Security Issues in Nanoscale Communication Networks

Vasos Vassiliou
Department of Computer Science
University of Cyprus

3rd NaNoNetworking Summit, Barcelona, Spain, June 22-23 2011

Outline

- Position Statement
- Introduction
- Nanonetwork Applications and Security Concerns
- Computer and Nano-Network Immunology
- Conclusion

Position Statement

- Security from the start !

- It is essential that early nano-scale communication networks include security features, even if those features stretch the capabilities of such devices

- *"I will not now discuss how we are going to do it, but only what is needed in principle – in other words, what is needed according to the laws of computing and networking."*

Nano-Network Applications

Nano Network Characteristics

- □ Nano-machine as "a device, consisting of nano-scale components, able to perform a specific task at nano-level, such as communicating, computing, data storing, sensing and/or actuation". [Akyildiz et al., ComNet 2008]
- □ Creating multifunctional complex nano-nodes is not an option
- □ Complex task handling will be enabled only by communication of nano-machines and the creation of nano-networks

Nano Network Characteristics

- □ Nano networks will enable the interaction with remote nano-machines by means of broadcasting and multihop communication mechanisms. [Akyildiz et al., ComNet 2008]
- □ Nano networks will provide intra-body communication of nano-machines and also interface with the outside world [Akyildiz et al., J-WC 2010]

Nano Network Limitations

- Energy is a constraint as with every miniature devices
- Source and channel coding as well as cryptography require computational overhead which:
  - grows very rapidly with the large scale of nano-devices in a network
  - is difficult at the nanoscale because there is limited processing that can be packed into small volumes.

Nano-Network Applications (i)

- Bio-Medical [Akyildiz et al., ComNet 2008, NanoCom 2010]
  - Immune system support: identify/detect and control/eliminate foreign and pathogen elements, such as cancer cells
  - Bio-hybrid implants: Provide interfaces between the implant (organs, nervous tracks or lost tissues) and the environment.
  - Drug delivery systems: support substance regulating mechanisms or deliver neurotransmitters or specific drugs.
  - Health monitoring: Use of inbody nano-sensor networks to monitor oxygen, hormones, etc. The information retrieved by these systems must be accessible by relevant actors.
  - Genetic engineering: Manipulation and modification of nano-structures such as molecular sequences and genes can be achieved by nano-machines.

Nano-Network Applications (ii)

- Industrial applications
  - Food and water quality control: detect very small amounts of bacteria, chemical, biological agents, and toxic components
  - Functionalized materials and fabrics: Antimicrobial and stain-repeller textiles. Nano-actuators to improve the airflow in smart fabrics.
  - Wearhousing and product monitoring: Nano-sensor networks can be deployed into cargo containers to detect the unauthorized entrance of chemical, biological or radiological materials.

Nano-Network Applications (iii)

- Person-centric Applications
  - Ultrahigh sensitivity touch surfaces: physical nanosensors can be used in a distributed manner to develop touch surfaces with high sensitivity and precision.
  - Haptic interfaces: haptic technology interfaces with the user by the sense of touch. Physical nanosensors and nanoactuators can be used to enhance remote controls of complex machinery, amongst others.
  - Future interconnected office: the interconnection of nanosensor and nanoactuator devices with existing communication networks

Nano-Network Applications (iv)

- Military applications
  - Nuclear, biological and chemical (NBC) defenses: nanonetworks deployed over the battlefield or targeted areas to detect aggressive chemical and biological agents and coordinate the defensive response
  - Nano-functionalized equipment: advanced camouflage and army uniforms can take advantage of nanonetworks to monitor and control temperature signatures
  - Damage detection systems: physical nanosensors can be used to detect very small cracks in textiles, civil structures, vehicles and even rockets.

Nano-Network Applications (v)

- Environmental applications
  - Biodegradation: sense and tag different materials that can be later located and processed by smart nano-actuators.
  - Animals and biodiversity control: nanonetworks using pheromones as messages can trigger certain behaviors on animals and interact and control their presence in particular areas.
  - Air pollution control: nano-filters can be developed to improve the air quality by removing harmful substances
  - Plant monitoring systems: monitor and/or release chemical composites related to predator defenses or pollinating

Nano-Network Security Issues

Security – Objectives

- Availability:
  - Services are available
- Authorization:
  - Only authorized members can provide information to the network
- Authentication:
  - Ensure that communication between nodes is genuine. Malicious nodes can not masquerade as genuine
- Confidentiality:
  - Only desired recipients can understand a given message
- Integrity:
  - Ensure that a malicious intruder did not modify the message

Security – Objectives

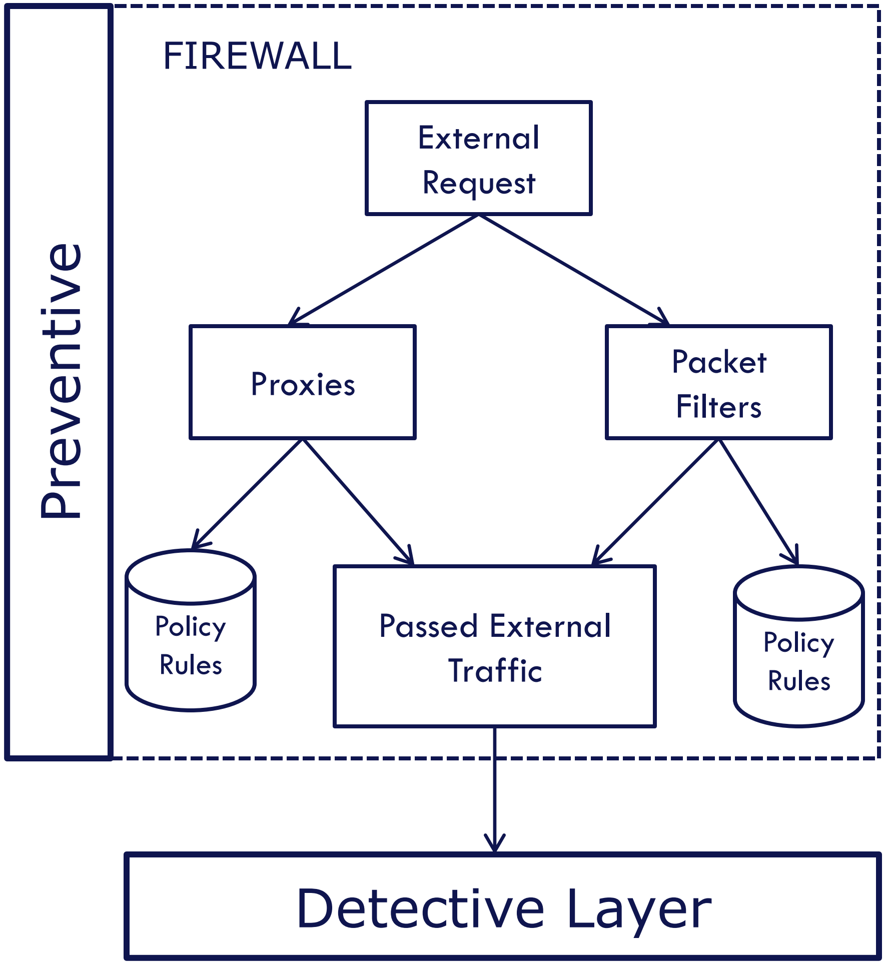
- Non-repudiation:
  - Denotes that a node can not deny sending a message
- Freshness:
  - Implies that the data is recent and ensures that no adversary can replay old messages
- As new nodes are deployed and old sensors fail, then consider:
  - Forward secrecy:
    - A node must not read any future messages after it leaves the network
  - Backward secrecy:
    - A joining node must not read any previously transmitted messages

Security – General Infrastructure

University of Cyprus

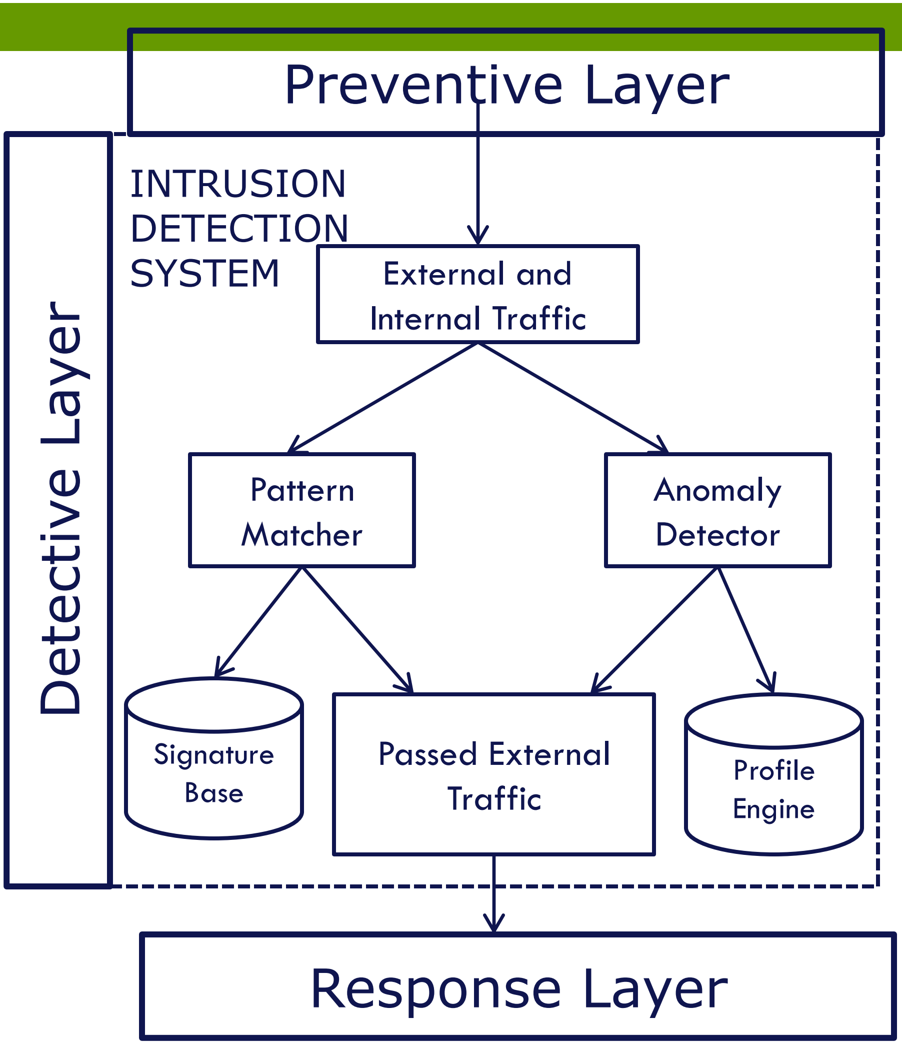
NETwork REsearch Laboratory

- **Preventive Layer**
  - It uses firewalls to prevent any external traffic that does not meet the entry criteria from entering the network (or to prevent external traffic meeting non-entry criteria from entering the network)
- Detective Layer
- Response Layer



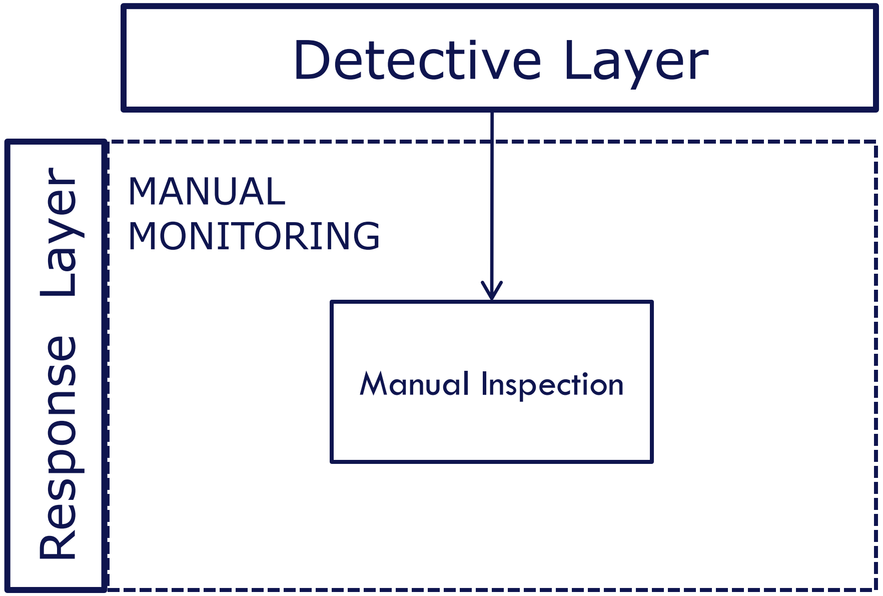
Security – General Infrastructure

- Preventive Layer
- **Detective Layer**
  - After the packets enter the network they are examined under two methodologies that seek to find out if the packets were invoked by malicious code or if they carry malicious code
  - Pattern Detector: known attacks
  - Anomaly Detector: novel attacks
- Response Layer



Security – General Infrastructure

- □ Preventive Layer
- □ Detective Layer
- □ **Response Layer**
  - 1. Coordinated by analyst
  - 2. Examine audit trails to determine if the alerts are valid
  - 3. If there is indeed an attack in the network, try to categorize the attack, explore the damage, and take appropriate corrective measures to remove it



Security

- Nano Technology’s foundation should incorporate techniques to increase security at an early stage
  - Embedded security techniques for data integrity, confidentiality, and availability are necessary

- Passive or Active Attacks
  - Passive:
    - Eavesdropping (invasion of Privacy)
    - Traffic Analysis
  - Active Attacks:
    - Denial of Service Attacks (DoS)
    - Data Manipulation (Tampering)
    - Masquerade
    - Replay

Security – Threats

Network Layers and Attacks		
Network Layer	**Attacks**	**Defenses Solutions**
Physical	Jamming	Region mapping etc
	Tampering	Hiding
Link	Collision	Error Correction Code
	Exhaustion	Rate Limitation
	Unfairness	Small frames
Network and Routing	Neglect and Greed	Redundancy, Probing
	Homing	Encryption
	Misdirection	Authorization
	Black holes	Authorization
Transport	Flooding	Client Puzzles
	Desynchronization	Authentication

Threats and Attacks (i)

- Denial of Service Attacks (DoS).
  - DoS attack is any event that diminishes or eliminates a network’s capacity to perform its expected function
- Tampering
  - Tampering refers to the physical tamper of nodes within the network for investigation, and to compromise it
- Selective Forwarding
  - A malicious node may refuse to forward every message it gets, acting as blackhole or it can forward some messages to the wrong receiver and simply drop others.

Threats and Attacks (ii)

- Spoofed, altered, or replayed information
  - While sending the data, the information in transit may be altered, spoofed, replayed, or destroyed. Since sensor nodes usually have only short range transmission, an attacker with high processing power and larger communication range could attack several sensors simultaneously and modify the transmitted information.

Threats and Attacks (iii)

- **Sinkhole attacks**
  - The attacker aims to attract all the traffic. Especially, in the case of a flooding based protocol, the malicious node may listen to requests for routes, and then reply to the requesting node with messages containing a bogus route with the shortest path to the requested destination.
- **Sybil attacks**
  - The compromised node presents itself as multiple nodes. This type of attack tries to degrade the usage and the efficiency of the distributed algorithms that are used. Sybil attacks can be performed against distributed storage, routing, data aggregation, voting, fair resource allocation, and misbehavior detection.

Threats and Attacks (iv)

- **Wormholes**
  - The malicious node tunnels messages from one part of the network over a link, that doesn’t exist normally, to another part of the network. The simplest form of the wormhole attack is to convince two nodes that they are neighbors.
- **HELLO flood attacks**
  - This attack is based on the use by many protocols of broadcast Hello messages to announce them in the network. So an attacker with greater range of transmission may send many Hello messages to a large number of nodes in a big area of the network. These nodes are then convinced that the attacker is their neighbor. Consequently the network is left in a state of confusion

Nano Network-specific Attacks

- The medium and scale lend themselves to exploitation:
  - real viruses in biological systems may compromise a molecular communication system
  - eavesdropping may occur by tapping into nanoscale networks with the attacker’s network sensors at the same scale
  - denial of service may be accomplished by flooding nanoscale networks with small physical matter
  - careful and controlled induced faults in the physical nature of the nanoscale network in order to discreetly corrupt the integrity of the information.

[Bush, NYS CSC 2008]

Nano Network-specific Attacks

- Wet/Fluidic Medium physical attacks
  - Encoding and decoding need to be unique for each Nano-Network as intruders may eavesdrop

    [Pierobon, J-SAC 2010][Suda, GECCO 2005]
  - Sender may emit ligands (create connection) to malicious nano-nodes, same applies for gab junctions

    [Suda, GECCO 2005]
  - Signal Propagation may result in unreliable data by nature and/or by malicious intent

    [Pierobon, J-SAC 2010]

Physical Attacks

- Deployment of Nano-Networks
  - Physically tampering with the network
- Communication frequency
  - Need to be aware of jamming attacks, i.e. distortion of frequencies!
  - Increase spreading loss and absorption loss
  - Increase noise

Information Privacy

- Eavesdropping/Invasion of Privacy
  - Energy limitation for nano-nodes can be a possible security breach
  - Encryption of data may be of challenge
  - Malicious nodes may intercept communication channel to "listen" to transmitted messages.
  - Information Modulation
    - Pulse Rate communication
      - Injection of misleading pulse rates for rerouting or energy depletion
      - Flooding the network with unnecessary pulses (ie. Replay and Hello attacks)

Protocols and Security

- Security in protocols
  - Addressing of nano nodes can be crucial in maintaining a secure nanonetwork.
    - Disguise as benign nano-node using a valid id
    - Security methods in WSN exist i.e. knowledge of neighborhood nano-nodes, but in NN it can diminish its lifetime
  - Information Routing
    - Dispose of ACK messages,
    - Rerouting messages to the malicious node ie. Black hole attack

Security breach scenario

- Heart monitor application
  - Monitor of heart ie. heartbeat
- Nano-nodes at points of interest
- Data transmission
  - Specific intervals
  - Event based

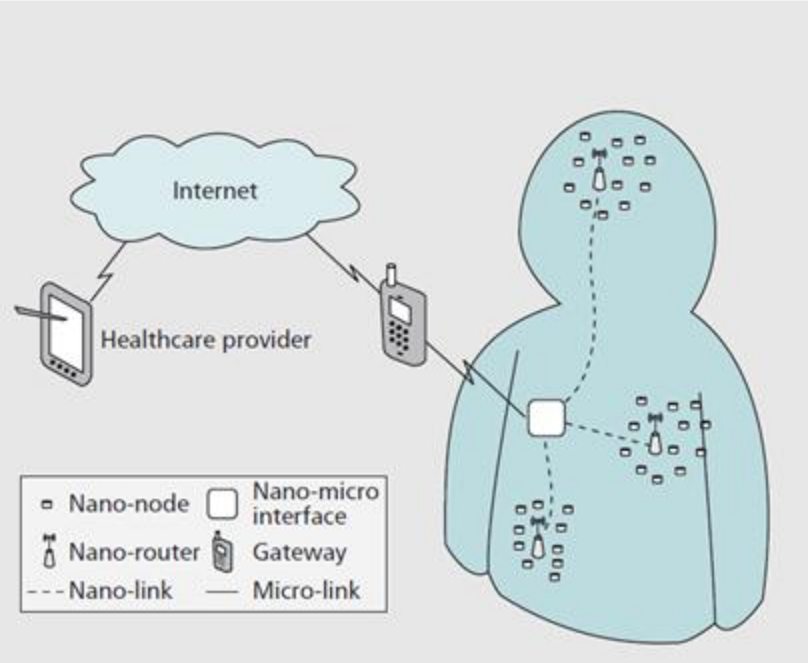


Fig. Source: Akyildiz et al., J-WC 2010

Security breach scenario

- Communication
  - Molecular communication
    - Molecular transport in fluid medium
      - Nano-devices encode data as DNA biomolecules [ref]
  - Data integrity, confidentiality, availability
      - Natural intervention: bacteria
      - Malicious intervention
        - Misguided information
        - Invasion of privacy
        - Denial of Service attack

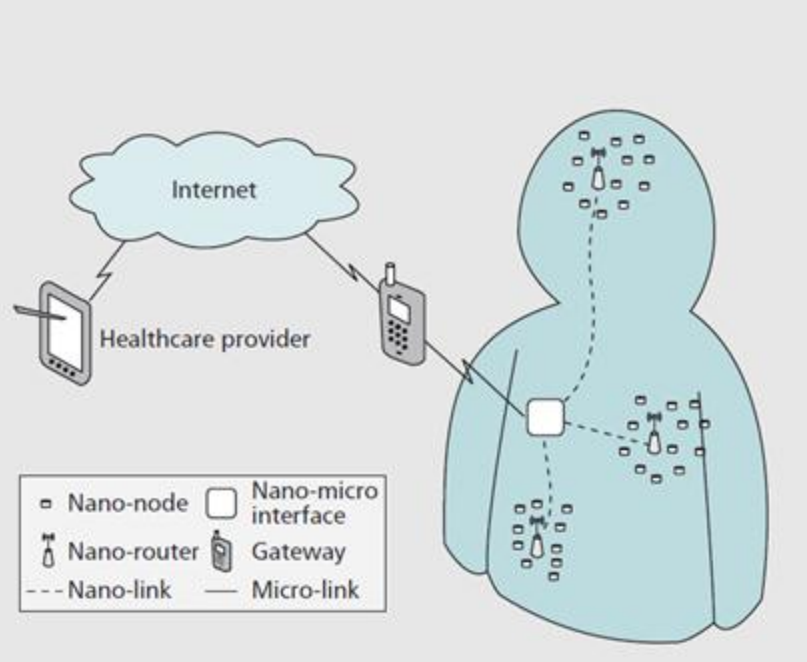
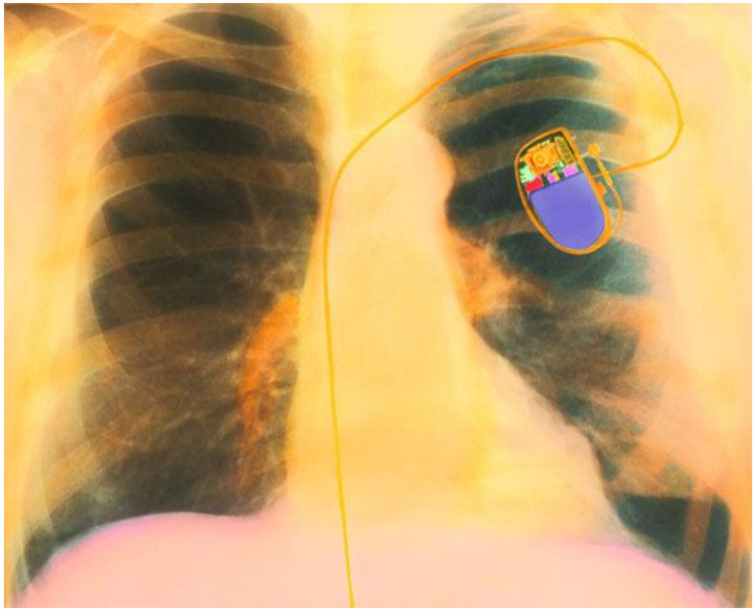


Fig. Source: Akyildiz et al., J-WC 2010

Wear a jammer to stop your pacemaker being hacked

- Hacking seems to be everywhere these days. But what if someone tried to retrieve data from your pacemaker? Or even tried to give you an electric shock with it?
- Solution: a jammer that can be worn. The jammer prevents anything from transmitting to the medical device unless it gives the right password or code.



Source: *New Scientist, One Per Cent Blog, June 17 2011*

Issues of Privacy

- Clear picture of the impact of nanotechnology on privacy
- People will knowingly or unknowingly carry around everyday objects which are tagged
  - ranging from clothing to watches, mobile phones, chip cards, identity documents, bank notes, or jewelry.
- The tags can all be read and uniquely identified from a distance by readers which may be hidden or not in the line of sight.
- This will make objects, and the people carrying or accompanying them, traceable.

Computer and NanoNetwork Immunology

Intrusion Detection System (IDS) – Definition

- Intrusion Detection Systems are protocol independent systems that are specific for a particular application, and are able to detect specific attacks without consuming excessive amounts of energy or memory
  - Pattern Detectors
    - Detect known attacks through the use of databases
    - Requires memory which a limitation in sensor nodes
  - Anomaly Detectors
    - Detection of novel attacks – any abnormalities in the network are classified as malicious
    - Requires profiling

Intrusion Detection System (IDS) – Objectives

- OBSERVE
  - Application transactions, message frequency
- ORIENT
  - Learn from new attacks (dynamically adapt)
- DECIDE
  - Whether transaction is malicious or not
- ACT
  - Serve or deny transaction (with or without human intervention)

Computer Immunology- Objective

- The Human Immune System (HIS) is the oldest “security” system in the world.
- The HIS characteristics can give insights on preventing and/or detecting novel malicious attacks
- The main characteristics are
  - Self and Non-Self
  - Multi-layered
  - Distributed Detection System
  - Unique Immune System
  - Creating antibodies
  - Imperfect Detection

Computer Immunology-
Self and Non-Self

- A human body's ability is to distinguish between
  - "self" – cells that are normal and healthy and
  - "non-self" – any foreign object that does not belong to "self"

Wired Networks

- Defining "self" and "non-self" varies between Intrusion Detection System (IDS) vendors
  - combination of: network traffic, system calls

Wireless Sensor Networks

- Define self based on a set of MAC and Routing packets.
- Time between the reception of two consecutive messages, packet retransmission (time and occurrence), message payload, packet repetition, transmission range, number of collisions

Computer Immunology – Multiple layers

- Physiological structure of a human body is constructed to prohibit any non-self objects from entering:
  - Passive barriers –skin
  - Generalized inflammatory responses, and
  - Adaptive responses

Wired Networks

Networks include :

- Preventive Layer – Firewall
- Detective Layer – IDS
- Response – Manual Monitoring

Wireless Sensor Networks

- Applying security at each network layer
  - Physical
  - Link
  - Network and routing
  - Transport

Computer Immunology – Distributed Immune System

- The computer should have a distributed detection system, just like the human immune system
  - More than one control point
  - All control points should interact

Wired Networks

- Usually unique points of network control

Wireless Sensor Networks

- Collaboration of Local and Global Agents – Spontaneous Watchdogs

Computer Immunology – Unique Immune System

- Every individual has a unique immune defense; otherwise, a deadly contagious disease would result the end of the human race

- Every network should employ a unique detection system to limit its vulnerability to malicious attacks.

Computer Immunology – Creating antibodies

- The human immune system develops antibodies from previous disease and responds quickly when it re-encounters the same disease.

- In computer network security systems
  - Use pattern detectors to prevent known attacks, and
  - Anomaly detectors to detect novel attacks

Computer Immunology – Imperfect detection

- A two phase detection human immune function
  - It learns from the first response of the disease and
  - learning is distributed in the individual or human population

Wired Networks

- IDS vendors update their database and
- Notify their clients of the existence of the new malicious code

Wireless Sensor Networks

- Cooperative effort through the network
  - Collaboration of Local and Global Agents
- Monitoring nodes / Triangulation

Human Immune System

- **Thymus:** Production, maturation, and release of T-lymphocytes (T-Cells) within the human body.
- **Lymph:** Fluid with lymphocytes that bathes the tissues of an organism. On the way, it is filtered through the lymphatic organs (spleen and thymus) and lymph nodes
- **Antigen:** is a substance/molecule that, when introduced into the body, triggers the production of an antibody by the immune system
- **B-Cell:** Creates antigens and remembers of previous encountered bacteria
- **T-Cell:** Biologically bind with non-self cells. Once they bind, human immune responds to the bacteria

Computer Immunology – Sensor Networks

- Self in Sensor Networks is defined as:
  - Correct Sensor Readings
  - Appropriate behavior of a running application event
  - Authenticated set of neighbors
- System Architecture

Sensing nodes

Self-Organization to a tree structure
Each tree will be monitored by a control node

Monitoring nodes

SONN: self-organizing Neural Network with Competitive learning
The monitor nodes will be responsible for identifying abnormalities

Lymph (database)

B- cell analogy: detection of non-self through the use of a database

Thymus (machine)

T- cell analogy: Any abnormality will be sent to the Thymus machine

Base Station

Its role is to provide a solution and update Lymph and Thymus

Reaction Timing

- Proactive - Negative Selection Process
  - T-cells that represent non-self cells flood the human body trying to biologically bind with non-self cells
  - Flood the network with abnormal behavior scripts and if there is a match with current traffic/metrics then raise an alarm
- Reactive - Danger Theory (1994)
  - Supports that the human immune system does not react unless danger is detected and based on the strength of the danger signal the HIS reacts appropriately (Based on cell-death – necrosis (danger) and apoptosis (self cell death)
  - When malicious behavior is detected in the network raise a danger signal and react as appropriate.

Intrusion Detection Guidelines

- OODA loop
  - Observe: application transaction, message frequency (self and non-self)
    - for specific of attacks at specific network layers
  - Orient: learn from new attacks
    - update their memory of possible attacks
  - Decide: malicious or benign transaction?
    - based on predetermined boundaries
  - Act: serve or deny transaction
    - Avoid malicious node
- Integrated in timely enough fashion to have an effect on consequences

Computer Immunology – Nano-network issues

Wireless Sensor Networks

- Negative Selection/T-Cell scripts
  - Flood the network with non-normal activity
  - Knowledge of normal activity boundaries and react when an anomaly is detected
- Danger theory
  - Monitor network and react only when certain of malicious intervention and not of natural causes
- B cells
  - Small databases that can maintain previous attack signatures and to be compared with current attack

Nano Networks

- Negative Selection
  - Flooding the network can decrease the lifetime at a faster pace
  - Knowledge of protocol activity can increase security
- Danger theory
  - In intra-body applications: Use of the actual human immune system to determine the nature of abnormality

Conclusions

- Nanotechnology is an emerging field that has gained a great interest from the research community.
- At the current stage security challenges are not even considered.
- Taking into consideration the implications of a security breach and the nano-technology limitations, security techniques have to a part of the bottom-up design approach

Conclusions

- It is evident that human immune characteristics can be used as blueprints for establishing a secure system.

- Human immune techniques as guidelines for security in sensor and nanoscale networks to establish
  - Data Integrity,
  - Network Availability, and
  - Confidentiality

Thank You!

Any Questions?

Contact: vasosv@cs.ucy.ac.cy