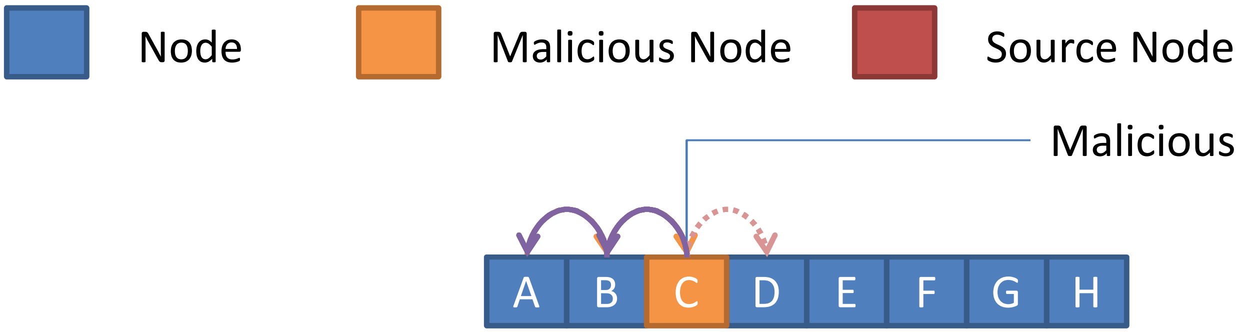


Binary Search: Advantages/Disadvantages

- Pros:
  - Takes the same amount of time to detect a malicious node whether it is near the start of the path or near the end of the path.

Detecting Selective Forwarding (Forward Search)

- Forward Search:
  - – In sending a packet from node A to the BS, an acknowledgement is expected from every node along the path. Otherwise, the acknowledgement data available is used to find the malicious node.



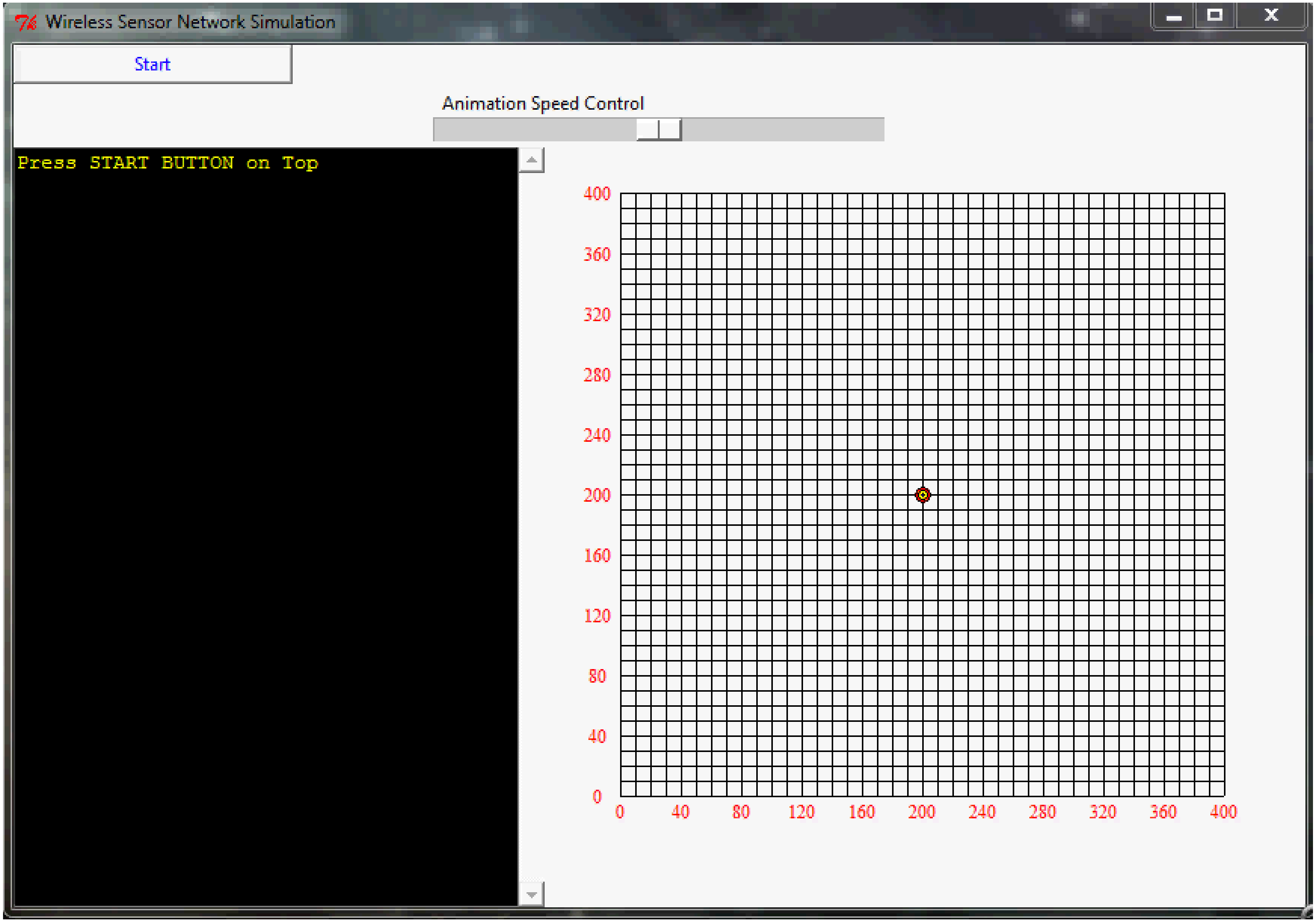
Forward Search: Advantages/Disadvantages

- Pros:
  - Can detect the presence of malicious nodes even before reaching the base station.

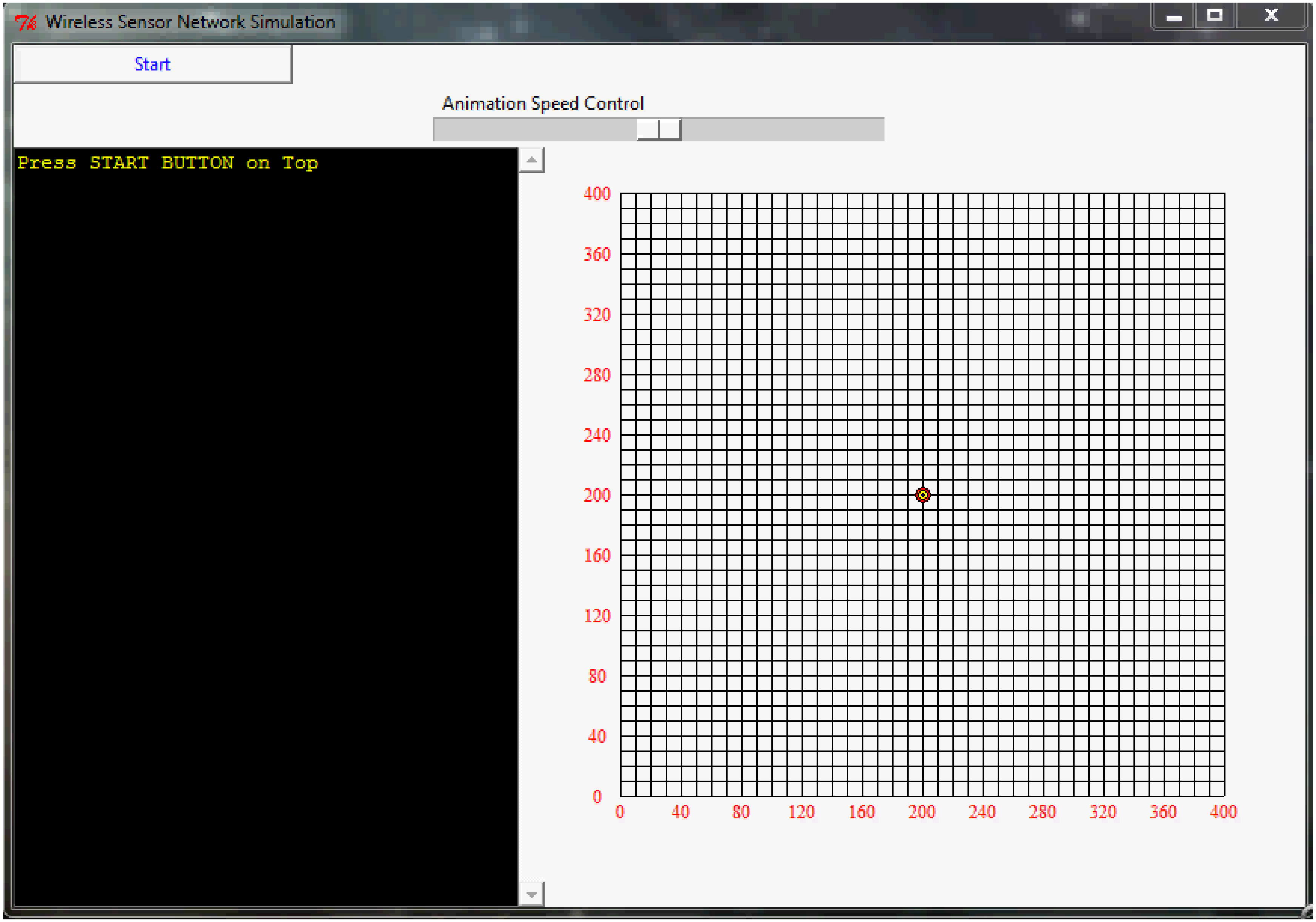
- Cons:
  - Produces a lot of overhead, which is unnecessary if there is no malicious node in the path.

WSN Simulation

- Graphical simulation of a randomly distributed wireless sensor network.
- Compares the Binary Search and Forward Search detection methods and outputs results.
- Programmed using the Python language and the *Tkinter* graphics module.

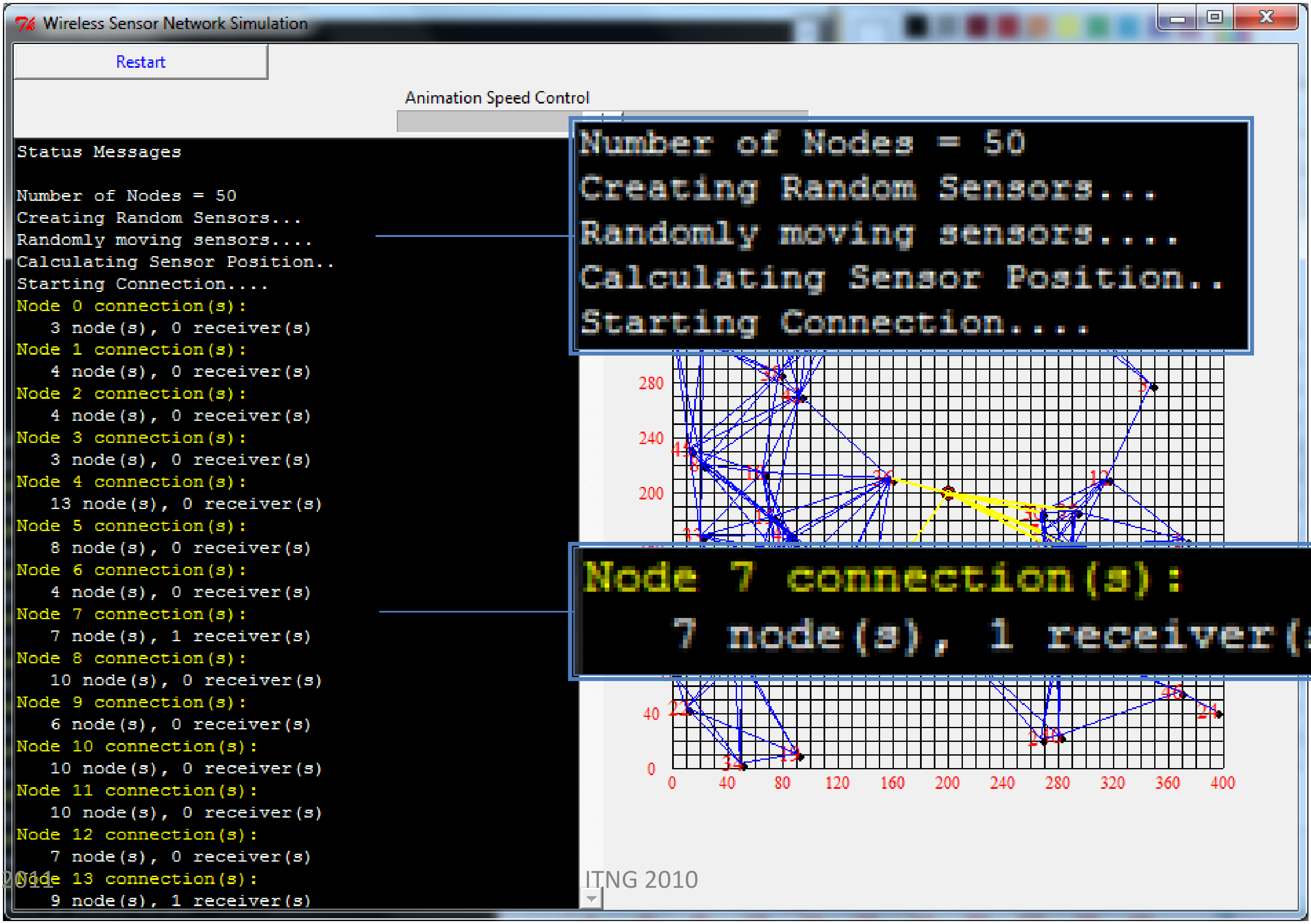


```
Press START BUTTON on Top
```



```
Press START BUTTON on Top
```

WSN Simulation



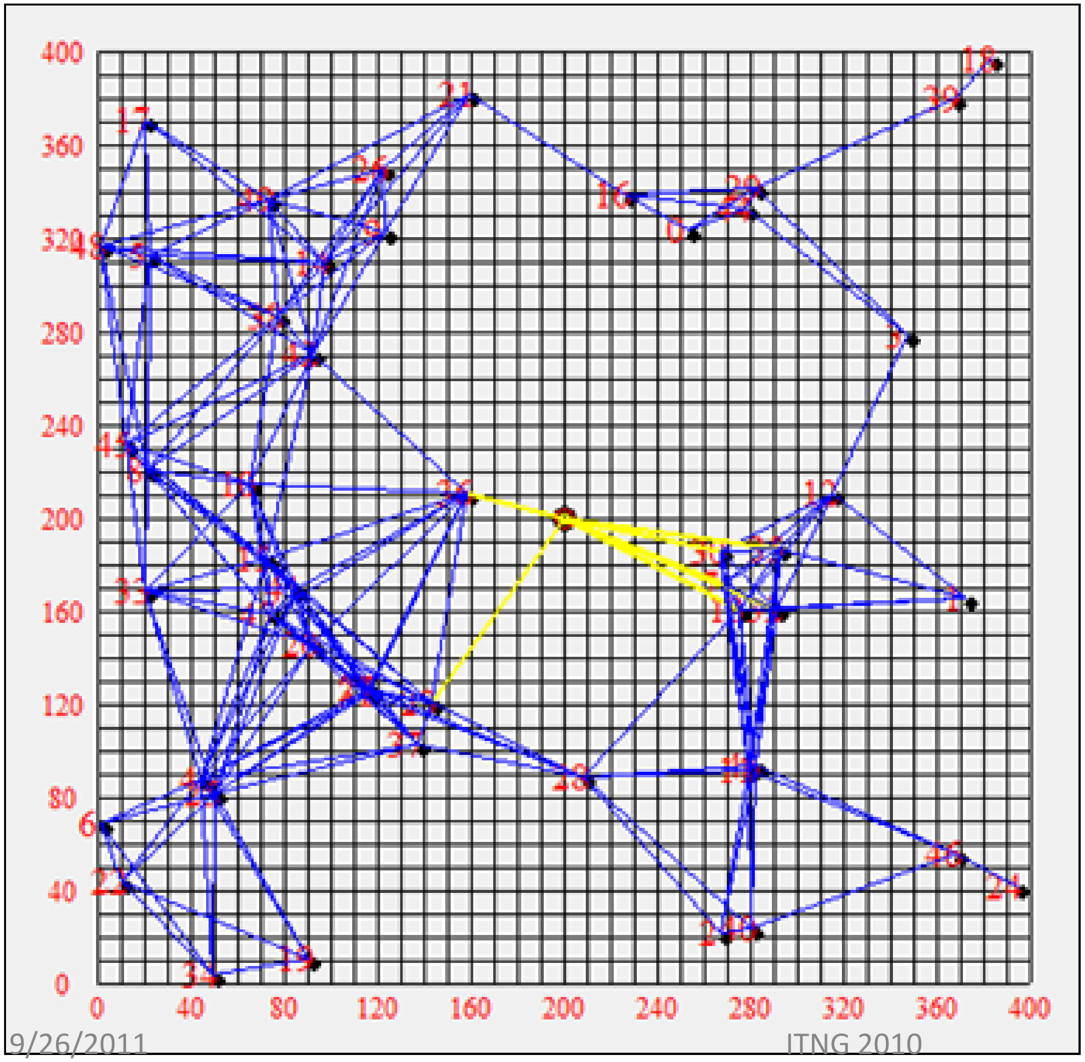
```
Status Messages

Number of Nodes = 50
Creating Random Sensors...
Randomly moving sensors....
Calculating Sensor Position..
Starting Connection....
Node 0 connection(s):
   3 node(s), 0 receiver(s)
Node 1 connection(s):
   4 node(s), 0 receiver(s)
Node 2 connection(s):
   4 node(s), 0 receiver(s)
Node 3 connection(s):
   3 node(s), 0 receiver(s)
Node 4 connection(s):
   13 node(s), 0 receiver(s)
Node 5 connection(s):
   8 node(s), 0 receiver(s)
Node 6 connection(s):
   4 node(s), 0 receiver(s)
Node 7 connection(s):
   7 node(s), 1 receiver(s)
Node 8 connection(s):
   10 node(s), 0 receiver(s)
Node 9 connection(s):
   6 node(s), 0 receiver(s)
Node 10 connection(s):
   10 node(s), 0 receiver(s)
Node 11 connection(s):
   10 node(s), 0 receiver(s)
Node 12 connection(s):
   7 node(s), 0 receiver(s)
Node 13 connection(s):
   9 node(s), 1 receiver(s)
```

```
Number of Nodes = 50
Creating Random Sensors...
Randomly moving sensors....
Calculating Sensor Position..
Starting Connection....
```

```
Node 7 connection(s):
   7 node(s), 1 receiver(s)
```

Network Graph



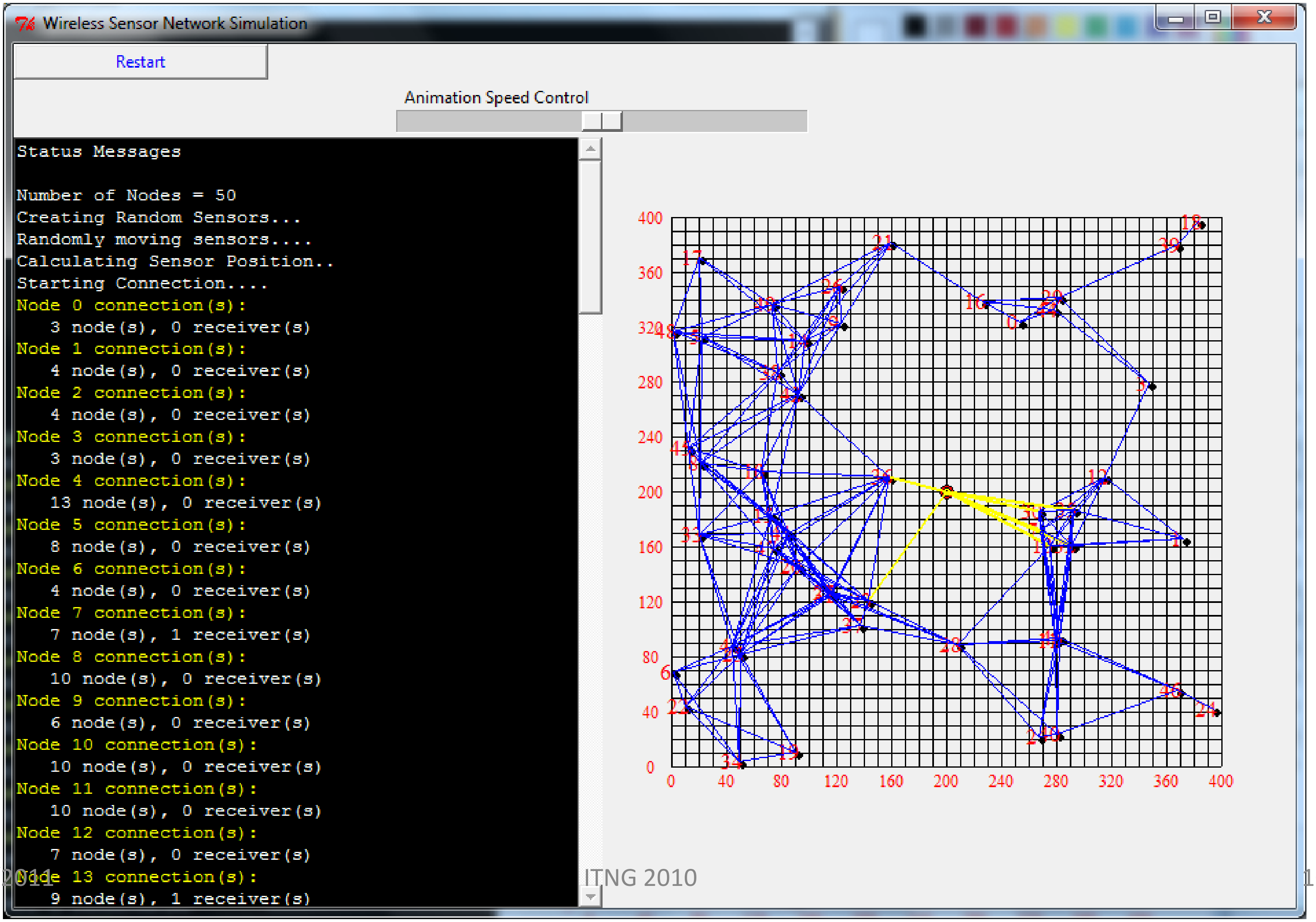
Base Station (BS)

Node

▬ Link between two (2) nodes

▬ Link between a node & the BS

WSN Simulation

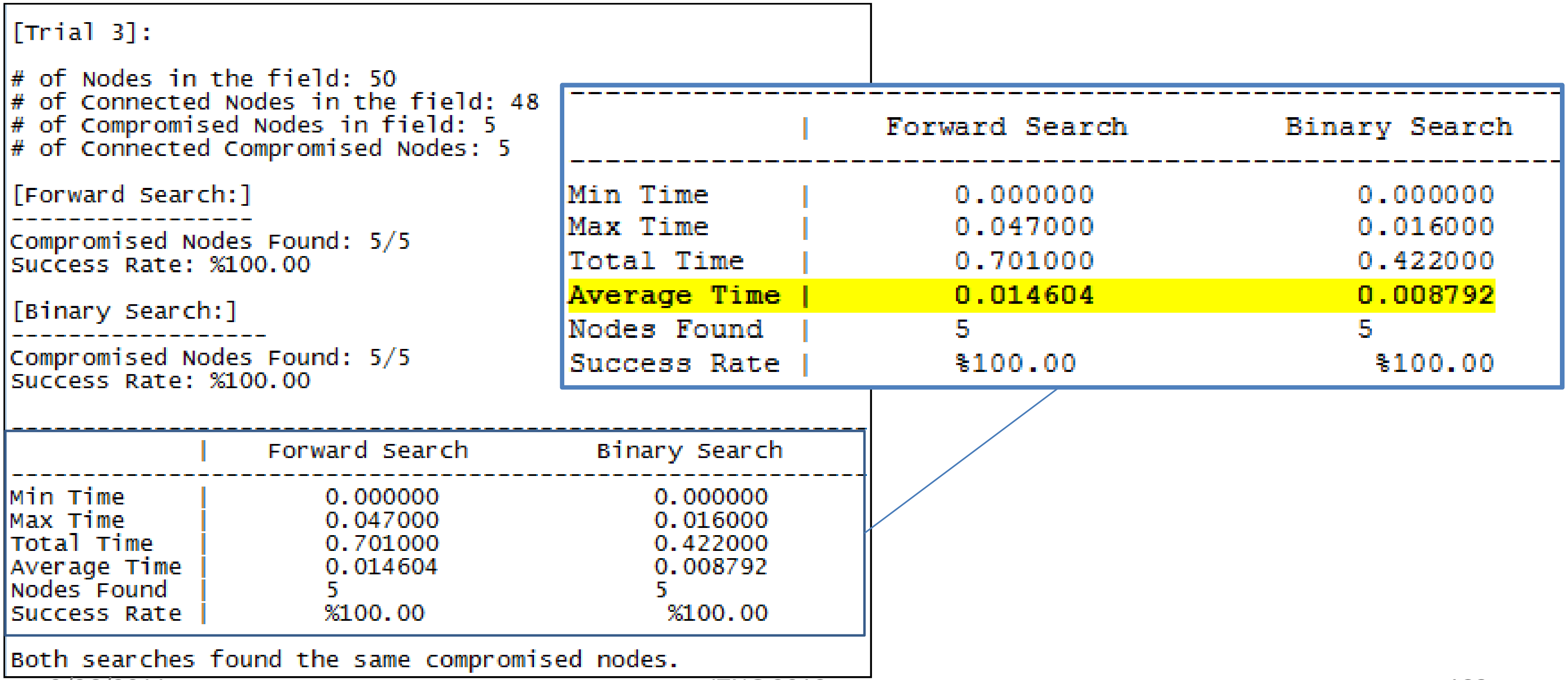


```
Status Messages

Number of Nodes = 50
Creating Random Sensors...
Randomly moving sensors....
Calculating Sensor Position..
Starting Connection....
Node 0 connection(s):
   3 node(s), 0 receiver(s)
Node 1 connection(s):
   4 node(s), 0 receiver(s)
Node 2 connection(s):
   4 node(s), 0 receiver(s)
Node 3 connection(s):
   3 node(s), 0 receiver(s)
Node 4 connection(s):
   13 node(s), 0 receiver(s)
Node 5 connection(s):
   8 node(s), 0 receiver(s)
Node 6 connection(s):
   4 node(s), 0 receiver(s)
Node 7 connection(s):
   7 node(s), 1 receiver(s)
Node 8 connection(s):
   10 node(s), 0 receiver(s)
Node 9 connection(s):
   6 node(s), 0 receiver(s)
Node 10 connection(s):
   10 node(s), 0 receiver(s)
Node 11 connection(s):
   10 node(s), 0 receiver(s)
Node 12 connection(s):
   7 node(s), 0 receiver(s)
Node 13 connection(s):
   9 node(s), 1 receiver(s)
```

Results of 1000 Trials of 50-Node Networks

- Binary Search **performed 1.8 times faster** than the Forward Search.
- Forward Search and Binary Search have approximately the **same malicious node identification rate (86%)**.



```
[Trial 3]:

# of Nodes in the field: 50
# of Connected Nodes in the field: 48
# of Compromised Nodes in field: 5
# of Connected Compromised Nodes: 5

[Forward Search:]
-----------------
Compromised Nodes Found: 5/5
Success Rate: %100.00

[Binary Search:]
----------------
Compromised Nodes Found: 5/5
Success Rate: %100.00

--------------------------------------------------------------
              |    Forward Search          Binary Search
--------------------------------------------------------------
Min Time      |         0.000000                0.000000
Max Time      |         0.047000                0.016000
Total Time    |         0.701000                0.422000
Average Time  |         0.014604                0.008792
Nodes Found   |         5                       5
Success Rate  |         %100.00                  %100.00

Both searches found the same compromised nodes.
```

```
--------------------------------------------------------------
              |    Forward Search          Binary Search
--------------------------------------------------------------
Min Time      |         0.000000                0.000000
Max Time      |         0.047000                0.016000
Total Time    |         0.701000                0.422000
Average Time  |         0.014604                0.008792
Nodes Found   |         5                       5
Success Rate  |         %100.00                  %100.00
```

Conclusions

- The current approaches detect the malicious node on the communication path.
- We used two approaches for detecting the malicious node (selective packet dropping)
  - **selective forward search**
  - **binary search**
- The simulations show that binary approach is better than the selective forward approach

The future work includes the application of game models to detect the malicious nodes

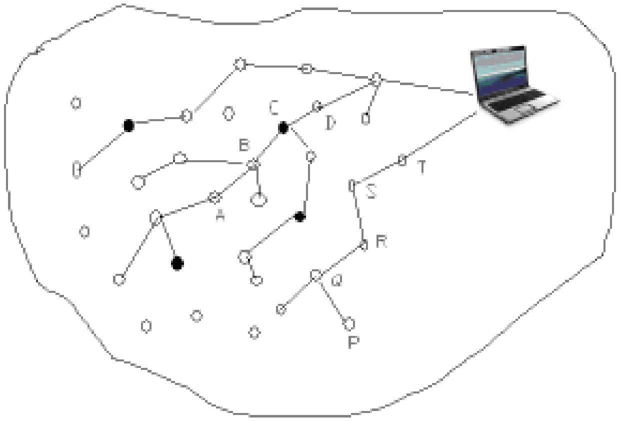
Note: The geometric model provided in the paper was not discussed

Security Issues and models

Example 2

Status of Current WSN Model Security

- Large Number of Sensors with no global Identification, Constantly changing topology, limited resources, deployed densely, prone to failure
- Filled nodes in the figure are malicious nodes
- Packets transferring through these nodes will be dropped randomly (selective forward attack)
- Multipath forwarding has poor security
- Traditional transport layer protocols for WSN also fail to guarantee



Possible Attacks

- The sensor node protocol stack includes application layer, transport layer, network layer, data link layer, and physical layer.
- The DoS (denial of service) vulnerabilities are normally for the last four layers of the stack (except application layer).
- The physical layer attack includes the jamming interferences with radio frequencies and physical tampering of nodes.
- The data link layer attacks include the collision (link layer jamming), abuse of MAC priority schemes, and exhaustion of battery resources.
- The network layer attacks include (a) Spoofed, altered or replaying information, (b) Selective forwarding, (c) Sinkhole attacks, (d) Sybil attack, (e) Wormholes, (f) Hello flood attacks, and (g) Acknowledgement spoofing.
- The transport layer can be attacked via flooding or de-synchronization.

Preliminary Model – Pay off function

- Main function in sensor network – transfer the data to base station
- Hackers – take control of routing layer
- Form the nodes as clusters – Cluster heads transfer data securely
- Therefore, hackers target at routing layer at cluster head
- Watchdog model helps to detect the attack [Towards Intrusion Detection in Wireless Sensor Networks]

- The pay off function to transfer the data from node i to node j

$$U_{i,j}(t) = \alpha \times \Omega_{i,j}(t) + \beta \times \Phi_{i,j}(t) + \gamma \times \Psi_{i,j}(t)$$

where

$\Omega_{i,j}(t)$=Cooperation; $\Phi_{i,j}(t)$=Reputation

$\Psi_{i,j}(t)$=security level and $\alpha + \beta + \gamma = 1$

Detecting compromised node

Maintain the table of entries includes

- history of packet drop rate
- Selection of alternate routs
- Enforcement of security levels

- IDS calculates the pay-off at node level before packet transfers and transfer takes place if pay off is within limits of threshold
- Action: If most of the nodes are compromised – replace cluster head
- Remove the node (s) from network means re-generate the authentication key for the new cluster

Game Theory Basics

Define game G as $G = \langle N, A, \{u_i\} \rangle$

N finite set of players

A Action Space (Cartesian product $A = A_1 \times A_2 \times \ldots \times A_n$)

$\{u_i\}$ Utility function ($\{u_i\} = \{u_1, u_2, \ldots, u_n\}$)

The utility function qualifies the player's preferences over the game of possible outcomes

The outcomes are chosen by a particular player i with action a_i as u_i

and the particular actions chosen by all other players is a_{-i} .

Game Model

- IDS maintains the normal functionality
- Hacker tries to compromise the node
- The probability of defending N nodes (one cluster)

$$E_c = \sum_{i=1}^{N} P_i$$

where P_i is the probability to defend the node

Assuming the total energy is 1, the energy remained with IDS after defending the cluster is: $E_r = 1 - \sum_{i=1}^{N} P_i$

- The energy spend by the attacker $E_a = k\sum_{i=1}^{N} P_i$ for $k \geq 0$
- The node compromises depending upon the k value as given below
  - $k > 1$ to succeed the attack ($E_a > E_c$)
  - $k = 1$ the attacker force is equal to IDS protection (the node may or may not compromise)
  - $k = 0$ then there is no attack on any node
  - $k <= 1$ The node does not compromise

Game Model __Contd..

The payoff (U) is the IDS utility cost – the cost to defend

$$U = E_c - E_a$$

This leads to $U = (1 - \kappa)\sum_{i=1}^{N} P_i$

If k > 1 the attack is successful otherwise fail

Why zero-sum game

The game is between IDS and attacker (two players). Only one player wins and the other looses. The winner gains the total points. In a zero-sum game, if more than two players participate, the winner gains all points. Therefore the currant problem is designed as zero-sum game.

Note: If any one designs this problem as non zero-sum game, the players work cooperatively and more than one winner is possible.

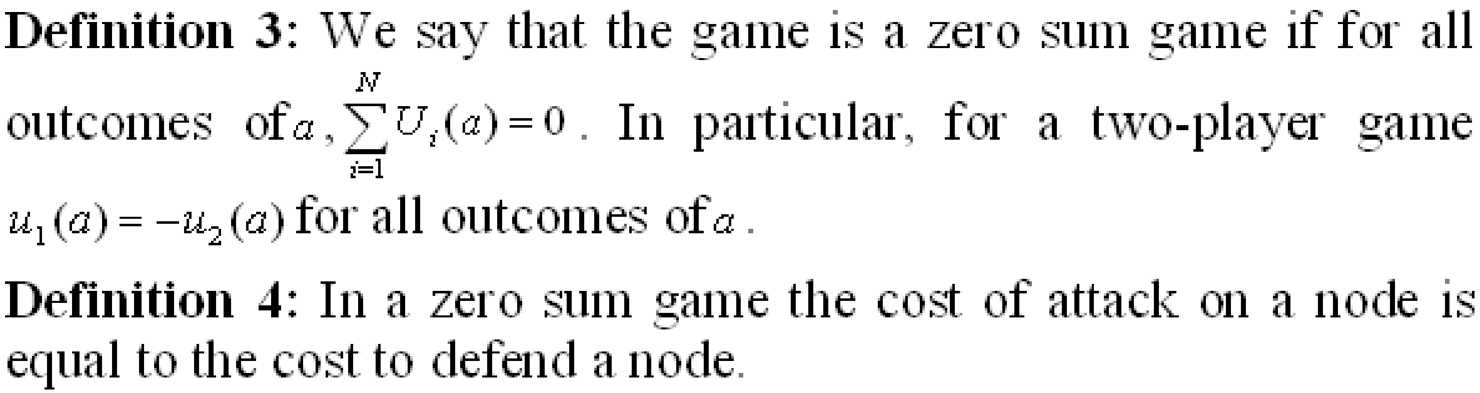
Definitions

Definition 1: An outcome of a game is Pareto optimal if there is no other outcome that makes every player at least as well off and at least one player strictly better off:.

Theorem 1: A zero sum game is not a Pareto optimal

If a change from one allocation to another can make at least one individual better off without making any other individual worse off, then it is called a Pareto improvement. An allocation is Pareto efficient or Pareto optimal when no further Pareto improvements can be made. This is often called a strong Pareto optimum (SPO). This explanation leads that our zero sum game is not Pareto optimal.

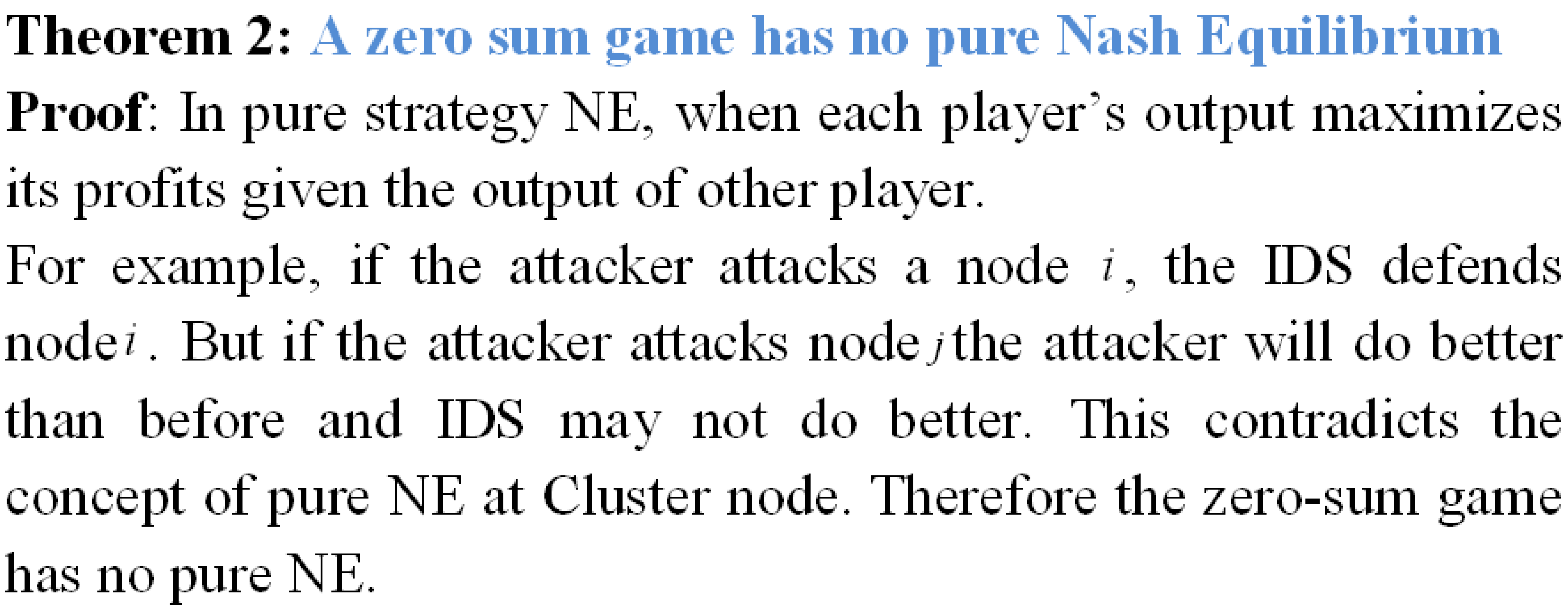
Definition 2: If the zero sum game is Pareto optimal then it is called a conflict game



Definition 3: We say that the game is a zero sum game if for all outcomes of a, $\sum_{i=1}^{N} U_i(a) = 0$. In particular, for a two-player game $u_1(a) = -u_2(a)$ for all outcomes of a.

Definition 4: In a zero sum game the cost of attack on a node is equal to the cost to defend a node.

Nash Equilibrium

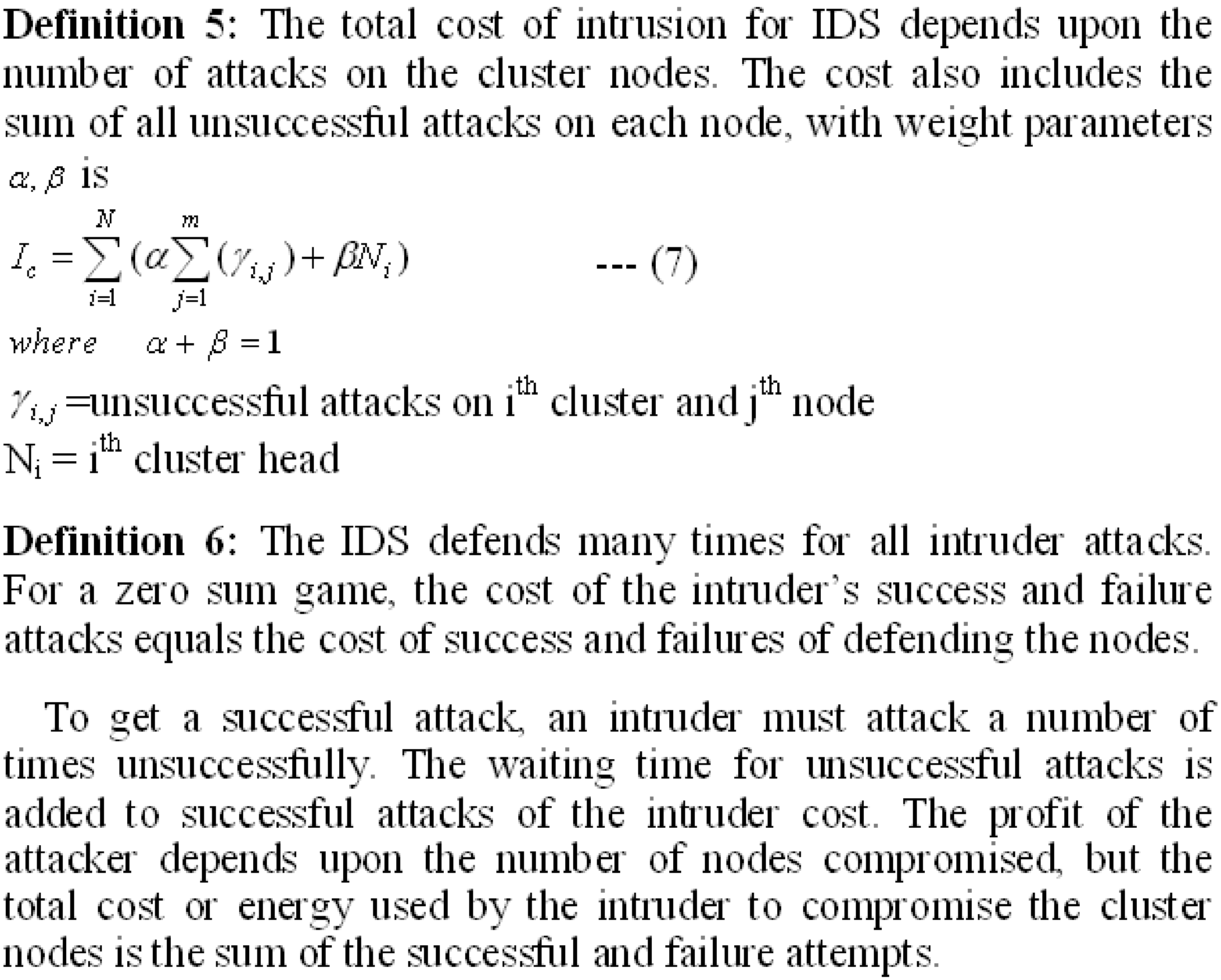


Theorem 2: **A zero sum game has no pure Nash Equilibrium**

Proof: In pure strategy NE, when each player's output maximizes its profits given the output of other player.

For example, if the attacker attacks a node i, the IDS defends node i. But if the attacker attacks node j the attacker will do better than before and IDS may not do better. This contradicts the concept of pure NE at Cluster node. Therefore the zero-sum game has no pure NE.

Cost to defend the Cluster



Definition 5: The total cost of intrusion for IDS depends upon the number of attacks on the cluster nodes. The cost also includes the sum of all unsuccessful attacks on each node, with weight parameters α, β is

$$I_c = \sum_{i=1}^{N} (\alpha \sum_{j=1}^{m} (\gamma_{i,j}) + \beta N_i) \qquad \text{--- (7)}$$

$where \quad \alpha + \beta = 1$

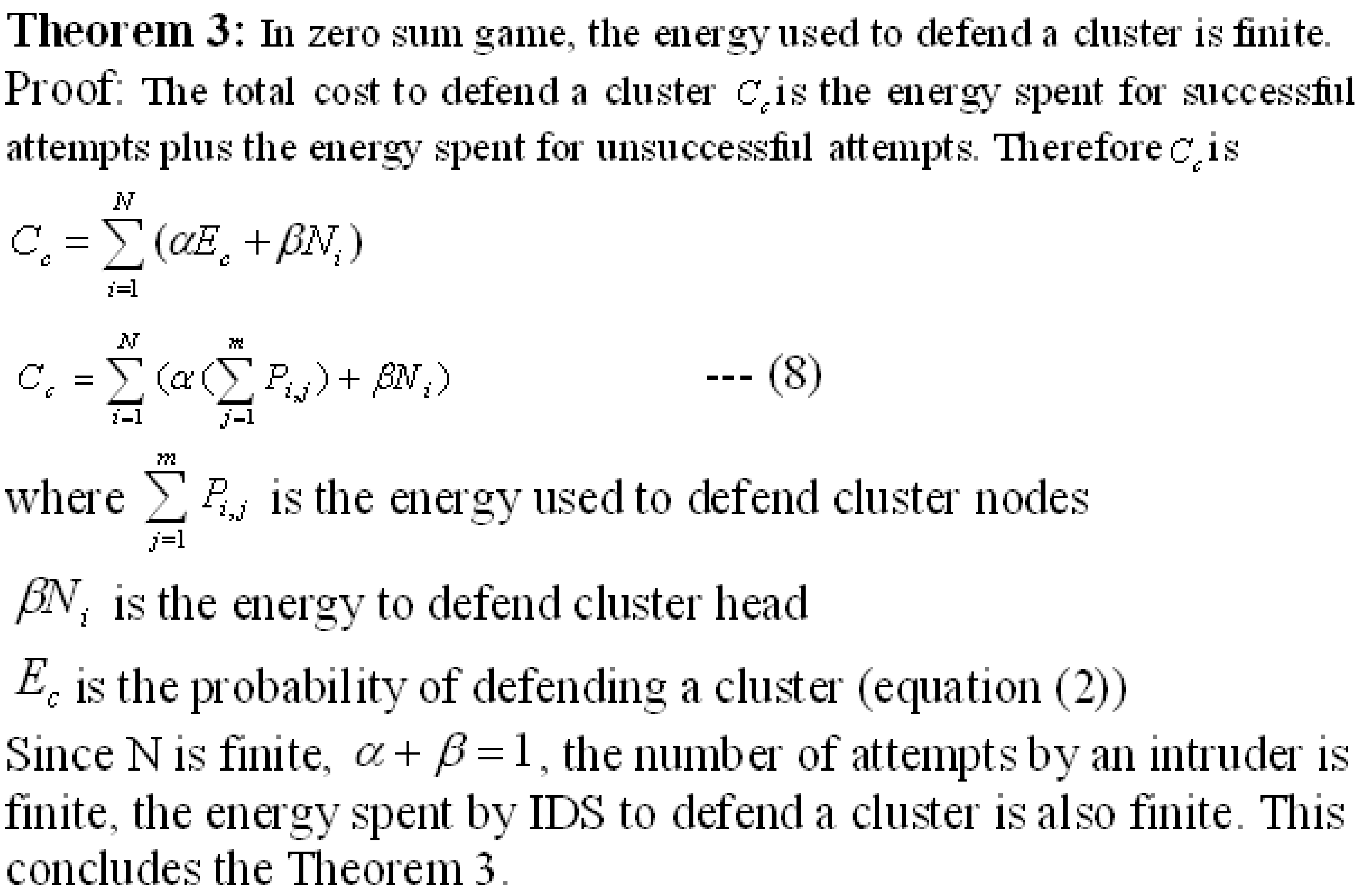
$\gamma_{i,j}$ =unsuccessful attacks on ith cluster and jth node

N_i = ith cluster head

Definition 6: The IDS defends many times for all intruder attacks. For a zero sum game, the cost of the intruder's success and failure attacks equals the cost of success and failures of defending the nodes.

To get a successful attack, an intruder must attack a number of times unsuccessfully. The waiting time for unsuccessful attacks is added to successful attacks of the intruder cost. The profit of the attacker depends upon the number of nodes compromised, but the total cost or energy used by the intruder to compromise the cluster nodes is the sum of the successful and failure attempts.

Energy Function



Theorem 3: In zero sum game, the energy used to defend a cluster is finite.

Proof: The total cost to defend a cluster C_c is the energy spent for successful attempts plus the energy spent for unsuccessful attempts. Therefore C_c is

$$C_c = \sum_{i=1}^{N} (\alpha E_c + \beta N_i)$$

$$C_c = \sum_{i-1}^{N} (\alpha (\sum_{j-1}^{m} P_{i,j}) + \beta N_i) \qquad \text{--- (8)}$$

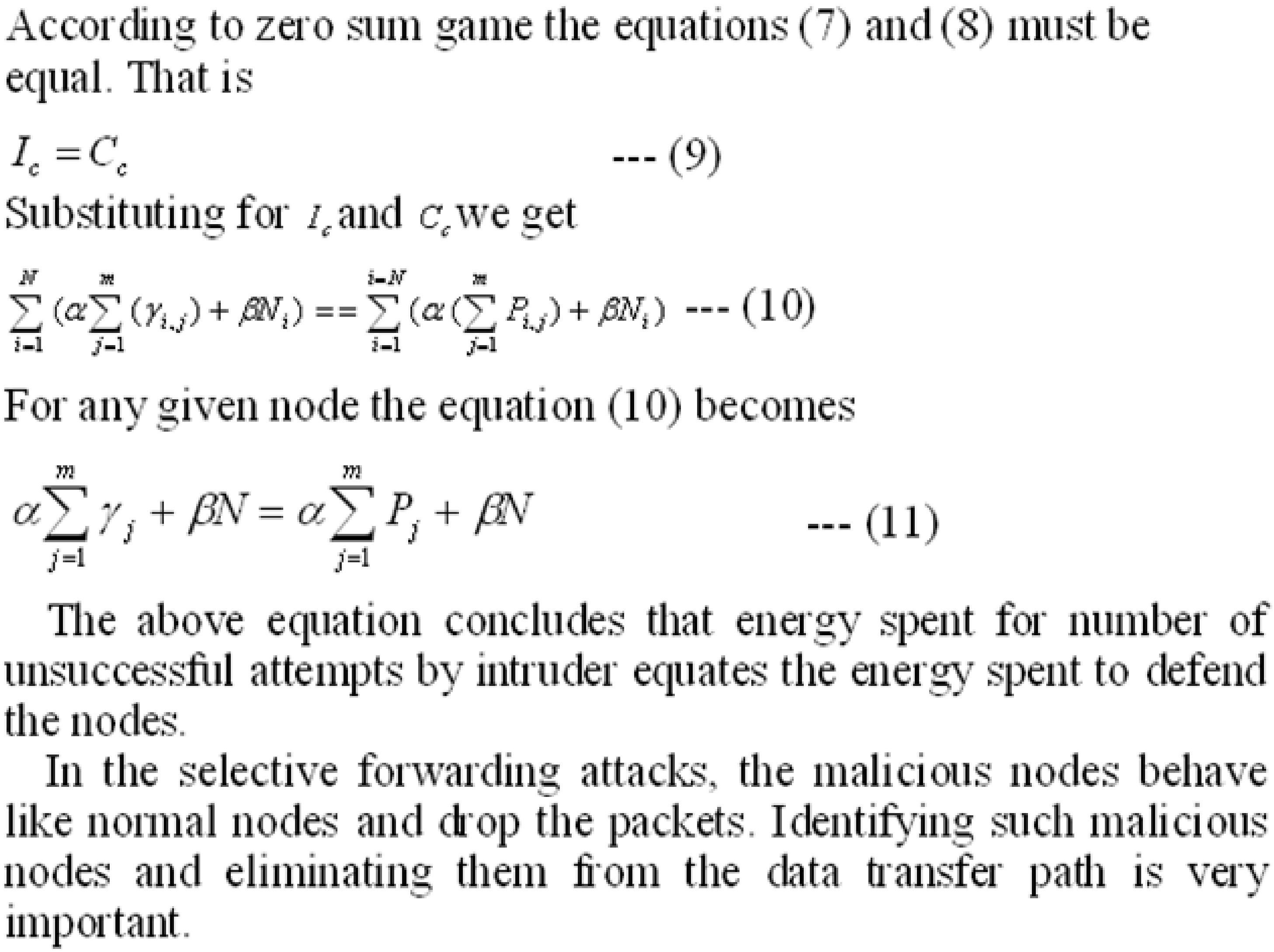
where $\sum_{j=1}^{m} P_{i,j}$ is the energy used to defend cluster nodes

βN_i is the energy to defend cluster head

E_c is the probability of defending a cluster (equation (2))

Since N is finite, $\alpha + \beta = 1$, the number of attempts by an intruder is finite, the energy spent by IDS to defend a cluster is also finite. This concludes the Theorem 3.

Energy Function



According to zero sum game the equations (7) and (8) must be equal. That is

$$I_c = C_c \qquad \text{--- (9)}$$

Substituting for I_c and C_c we get

$$\sum_{i=1}^{N}(\alpha\sum_{j=1}^{m}(\gamma_{i,j})+\beta N_i) == \sum_{i=1}^{i=N}(\alpha(\sum_{j=1}^{m}P_{i,j})+\beta N_i) \qquad \text{--- (10)}$$

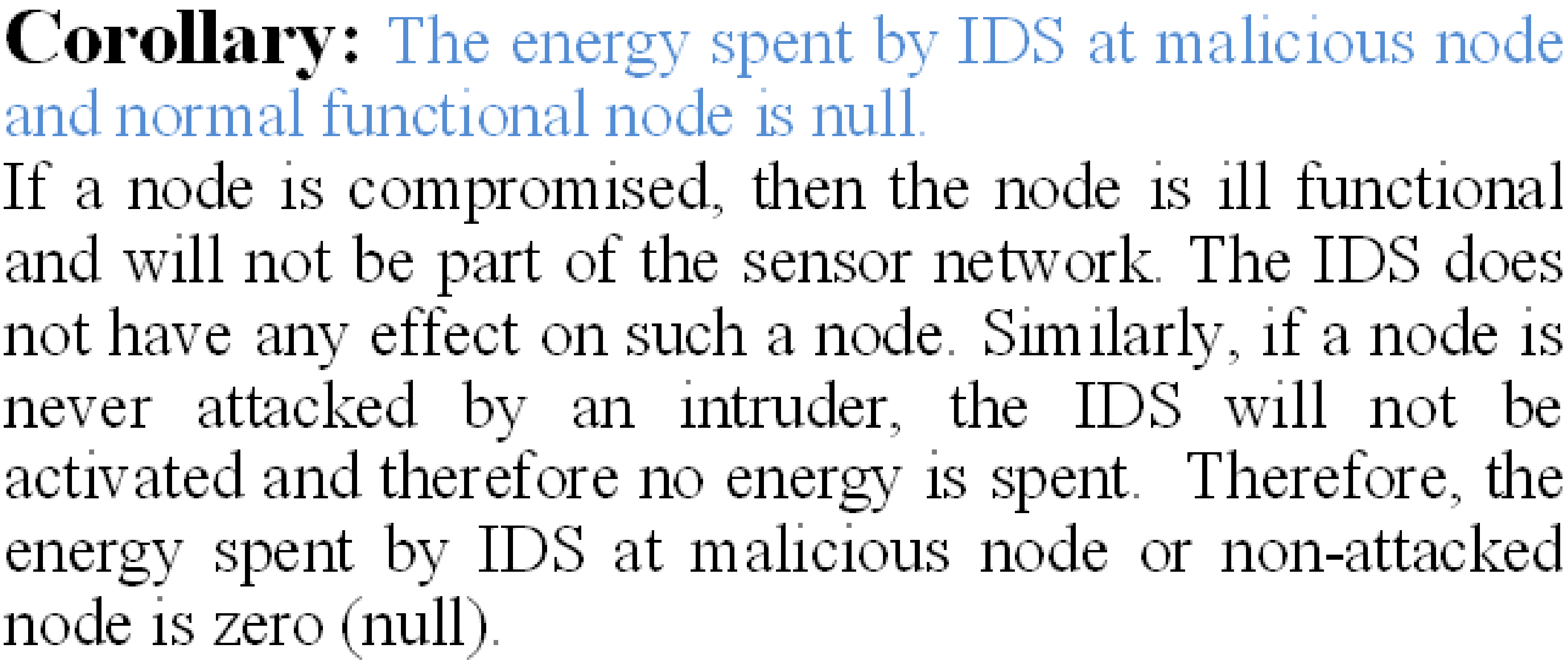
For any given node the equation (10) becomes

$$\alpha\sum_{j=1}^{m}\gamma_j + \beta N = \alpha\sum_{j=1}^{m}P_j + \beta N \qquad \text{--- (11)}$$

The above equation concludes that energy spent for number of unsuccessful attempts by intruder equates the energy spent to defend the nodes.

In the selective forwarding attacks, the malicious nodes behave like normal nodes and drop the packets. Identifying such malicious nodes and eliminating them from the data transfer path is very important.

Energy Function



Corollary: The energy spent by IDS at malicious node and normal functional node is null.

If a node is compromised, then the node is ill functional and will not be part of the sensor network. The IDS does not have any effect on such a node. Similarly, if a node is never attacked by an intruder, the IDS will not be activated and therefore no energy is spent. Therefore, the energy spent by IDS at malicious node or non-attacked node is zero (null).

Detection of malicious node

Consider the path SABCDEF→ BS in Figure 2, where D is a malicious node. Let A and E be the selected acknowledge points (ξ=2). The following are the possibilities:

- Any node in the path is malicious (compromised with an intruder)
- One or more of the nodes (for example B) are malicious (before or between the acknowledge points)
- Node A or node E is malicious (assume that selected acknowledgement points are not malicious)

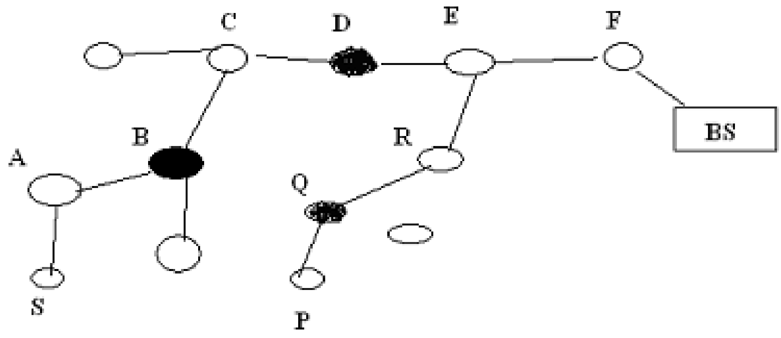


Figure 2. Multi-hop Acknowledgement

Detection of malicious node

Consider the path SABCDEF→ BS

There are n (7) nodes in a forwarding path, m (2) of which are malicious.

Let there be q (1) non-malicious nodes between any two malicious nodes.

Let ξ (2) be the number of selected acknowledgement points in the packet path and σ be the percent of nodes which are randomly selected as check points.

The probability of detecting a malicious node (P_d) is given by

$$P_d = P_k = 1 - P_{km} \qquad \text{--- (12)}$$

where

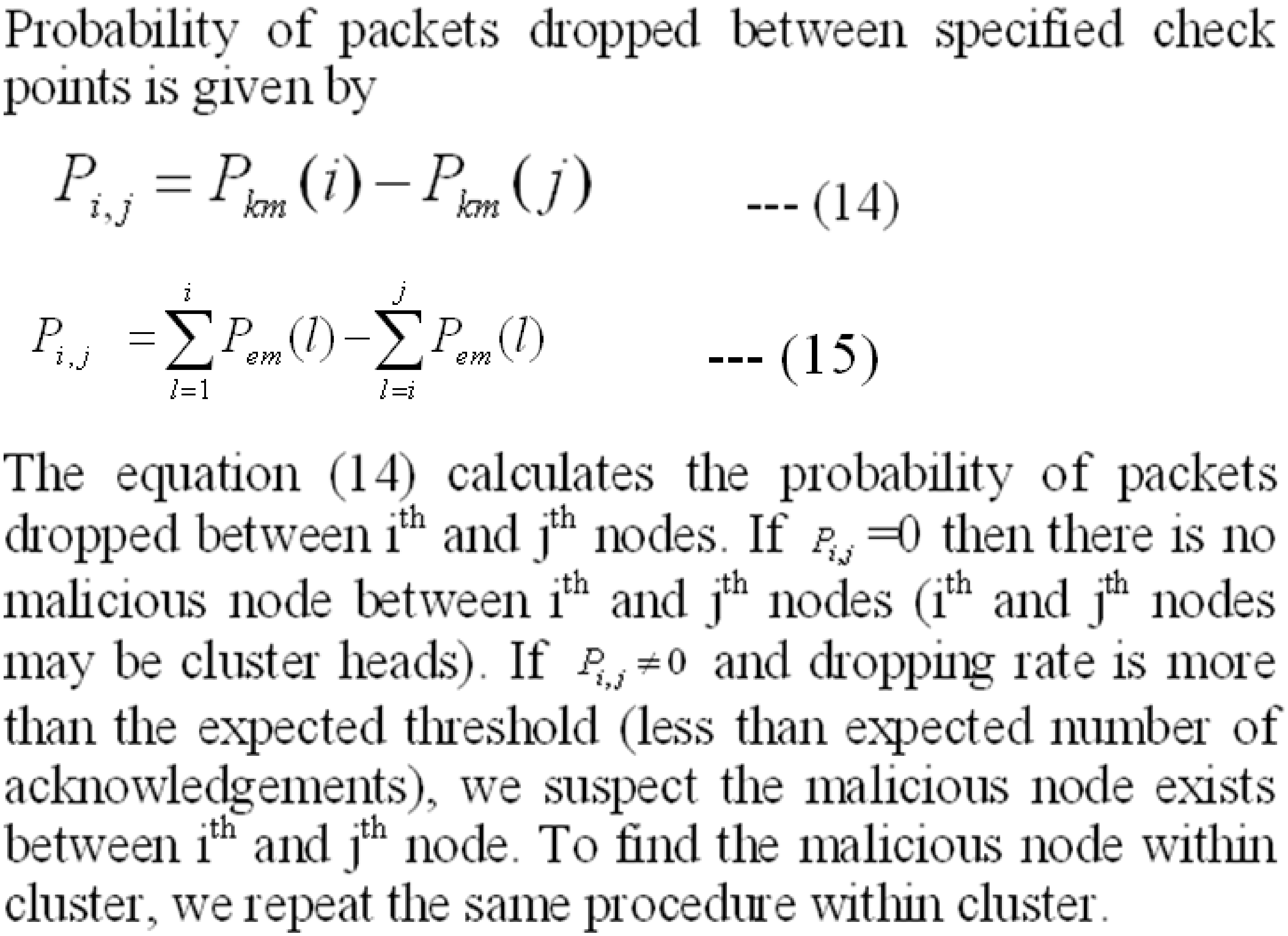
P_k Probability of packets dropped by selected acknowledgement points

P_{km} Probability of acknowledgements at the source by the selected points of acknowledgements

$$P_{km} = \sum_{i=1}^{m} P_{em}(i) \qquad \text{--- (13)}$$

$P_{em}(i)$ is the probability of packets dropped by all malicious nodes in the path

Packet Dropping Rate Between any two Nodes



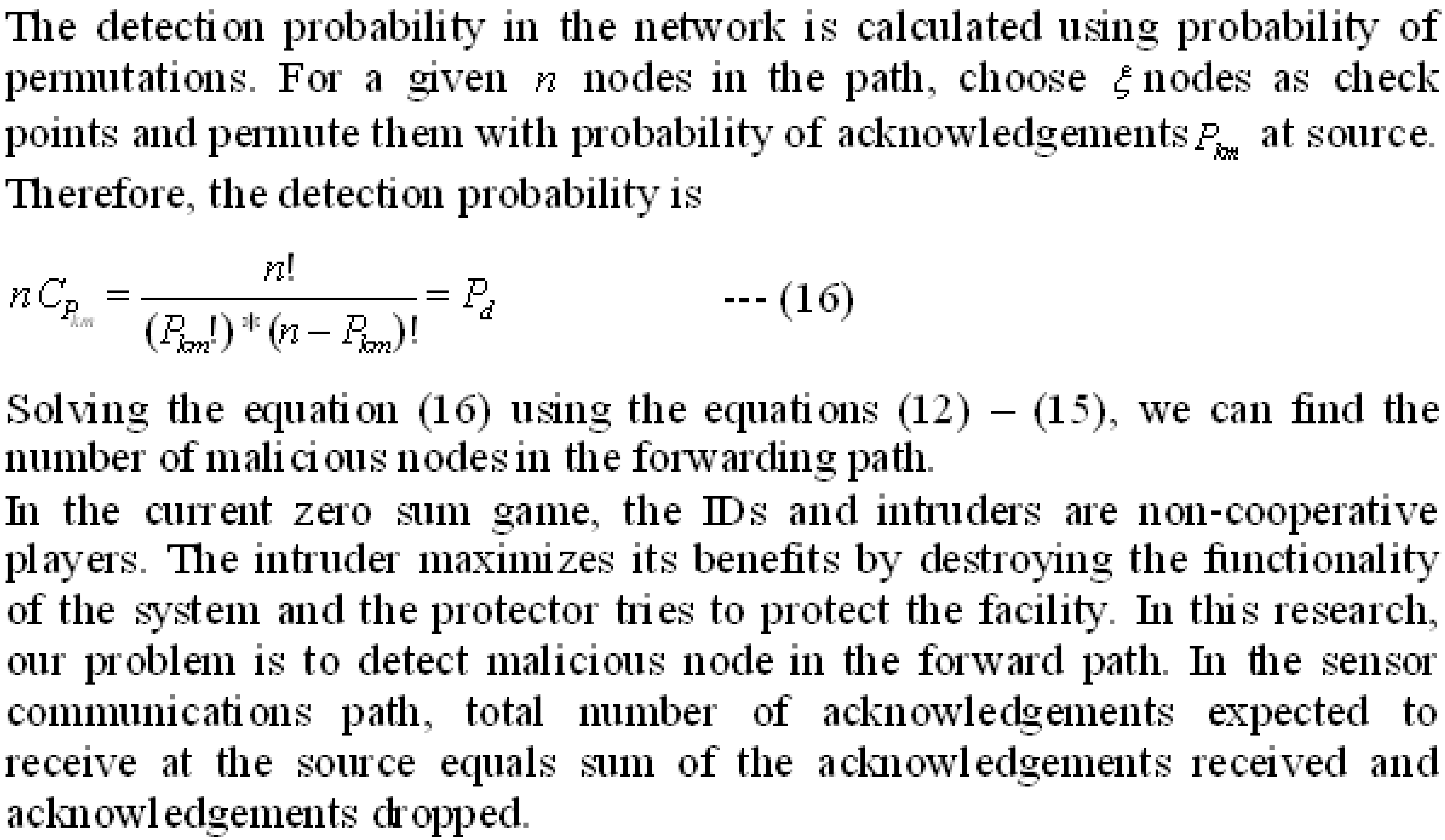
Probability of packets dropped between specified check points is given by

$$P_{i,j} = P_{km}(i) - P_{km}(j) \qquad \text{--- (14)}$$

$$P_{i,j} = \sum_{l=1}^{i} P_{em}(l) - \sum_{l=i}^{j} P_{em}(l) \qquad \text{--- (15)}$$

The equation (14) calculates the probability of packets dropped between i^th^ and j^th^ nodes. If $P_{i,j} = 0$ then there is no malicious node between ith and jth nodes (ith and jth nodes may be cluster heads). If $P_{i,j} \neq 0$ and dropping rate is more than the expected threshold (less than expected number of acknowledgements), we suspect the malicious node exists between ith and jth node. To find the malicious node within cluster, we repeat the same procedure within cluster.

Alternate calculation of Detection Probability



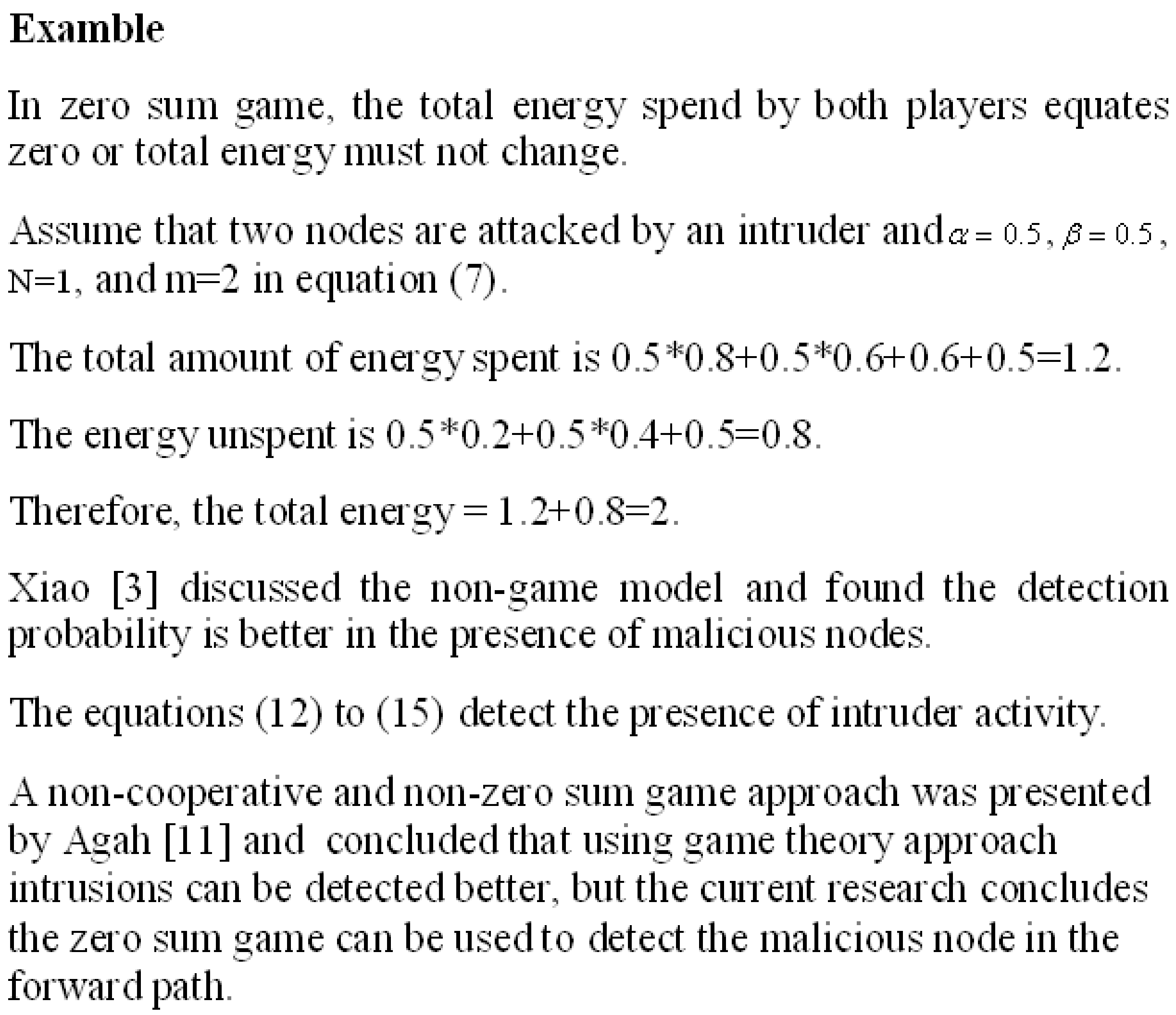
The detection probability in the network is calculated using probability of permutations. For a given n nodes in the path, choose ξ nodes as check points and permute them with probability of acknowledgements P_{km} at source. Therefore, the detection probability is

$$nC_{P_{km}} = \frac{n!}{(P_{km}!) * (n - P_{km})!} = P_d \qquad \text{--- (16)}$$

Solving the equation (16) using the equations (12) – (15), we can find the number of malicious nodes in the forwarding path.

In the current zero sum game, the IDs and intruders are non-cooperative players. The intruder maximizes its benefits by destroying the functionality of the system and the protector tries to protect the facility. In this research, our problem is to detect malicious node in the forward path. In the sensor communications path, total number of acknowledgements expected to receive at the source equals sum of the acknowledgements received and acknowledgements dropped.

Discussion of Results



Examble

In zero sum game, the total energy spend by both players equates zero or total energy must not change.

Assume that two nodes are attacked by an intruder and $\alpha = 0.5$, $\beta = 0.5$, N=1, and m=2 in equation (7).

The total amount of energy spent is 0.5*0.8+0.5*0.6+0.6+0.5=1.2.

The energy unspent is 0.5*0.2+0.5*0.4+0.5=0.8.

Therefore, the total energy = 1.2+0.8=2.

Xiao [3] discussed the non-game model and found the detection probability is better in the presence of malicious nodes.

The equations (12) to (15) detect the presence of intruder activity.

A non-cooperative and non-zero sum game approach was presented by Agah [11] and concluded that using game theory approach intrusions can be detected better, but the current research concludes the zero sum game can be used to detect the malicious node in the forward path.

Conclusions

- The presentation discusses various WSNs and attacks on WSN
- Discussed the currant state of the security models attack models
- Presented game theory basics and game model for detecting the malicious node
- Discussed the cost to defend the node and packet dropping rate at any node
- Future research includes collaborative game models and non-zero sum game models for detecting malicious nodes and sinkhole detection

Security Issues and models

Example 3

Trust Management System

- Useful for detecting a node which is not behaving as expected (either faulty or malicious)
- Attach trust value for each node (not in WSN)
- So, find the trust value using logical calculations
  - The calculations may be using: statistics, data value, intrusion detection, or personal detection of other nodes – not suggested in WSN

Therefore, Trust may be done by using Reputations

Current State of Trust Management System in WSN

1. Reputation-based Framework for High Integrity Sensor Networks- saurabh Ganeriwal and Mani B. Srivastava

   Proposed a system that maintains reputation for other nodes and use it to evaluate their trustworthiness. Currently developing beta reputation system (with Bayesian formulation) for reputation representation, updates and integration

2. Trust Management in Wireless sensor Networks – Mohammad Momani and Subhash Challa

   Trust between the nodes based on the sensed events (sensed continuous data of temperature). Used the beta reputations and used Bayesian probabilistic approach for mixing second hand information from neighboring nodes with directly observed information to calculate trust

None of these uses trust calculation of next node to send the data and compare the trust calculation of its neighboring nodes

Trust Management

- Helps to detect the node that selectively drops the packets
- Detects the Malicious node
- Selects the alternate path if successive node is not trusted

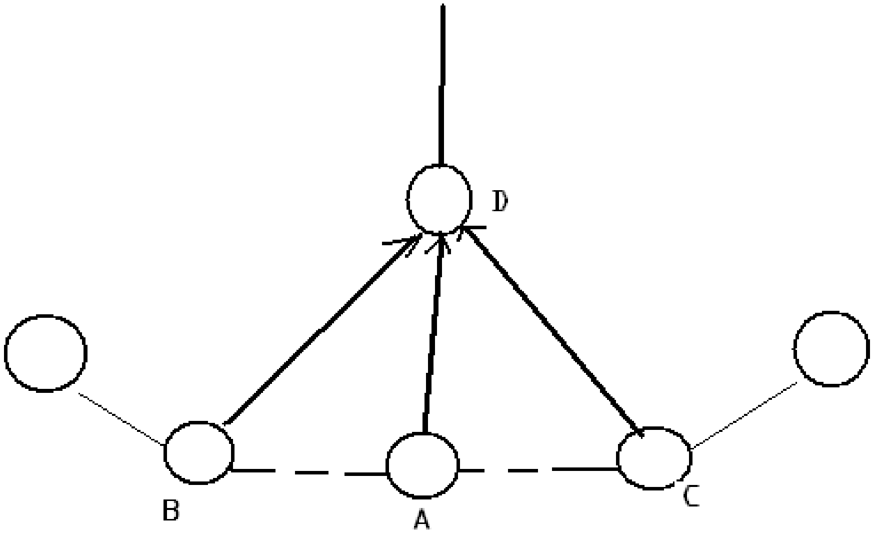


Figure 1: Scenario for node 'A' establishing trust of node 'D'

Game Model

- Interaction between the players is inherently dynamic
- Players always observe the actions of other players and decide optimal response
- In repeated games the decisions depend upon previous actions or conclusions of previous actions
- In Figure 1 the player 1 (node A) actions depend upon the Player 2 (node D)
- Cooperative effort we need to consider the outcome of neighboring players: for example player 3 and player 4 (within communication Distance of player 1 and common interaction with player 2)
- A strategy game is of the Form

$$G = (N, A, U) \qquad (1)$$

N – set of users;   A – set of actions;   U - payoff

Pay off verses dropping packets

If Ω is the common discount payoff and $g_i(a^t)$ is the per-period payoff of the ith node related to current action a^t, then the normalized payoff β (relation to utility of sequence $a^0, a^1, .., a^T$) at any node is given by [20]

$$\beta = \frac{1-\Omega}{1-\Omega^{T+1}} t \sum_{t=0}^{t=T} g_i(a^t) \qquad (2)$$

The trust of the player depends upon the outcome of β.

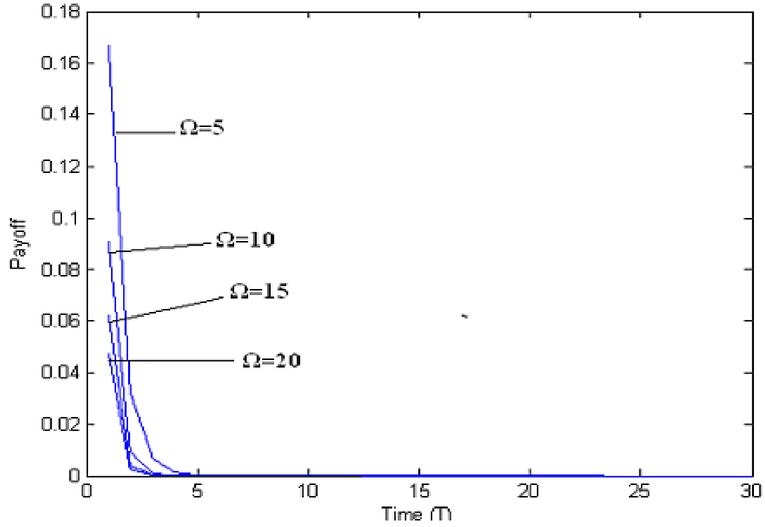
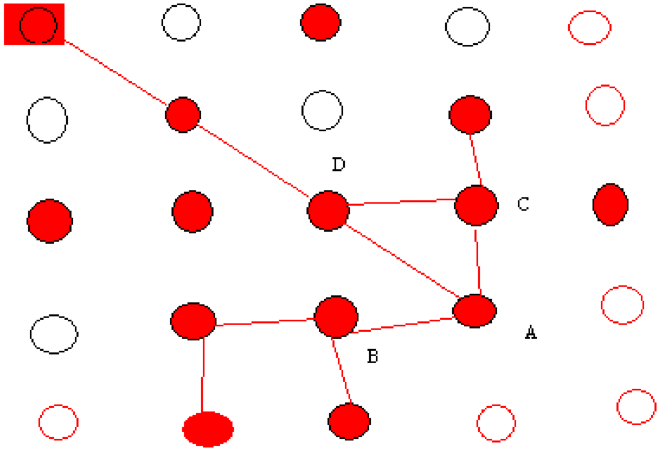


Figure 2. Payoff β verses packet dropping in a given time period

Sensor Network nodes and their relation with Neighboring Nodes

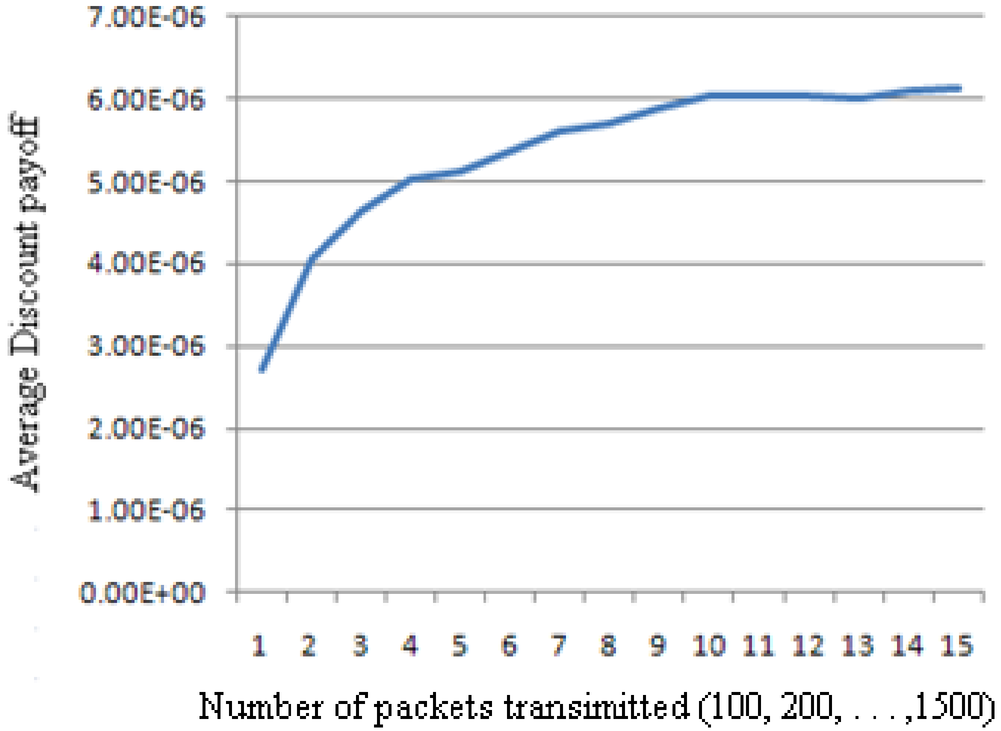
$$M = [M_{i,j}] = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 \end{bmatrix} \qquad (3)$$



Trust-based Packet Forwarding

- Reputation is used to predict the behavior of the node
- To predict the behavior of node 2, we created a table at **node 1** that over hears the packets transferred from node 2
- If node 2 is malicious then the node 1 finds the alternate route
- If node 2 is malicious then checks the neighboring nodes about the trust factor

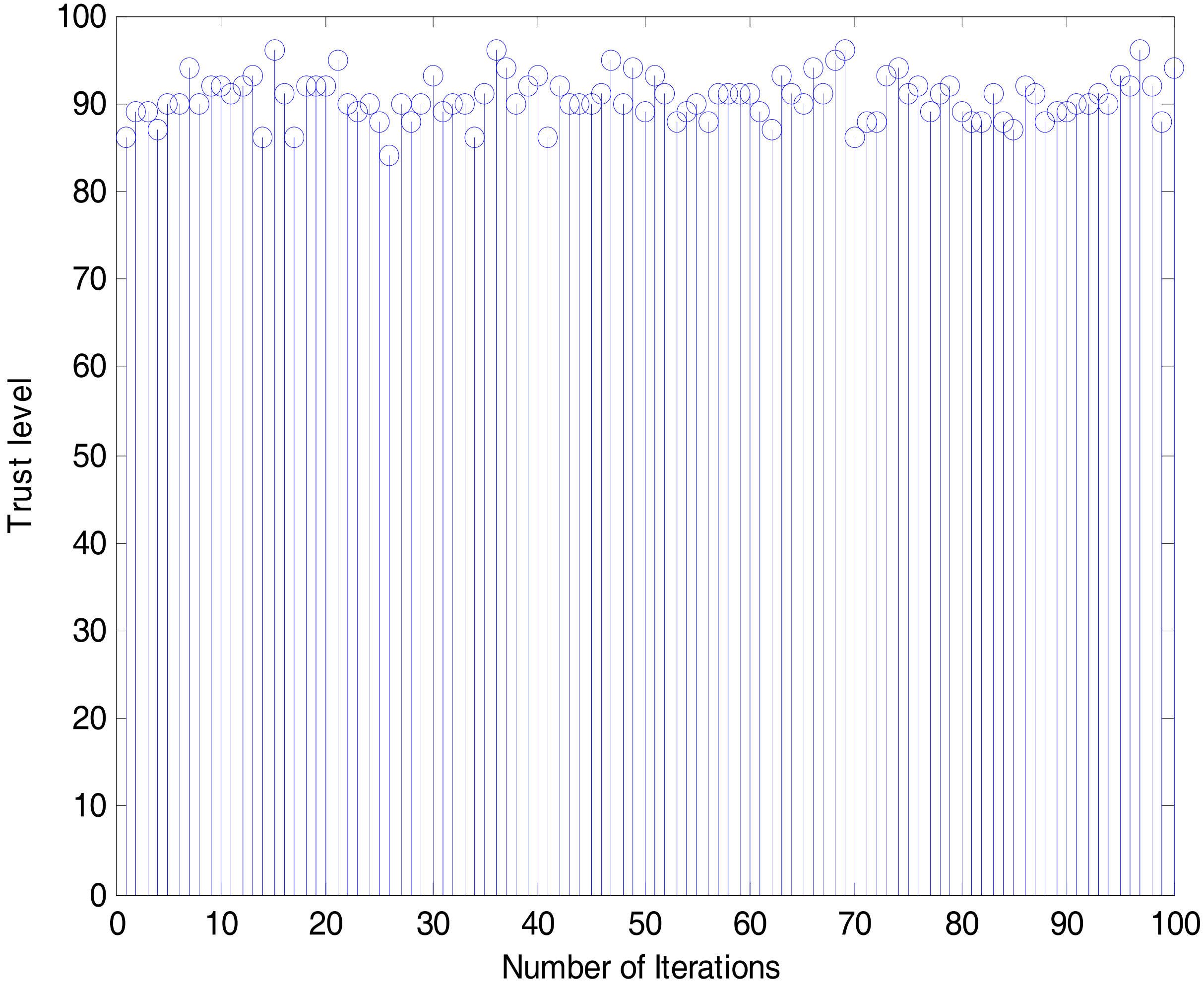
Average Discount Payoff vs number of Packets dropped



Trust Relation Generated in 100 iterations

- The process was repeated and the percentage of trust in hundred attempts is shown in Figure 5.
- The random generation of trust data is not a correct process but it helps in simulations.
- The average trust of a hundred samples in Figure 5 is approximately 90.42. T
- he average hundred samples each time is approximately 90.42.
- The threshold was set as 90 and above and satisfies the simulation results.
- Therefore, we can assume that if the transfer rate is above 90% the node can be truste

Trust Relation Generated in 100 iterations



Conclusions

- The current available research models deal with secure transfer of packets, intruder detection, sinkholes, and similar approaches.
- All these methods need a lot of processing, storage, and energy.
- There is no literature available for a simple security model for wireless sensor networks that confirms the successive node to transfer the packets.
- The proposed model is a unique approach to transfer the data securely and at the same time confirms the trust of next level nodes.

Future Directions

- What happens if an intruder at successive node level acts as a real node and acknowledges to the preceding node with 100% success of packet transfer and then transfers the packets to the sinkhole?
  - *This problem was solved using the NS2 package by creating a table at the previous node and observing the successive node. The experiment will be useful for detecting the sinkhole. The results will be presented in the next conference.*
- What happens if the intruder modifies the packets and forwards them to the next level and then these corrupted packets reach the destination?
  - *This is an open problem and will be attempted and solved soon.*
- What happens if the intruder stores the packet forwarding table appropriately (as the preceding node requires for successful transformation) and never forwards the packets (acts as an intelligent sinkhole).
  - *This problem will be solved with (a) before we publish the results.*

Security Issues and models

Future Research

Automatic Trust-based approach

Security Issues and models

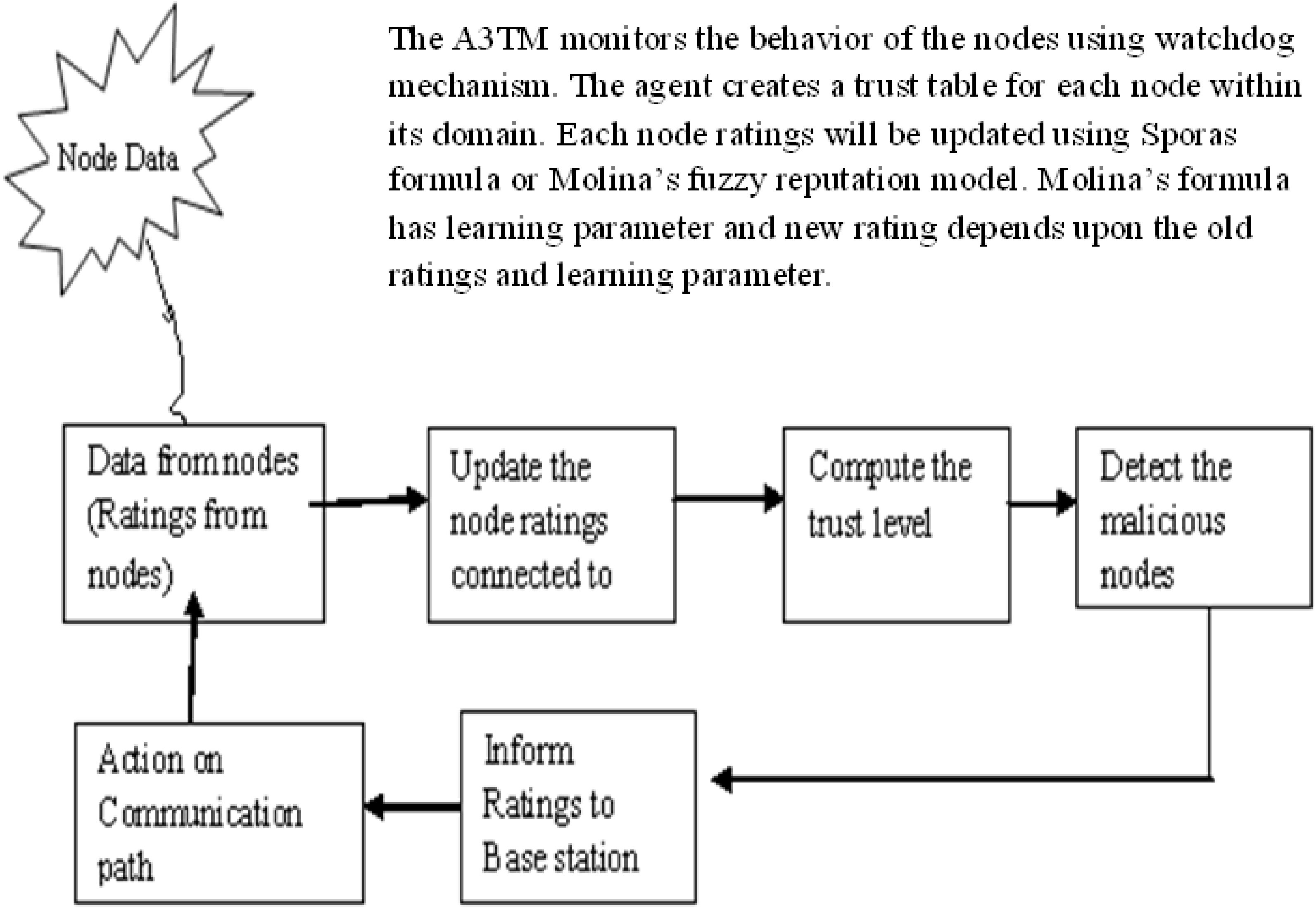
New Model:

Adoptable automatic agent-based trust model (A3TM) that detects the intentional and malicious acts of the intruder

- The repeated actions of each node will be rated by the node transferring the packets. Each node maintains the ratings and updates its ratings.
- each node in the WSN belongs to a cluster.
- The data of each node that belongs to the cluster will be maintained by the cluster agent.
- the nodes are relieved from processing and maintaining of the information.
- An adaptable automatic system (agent-based trust model) requires learning component

Security Issues in WSN
A3TM Model

The A3TM monitors the behavior of the nodes using watchdog mechanism. The agent creates a trust table for each node within its domain. Each node ratings will be updated using Sporas formula or Molina's fuzzy reputation model. Molina's formula has learning parameter and new rating depends upon the old ratings and learning parameter.


Node Data
Data from nodes (Ratings from nodes)
Update the node ratings connected to
Compute the trust level
Detect the malicious nodes
Inform Ratings to Base station
Action on Communication path

Security Issues in WSN
Mechanism

The watchdog mechanism collects the data (node ratings) from nodes and provides the agent. The agent takes the external ratings and feedback from system computations. The data collection depends upon an event triggers or presets widow time. The node below trust level will be informed to the base station. The base station decides to delete the node from communication path or continue.

Functions:

Security Issues in WSN
Functions

Data from nodes (Ratings from nodes): The reward or punishment (increment or decrement) of the ratings of every node using Sporas formula is available to the agent. The information of each node will be recorded when an event triggers or at a fixed window time. This watch dog mechanism collects the current data.

Update the node ratings connected to Agent: The current ratings will be updated at this station. It checks the current ratings of each node. If the ratings of a node fall below the threshold, it tags the node.

Compute the trust level: The trust level of suspicious node will be calculated. The tagged node will be verified with neighbors using collaborative mechanism and provides information to the next level.

Detect the malicious nodes: The trust level will be compared with the threshold value and decides the node is malicious or under suspension. The decision will be informed to the next level.

Inform Ratings to Base station: The decision and ratings of the nodes will be informed to the base station. The base station then recommends the further action.

Action on Communication path: With the recommendation of base station, it takes the appropriate action (keep the node or discord) and informs to the station ‘Data from nodes’. The action (keep the node or discord) must be informed to the Data from nodes because the update of discarded node no longer needed.

The process will continue automatically. The previous information of nodes is stored and updated in each interval. The new ratings of the nodes depend upon the previous ratings and ratings of neighbor nodes.

Security Issues in WSN
Conclusions

- Introduced the Wireless Sensor Network and topology
- Various applications, protocols, and threats were discussed
- Security Issues and approaches to solve
- Examples
  - Forward attack
  - Game model
  - Trust-based model
- Future researach

Security Issues in WSN References

Y. B. Reddy and R. Selmic., “Agent-based Trust calculation in Wireless Sensor Networks” SENSORCOMM 2011, August 21-27, 2011.

Y. B. Reddy and R. Selmic., “Cooperative and Collaborative Approach for Secure Packet Transfer in Wireless Sensor Networks” SENSORCOMM 2011, August 21-27, 2011.

Y. B. Reddy and S. Kafle., “Protecting data from unauthorized users using Honeypots Technique”, CSOC 2011, January 24-31, 2011

Y. B. Reddy and R. Selmic., “Secure Packet Transfer in Wireless Sensor Networks – A Trust-based Approach”, IARIA- ICN 2011, January 23-28, 2011 - St. Maarten.

Y. B. Reddy and R. Selmic., “Trust-based Packet Transfer in Wireless Sensor Networks”, Communications and Information Security (CIS2010), IASTED, Nov 8-10, 2010,USA

Y. B. Reddy., J. Durand, and Sanjeev Kafle., “Detection of Packet Dropping in Wireless Sensor Networks”, ITNG 2010

Y. B. Reddy., “Potential Game Model to Detect Holes in Sensor Networks”, IFIP/NTMS 2009

Y. B. Reddy, “Detecting Sinkhole Attack by Observing the Quality of Link in Wireless Sensor Networks”, ICWN’09 - The 2009 International Conference on Wireless Networks, July 13-16, Las Vegas.

Y. B. Reddy and S. Srivathsan, “Game Theory Model for Selective Forward Attacks In Wireless Sensor Networks”, 17th Mediterranean Conference on Control and Automat, Gr-54640, June 24-26, 2009.

Y. B. Reddy, “A Game Theory Approach to Detect Malicious Nodes in Wireless Sensor Networks”, SENSORCOM09, Athens, Greece.

D. Abreu., P. Dutta., and L. Smith., “The Folk Theorem for Repeated Games: A NEU Condition”, *Econometrica*, vol. 62, 1996.

J. Audun., R. Ismail., and C. Boyd., “A survey of Trust and Reputation Systems for Online Service Provision”, *Decision Support Systems*, 2006.

M. Fernandez-Gago., R. Roman., J. Lopaz., “A Survey on the Applicability of Trust Management Systems for Wireless Sensor Networks”, *3rd International Workshop on Security, Privacy, and Trust in Parvasive and Ubiquitous Computing*, July 2007.

J. Hur., Y. Lee., S. Hong., and H. Yoon., “Trust-based secure aggregation in Wireless Sensor Networks”, *Sensor and Ad Hoc Communications and Networks (SECON '06)*, 2006.

Z. Ji., W. Yu., and K. J. Liu, K., “Belief-based Packet Forwarding in Self-organized Mobile Ad Hoc Networks with Noise and Imperfect Observation”, *IEEE WCNC* 2006.

R. Kannan. and S. S. Iyengar., “Game-theoretic models for reliable path-length and energy-constrained routing with data aggregation in wireless sensor networks”, *IEEE J. of Selected Areas in Communications*, Aug 2004.

R. Machado., and S. Tekinay., “A survey of game-theoretic approaches in wireless sensor networks”, *Computer Networks*, Nov. 2008.

M. Momani., and S. Challa., “Trust management in Wireless Sensor Networks”, *5th IEEE/ACM Int. Conf. on Hardware/Software Codes and System Synthesis*, 2007.

Y. Rebahi., V. Mujica., and D. Sisalem., “A Reputation-Based Trust Mechanism for Ad Hoc Networks”, *the 10th IEEE Symposium on Computers and Communications (ISCC’05)*, 2005.

S. Tanachaiwiwat., P. Dave., R. Bhindwale., A. Helmy., “Location-centric Isolation of Misbehavior and Trust Routing in Energy-constrained Sensor Networks”, *IEEE IPCC*, October 2004.

B. Xiao., B. Yu., C. Gao., “CHEMAS: Identify Suspect Nodes in Selective Forwarding Attacks”, Journal of Parallel Distributed Computing, vol. 67, 2007.

Acknowledgement

I wish to express appreciation to Dr. Connie Walton, Provost & Vice President for Academic Affairs, Grambling State University for her continuous support.