Energy Depletion Attacks on Wireless Sensor Networks : A Survey

FARZANA.T

12MCS1004
Computer Science & Engineering
Guide: Mrs.Aswathy babu

February 23, 2016

Outline

Objective

To perform a literature survey on various energy depletion attacks affected in wireless sensor networks.

Outline

Wireless Sensor Network

- Consists of a number of sensors spread across a geographical area.
- Each sensor has wireless communication capability
- Has some level of intelligence for signal processing and networking of the data

Wireless Sensor Network cntd....

- Sensor node has restricted power supplies, low bandwidth, small memory and limited energy.
- Leads to very demanding environment to provide security.

Energy Depletion Attack

- Attacker would send data to drain a node battery and reduce network bandwidth.

Outline

Literature survey

- Wireless Sensor Network Denial of Sleep attack[1]
- Intrusion Tolerant routing in Wireless Sensor Network[2]
- Cross-Layer Design for Energy Conservation in Wireless Sensor Network[3]
- Energy Efficient Opportunistic Routing in Wireless Sensor Network[4]
- Sleep Deprivation Attack Detection in Wireless Sensor Network[5]
- Vampire Attack: Draining Life from Wireless Sensor Network[6]

Outline

Wireless Sensor Network Denial of Sleep attack[1]

- A subset of the denial of service class of network attacks targets on MAC layer.
- Penetrates a device's power management system to reduce the opportunities to transition into lower power states.
- Analyses energy resource vulnerabilities at MAC level.
- Avoided by the introduction of G-MAC protocol.

Wireless Sensor Network Denial of Sleep attack[1]

- G-MAC - Gateway MAC protocol.
- Energy efficient sensor MAC protocol designed to coordinate transmissions within a cluster.
- G-MAC periodically elects a new gateway node to equally distribute the energy requirements among all of sensors.
- Cluster nodes only respond to the gateway node.
- Network attackers cannot penetrate link layer of G-MAC protocol.

Wireless Sensor Network Denial of Sleep attack[1]

- Advantage
  Perform well in all traffic situations.
- Disadvantage
  All cluster nodes are dependent on gateway node.
  Deals only with MAC layer depletion attack.

Outline

Intrusion Tolerant routing in Wireless Sensor Network[2]

- Main objective is that design of intrusion tolerant secure WSN.
- Single compromised node can disrupt only a localised portion of the network.
- Introduces a new protocol INSENS to achieve intrusion tolerance.
- INSENS : INtrusion-tolerant routing protocol for wireless SEnsor NetworkS.

Intrusion Tolerant routing in Wireless Sensor Network[2] cntd....

- INSENS construct a forwarding table at each node to communicate between sensor node and base station.
- Multipath routing is built to achieve secure routing.
- Symmetric key cryptography is used for authentication between base station and sensor node.
- Limits flooding of messages by allowing communication only between base station and sensor node.

Intrusion Tolerant routing in Wireless Sensor Network[2] cntd....

- Advantage
  Minimize communication and computation overhead at sensor nodes.
- Disadvantage
  Maximize communication and computation overhead at base station.

Outline

- Objective
- Introduction
- Literature survey
- Wireless Sensor Network Denial of Sleep attack[1]
- Intrusion Tolerant routing in Wireless Sensor Network[2]
- Cross-Layer Design for Energy Conservation in Wireless Sensor Network[3]
- Energy Efficient Opportunistic Routing in Wireless Sensor Network[4]
- Sleep Deprivation Attack Detection in Wireless Sensor Network[5]
- Vampire Attack: Draining Life from Wireless Sensor Network[6]
- Conclusion
- References

Cross-Layer Design for Energy Conservation in Wireless Sensor Network[3]

- Considers Routing layer and MAC layer jointly.
- Network layer:
  Sending the traffic generated by sensor node through multiple paths instead of forwarding always through same path.
- MAC layer:
  Adjust retry limit of retransmission over each wireless link - different limits for different links.

Cross-Layer Design for Energy Conservation in Wireless Sensor Network[3] cntd...

- Advantage
  Reduces energy consumption.
- Disadvantage
  Does not consider any attack.

Outline

Energy Efficient Opportunistic Routing in Wireless Sensor Network[4]

- Opportunistic routing is based on broadcast transmission of data packets.
- Receptors need to be coordinated in order to avoid duplicated transmission.
- Achieved by ordering the forwarding node according to some criteria.
- Here nodes in the forwarder list are prioritized.
- Lower priority forwarder will discard the packet if packet has been forwarded by a higher priority forwarder.

Energy Efficient Opportunistic Routing in Wireless Sensor Network[4] cntd.....

- Advantage
  Concentrates on selecting and prioritizing the forwarder list to minimize the total energy of network.
- Disadvantage
  Does not consider any attack at routing level.

Outline

Sleep Deprivation Attack Detection in Wireless Sensor Network[5]

- Attack prevents the nodes from going in to sleep mode.
- Results depleting the battery and reducing the sensor lifetime from years to days.
- Proposes a hierarchical model to detect sensor nodes affected by this attack.
- Uses cluster based mechanism.

Sleep Deprivation Attack Detection in Wireless Sensor Network[5] cntd...

- Depending on battery capacity,sensor nodes are categorised as:
- Sink gateway
- Cluster-in-charge
- Sector monitor
- Sector-in-charge
- Leaf node

Sleep Deprivation Attack Detection in Wireless Sensor Network[5] cntd...

- Advantage
  Increases energy efficiency
- Disadvantage
  High communication overhead in some cases

Outline

- Objective
- Introduction
- Literature survey
- Wireless Sensor Network Denial of Sleep attack[1]
- Intrusion Tolerant routing in Wireless Sensor Network[2]
- Cross-Layer Design for Energy Conservation in Wireless Sensor Network[3]
- Energy Efficient Opportunistic Routing in Wireless Sensor Network[4]
- Sleep Deprivation Attack Detection in Wireless Sensor Network[5]
- Vampire Attack: Draining Life from Wireless Sensor Network[6]
- Conclusion
- References

Vampire Attack: Draining Life from Wireless Sensor Network[6]

- Composition and transmission of a message that causes more energy to be consumed by the network.
- Resource depletion attacks at the routing protocol layer, which permanently disable networks by quickly draining node's battery power.
- All protocols are susceptible to Vampire attacks.
- Do not disrupt immediate availability, but rather work over time to entirely disable a network.

Vampire Attack: Draining Life from Wireless Sensor Network[6] cntd....

- Employs vampire attack on existing routing protocol PLGP during packet transmission phase.
- PLGPa is proposed to avoid vampire attack.

Vampire Attack: Draining Life from Wireless Sensor Network[6] cntd....

Advantage:

- Vampire attack identified and can increase the networks life time.

Disadvantage:

- Only packet transmission phase is avoided from vampire attack, route discovery phase is not considered.
- Only PLGP is considred,how the proposed solution works in other routing protocol is not considered.

Comparison

Sl no.	Techniques	Affected OSI layer
1	Denial of sleep attack	MAC
2	Cross layer design	MAC and network
3	Energy efficient opportunistic routing	MAC
4	Sleep deprivation attack	MAC
5	Vampire attack	Network

Outline

Conclusion

Performed a literature survey on various energy depletion attacks in WSN.

Outline

References

[1] Michael Brownfield,Yatharth Gupta, "Wireless Sensor Network Denial of Sleep Attack", *Proceedings of 2005 IEEE workshop on information assurance,June 2005*.

[2] Jing Deng, Richard Han, Shivakanth mishra, "INSENS: Intrusion-Tolerant routing in Wireless Sensor Networks", *University of Colorado,Department of computer science Technical report,June 2006* .

[3] Fatma Bouabdullah, Nizar Bouabdullah,Raouf Bouabdullah "Cross-layer Design for Energy Conservation in Wireless Sensor Networks", *IEEE GLOBECOM 2008,New Orleans,USA,December 2008*.

[4] Xufei Mao,Shaojie Tang, Xiahua Xu, "Energy efficient Oppurtunistic Routing in Wireless Sensor Network s", *IEEE transactions on parellel and distributed systems, VOL. 12, NO. 2, February 2011*

[5] Tapaliana Bhattasali,Rituparna Chaki,Sugata Sanyal "Sleep Deprivation Attack Detection in Wireless Sensor Networks", *International journal of computer applications(0975-8887)vol 40- No: 15,February 2012*

[6] Eugene Y. Vasserman, Nicholas Hopper, " Vampire Attacks: Draining Life from Wireless Ad Hoc Sensor Networks", *IEEE transactions on mobile computing, VOL. 12, NO. 2, February 2013*

[7] Yazeed Al-Obaisat,Robin Braun, "On Wireless Sensor Networks: Architectures,Protocols,Applications and Management", *Institute of Information and Communication Technologies,May 2004*

Thank You