Sensor Networks Security

Shambhu Upadhyaya
Wireless Network Security
CSE 566 (Lecture 23)

University at Buffalo The State University of New York

Outline

- Motivation
- Challenges
- Threat and trust model
- Overview of security solutions
- DoS attack case study for sensor networks
  - Physical layer
  - Link layer
  - Transport layer
- Protocol vulnerabilities

University at Buffalo The State University of New York

Motivation

- Sensor networks – promising approach
- Monitoring wildlife, machinery performance monitoring, earthquake monitoring, military application, highway traffic, etc.
- Perform in-network processing
  - Data aggregation and forwarding summaries
- Critical to protect it
  - Traditional security techniques cannot be applied
  - Deployed in accessible areas – subject to physical attacks
  - Close to people – poses additional problems

Sensor Networks Vulnerabilities

- *Military Applications*
  Military can use sensor networks for a host of purposes like detecting the movement of troops, etc.
- *Disasters*
  It may be necessary to protect the location and status of casualties from unauthorized disclosure
- *Public Safety*
  False alarms about chemical, biological, or environmental threats could cause panic or disregard for warning systems. An attack on the system's availability could precede a real attack on the protected resource
- *Home HealthCare*
  Because protecting privacy is paramount, only authorized users should be able to query or monitor the network

Challenges

- Challenges in sensor networks
  - Resource constrained environments
  - Large scale ad-hoc distribution
  - High fault tolerance requirement
  - Large range of operating environments
  - Limited Bandwidth
- Security challenges
  - Key establishment
  - Secrecy, authentication, privacy, robustness against DoS attacks
  - Secure routing
  - Node capture

Threat and Trust Model

- Outsider attacks
  - Eavesdropping passive attacks
  - Alter or spoof packets or inject interfering wireless signals to jam network
  - Disable sensor nodes by injecting useless packets and drain battery
- Insider attacks
  - Node compromise (capture and reprogram)
  - Possess the keys and participate in the secret communications
- Base station as a point of trust
  - Scalability becomes a problem
  - Base station becomes a bottleneck

Security Solutions

- Secrecy and authentication
  - Key establishment and management
  - PKI is expensive and subject to DoS attacks (bogus messages to initiate signature verification)
  - Multicast authentication using mTesla
- Availability
  - Jamming and packet injection (use spread spectrum, authentication, etc. to counter attack)
  - Routing attacks (use multi-path routing)
- Stealth attacks
  - Attack the service integrity
  - Make networks accept false data value (no good solutions available)

The Denial of Service Threat

- Denial of Service could be due to any of the following factors
  - An adversary trying to bring down the network
  - Hardware failures
  - Software bugs
  - Resource exhaustion
  - Environmental conditions
  - Any complicated interaction of the above factors

Design Considerations

- Operate in harsh environments
- Distinguish among DoS attacks and normal failure of node
- Considerations like protection of keys in case of physical attack
- Layered network architecture although computationally expensive helps in a better security design

Jamming Attacks (DoS)

- Jamming is transmitting signals to the receiving antenna at the same frequency band or sub band as the communications transmitter transmits
- Jamming, thus is used to hinder the reception at the other end
- Nodes can distinguish jamming from failure as in jamming constant energy rather than lack of response impedes communication

Jamming Attacks (Contd…)

- Most common defense against jamming attacks is to use spread spectrum techniques
- These techniques can be defeated by following the exact hopping sequence or by jamming a large bandwidth
- Defense
  - The nodes can combat jamming by switching to a lower duty cycle and hence preserving power

Jamming Attacks

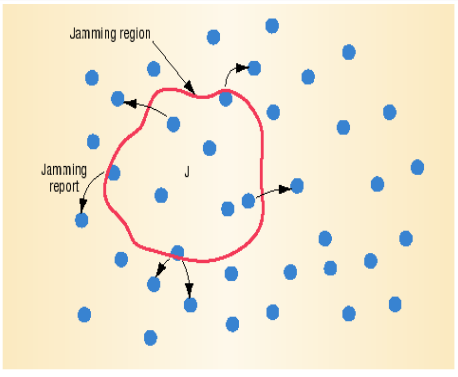

Figure 1. Defense against a jamming attack, phase one. Nodes along the edge of a jammed region report the attack to their neighbors.

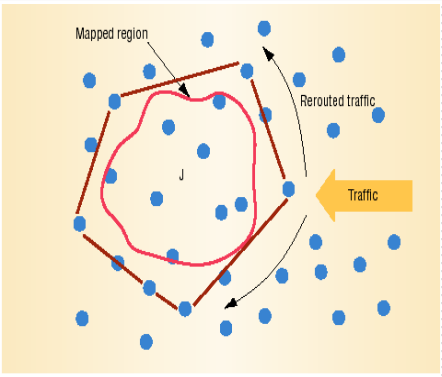

Figure 2. Defense against a jamming attack, phase two. Neighboring nodes collaborate to map the jamming reports, then reroute traffic around the jammed region.

Tampering (DoS)

- This attack involves physical access, interrogation and compromise of the nodes
- Providing physical security to all the nodes in a large sensor network is impractical
- Defense
  - The nodes should react to tamper in a fail-complete manner

Link Layer (DoS)

- Link Layer provides channel arbitration for neighbor to neighbor communication. It uses cooperative schemes like carrier sense that makes it vulnerable to DoS attacks
  - *Exhaustion*

    This involves induction of continuous collisions and other messages to exhaust the resources of the other nodes
  - *Collision*

    In this type of attacks adversaries induce a collision during the transmission of frame causing retransmission

Collision Attack

- This attack involves inducing a collision in just one octet of transmission
- The collision causes a checksum error at the other end
- Corrupted ACK control messages can cause expensive exponential back-off in some protocols

Collision Attack

- Error Correcting codes can be used to minimize the effect of such attacks but these have expensive overheads
- Although networks can use collision detection to thwart such attacks, however, a degree of cooperation is required among the nodes for network operation

Exhaustion Attack

- This type of attack involves introducing collisions in frames towards the end of transmission
- Thus the transmitting node continuously retransmits the packets and finally dies off
- A self sacrificing node can use the interactive nature of MAC protocols to launch an interrogation attack
- Defense
  - One solution is to make MAC admission control rate limiting so that network ignores excessive requests

Network Layer (DoS)

- Routing protocols that exist in the network layer must be simple enough to scale to a large number of nodes yet robust enough to cope with failures
  - *Homing Attack*
    In this type of attack the attacker tries to get down Nodes with special functions
  - *Neglect and Greed*
    In this attack the adversary node confirms the reception of the transmission but then drops it rather than forwarding it

Network Layer

- *Misdirection*

  This involves forwarding of packets along wrong paths so as to waste network bandwidth

- *Black Holes*

  This type of attacks are used in networks using distance vector routing where the adversary sends out incorrect route cost advertisements

Neglect and Greed

- This is one of the simplest form of attack where the malicious node acknowledges the reception of message from other node but then drops the packet
- This leads to waste of precious network bandwidth and causes retransmission
- If the node gives undue priority to its own messages then it is also called as *Greedy*

Neglect and Greed

- The *Dynamic Source Routing (DSR)* protocol is susceptible to this attack
- As the network caches routes, nodes use the same route to the destination and if a node is not generous, it may degrade or block traffic
- Defense
  - Use of multiple routing paths
  - Sending redundant messages

Homing Attack

- In a sensor network some nodes are assigned special responsibilities
- Location based network protocols that rely on geographic forwarding expose the network to such attacks
- In these attacks the attacker passively listens to the network and learns the location of such nodes
- Then with the help of powerful mobile devices these nodes are attacked and brought down
- Defense
  - One approach is to encrypt the headers so as to hide the location of the important nodes

Misdirection

- This is a more active form of attack where the messages are forwarded along wrong paths perhaps by fabricating malicious route advertisements
- One variant of this attack is the Internet Smurf attacks
- In sensor network an adversary can forge the address of a node and send route discovery messages to all the nodes
- Defense
  - This type of attack can be thwarted by using egress filtering
  - Using authentication of sender can also help

Black Hole Attack

- Networks using distance vector routing protocols are susceptible to this attack
- It involves network nodes sending zero cost route advertisements to all its neighbors
- As these cost advertisements propagate all network traffic is directed towards this node which leads to intense resource contention in the neighboring nodes
- Hence this forms a sort of Black Hole in the network
- Defense
  - Allow only authorized nodes to exchange route info
  - Monitoring of nodes and node watchdogs
  - Test network connectivity by probing
  - Use message redundancy

Transport Layer (DoS)

- This layer is responsible for maintaining end to end connections among the communicating entities. Sensor networks are vulnerable to the following attacks at this layer
  - *Flooding*
    Attacks protocols maintaining state at either end of the connection by causing memory exhaustion
  - *De-synchronization*
    This involves disrupting existing connections among the nodes by desynchronizing their transmissions

Flooding Attack

- This attack is similar to the TCP SYN attack where a node opens a large number of half open connections with another node to use up the resources
- Limiting the total number of connections prevents complete resource exhaustion but it also may prevent legitimate users from accessing the node
- Defense
  - This type of attack can be prevented by the use of client puzzles
  - The puzzles are computationally expensive and hence serve as a deterrent

De-synchronization

- This attack is used to disrupt existing connection by causing them to go out of synchronization
- This involves repeatedly sending forged messages to both of the communicating parties with various flags like Seq, Control flags set so that the nodes go out of synchronization
- If the attacker can maintain proper timing then it can prevent both the nodes from exchanging any useful information
- Defense
  - Use message authentication for control packets

Attacks and Defenses

Table 1. Sensor network layers and DoS defenses.

Network layer	Attacks	Defenses
Physical	Jamming	Spread-spectrum, priority messages, lower duty cycle, region mapping, mode change
	Tampering	Tamper-proofing, hiding
Link	Collision	Error-correcting code
	Exhaustion	Rate limitation
	Unfairness	Small frames
Network and routing	Neglect and greed	Redundancy, probing
	Homing	Encryption
	Misdirection	Egress filtering, authorization, monitoring
	Black holes	Authorization, monitoring, redundancy
Transport	Flooding	Client puzzles
	Desynchronization	Authentication

Attacks on Improved MAC Protocols in Sensor Networks

- Adaptive Rate Control Protocol
  - Developed to improve MAC layer performance but lends itself vulnerable to DoS attacks
- Real Time Location Based Protocols (RAP)
  - Uses a novel velocity monotonic scheduling (VMS) policy but adversary can exploit this feature

Adaptive Rate Control Protocol

- Random delays for transmissions
- Back off that shifts an application's periodicity phase
- Minimization of overhead in contention control mechanisms
- Passive adaptation of originating and route through admission control rates
- Anticipatory delay for avoiding multi-hop hidden-node problems

Adaptive Rate Control Protocol

- All these features help in improving the efficiency of the protocol but still rely on co-operation among nodes
- The protocol also gives preference to route-through traffic by reducing the back-off for such packets by 50%
- This increases the probability of Flooding attacks

Real Time Location Based Protocol (RAP)

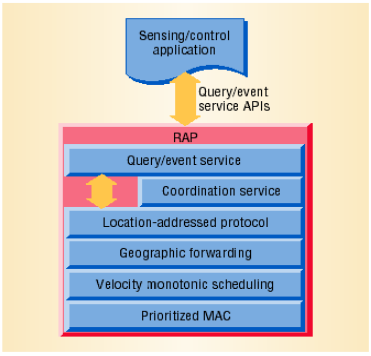

Figure 3. Real-time location-based protocols (RAP) architecture. RAP encompasses several network layers, from a prioritized media-access-control layer to the query-event API just below the application layer.

- The VMS layer stamps packets with a desired velocity, calculated from the distance to travel and the end-to-end deadline
- The originator can compute the velocity statically or the network can re-compute it dynamically at each intermediate node, based on the distance left and the time taken so far
- Nodes schedule packet relay by giving higher priority to higher-velocity packets

Real Time Location Based Protocol (RAP)

- An attacker can exploit the vulnerabilities in the RAP protocol by generating a large number of High Velocity packets. This can be achieved by
  - Making the deadlines short
  - Making the distance extraordinarily large
- This attack could succeed even if the network uses a location directory to detect out of network nodes

Real Time Location Based Protocol (RAP)

- The malicious node can also cause the packets being routed from it to miss their deadlines by intentionally lowering the velocity
- Also the RAP Protocol uses a synchronized clock to compute the time frame for the packets. Hence this also forms a possible area of attack

Conclusion

- Secure routing is vital to acceptance and use of sensor networks
- The current protocols lack the support and are inherently insecure
- Authentication and cryptography presents the first line of defense but is not enough
- Security in sensor networks is an open problem and requires much more work

References

Wood, A.D., and Stankovic, J.A., "Denial of Service in`Sensor Networks", IEEE Computer, Oct 2002, pp. 54-62

Shi E. and A. Perrig, "Designing Secure Sensor Networks", IEEE Wireless Communications, Dec. 2004

A. Perrig, J. Stankovic and D. Wagner, "Security in Wireless Sensor Networks", CACM, June 2004