Energy Depletion Attacks on Wireless Sensor Networks

FARZANA.T

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

December 19, 2013

Outline

- Introduction
- Literature survey
- Problem Definition
- Conclusion
- References

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

- Introduction
- Literature survey
- Problem Definition
- Conclusion
- References

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]

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.
- Avoided by the introduction of G-MAC protocol.

Intrusion Tolerant routing in Wireless Sensor Network[2]

- 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.

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.

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.

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.

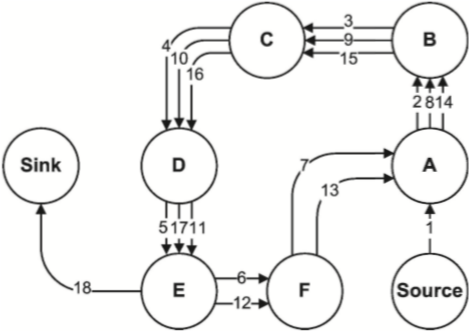
Vampire Attack: Draining Life from Wireless Sensor Network[6]

- 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.
- 2 vampire attacks: Stretch and carousel

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

Carousel attack

- adversary composes packets with purposely introduced routing loops
- sends packets in circles
- allowing a single packet to repeatedly traverse the same set of nodes



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

Stretch attack

- An adversary constructs artificially long routes, potentially traversing every node in the network
- Increases packet path lengths, causing packets to be processed by a number of nodes

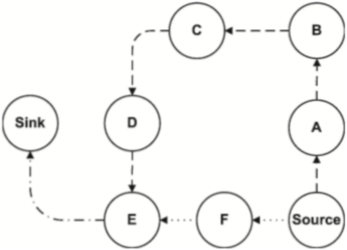


Figure: Stretch attack

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

- Employs vampire attack on existing routing protocol PLGP.
- PLGP: a clean-slate secure sensor network routing protocol by B.Prano, M.Luk, E.Gustad, A.Perrig.
- PLGP is vulnerable to Vampire attacks.
- Consists of a topology discovery phase, followed by a packet forwarding phase.

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

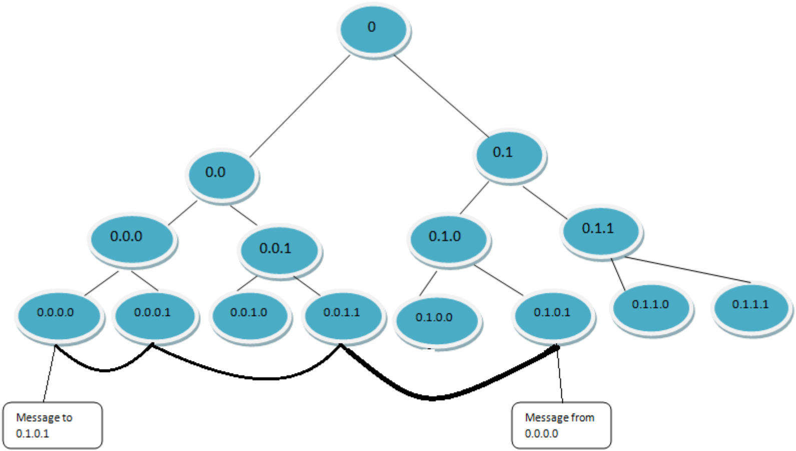
Discovery phase

- Deterministically organizes nodes into a tree that will later be used as an addressing scheme

Packet forwarding

- Node determines the next hop by finding the most significant bit of its address that differs from the message originators address.

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



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

Function `forward_packet` (p)

```
s ← extract_source_address(p);
c ← closest_next_node(s);
if is_neighbor(c) then forward(p, c);
else
    r ← next_hop_to_non_neighbor(c);
    forward(p, r);
```

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

- In PLGP, forwarding nodes do not know what path a packet took.
- Allowing adversaries to divert packets to any part of the network.
- Makes PLGP vulnerable to Vampire attacks

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

Provable Security against Vampire Attacks

- Proposed PLGP with attestations (PLGPa).
- Add a verifiable path history to every PLGP packet.
- PLGPa uses this packet history together with PLGPs tree routing structure.
- Every node can securely verify progress.
- Preventing any significant adversarial influence on the path taken by any packet which traverses at least one honest node.

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

```
Function secure_forward_packet (p)
  s ← extract_source_address (p);
  a ← extract_attestation (p);
  if (not verify_source_sig (p)) or
  (empty (a) and not is_neighbor (s)) or
  (not saowf_verify (a)) then
  |  return ;                                /* drop (p)  */
  foreach node in a do
  |  prevnode ← node;
  |  if (not are_neighbors (node, prevnode)) or
  |  (not making_progress (prevnode, node)) then
  |  |  return ;                             /* drop (p)  */
  |
  c ← closest_next_node (s);
  p′ ← saowf_append (p);
  if is_neighbor (c) then  forward (p′, c);
  else  forward (p′, next_hop_to_non_neighbor (c));
```

concept

A—>B—>C—>D—>E

- $ENC((\mathrm{Msg})_{Prk},4,A)_{PrA}$== X —> B
- B ——> $\mathrm{DEC}(X)_{PA} - -- >$ $\mathrm{ENC}(X,3,AB)_{PrB}$ == Y —>C
- C ——> $\mathrm{DEC}(Y)_{PB} - -- >$$\mathrm{ENC}(Y,2,ABC)_{PrC}$ == Z –> D
- D ——> $\mathrm{DEC}(Z)_{PC} - -- >$$\mathrm{ENC}(Z,1,ABCD)_{PrD}$ —->E

Outline

Problem Definition

- PLGPa includes path attestation increasing the size of every packet,incurring penalties in terms of bandwidth use, and thus radio power.
- Adding extra packet verification requirements for intermediate node increases processor utilization.
- Energy expenditure for cryptographic operations at intermediate hop is much greater than transmit or receive overhead.
- Only packet transmission phase is avoided from vampire attack, route discovery phase is not considered.
- Only PLGP is considered,how the proposed solution works in other routing protocol is not considered.

Outline

- Introduction
- Literature survey
- Problem Definition
- **Conclusion**
- References

Conclusion

- PLGPa is not vulnerable to Vampire attacks during the forwarding phase
- Overhead is the main problem of this method.
- Can reduce overhead, use single cryptographic function instead of onion encryption.

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