Combating Selective Forwarding Attacks: A Checkpoint-Based Countermeasure in Energy Harvesting-Motivated Networks

Cong Pu **Sunho Lim**
Dept. of Computer Science, Texas Tech University

Lauren Huie
Air Force Research Laboratory, New York

Abstract

A selective forwarding attack is a denial-of-service (DoS) attack in multi-hop wireless networks, where a single or multiple malicious nodes randomly or strategically disrupt network protocols or interfere with on-going communications. We design a light-weight countermeasure to selective forwarding attacks, where a randomly selected single checkpoint node is deployed to detect forwarding misbehaviors. The proposed countermeasure incorporates with timeout and retransmission techniques to cover unexpected packet loss due to forwarding misbehavior or bad channel quality. Extensive simulation experiments show that the proposed countermeasure can improve detection rate and packet delivery ratio as well as reduce false detection rate, successful drop rate, and energy consumption, compared to prior schemes.

Introduction & Motivation

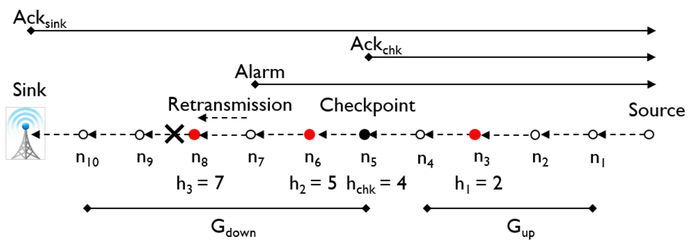
- Energy Harvesting-Motivated Networks (EHNets)
  - A large amount of autonomous sensors
  - Deployed in a hostile and unattended area
  - Harvest energy from surrounding environmental resources (e.g., vibration, light, wind, etc.)
  - Faithfully or collaboratively route data packets
- Energy Harvesting Model
  - Two-state Markov Process:
    - Active (S_a) and harvest (S_h) states
    - Node repeatedly switches state in exponential amount of time
- **Problem**:
  - Lack of physical protection
    - Node can easily be captured, tampered, or destroyed by an adversary
  - Open nature of wireless communication
    - An adversary can overhear, duplicate, corrupt, or alter sensory data
- Selective Forwarding Attack
  - One of well-known DoS attacks
  - Target network routing vulnerabilities of multi-hop relay
    - All node faithfully and collaboratively route data packets
  - **Attack Detail:**
    - A single or multiple malicious nodes randomly or strategically drop any incoming packet

Contribution of Our Work

- Challenges:
  - How to effectively detect selective forwarding attack?
  - How to reduce forwarding misbehavior and improve network performance?
- Light-weight Countermeasure to Selective Forwarding Attack
  - Three Techniques:
    - Single checkpoint node selection
    - Timeout
    - Retransmission

Single Checkpoint-Based Countermeasure

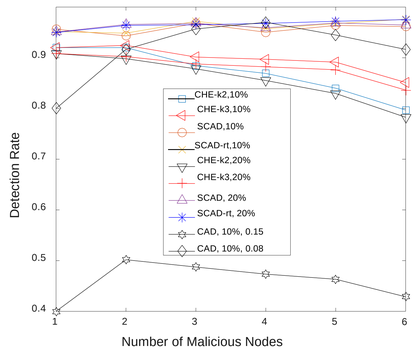
- Three Major Techniques
  - **Single Checkpoint Node Selection**
    - Source node randomly selects one of intermediate nodes located along the forwarding path to a **sink** as a **checkpoint node**
    - Sink and Checkpoint Node
      - Reply *Ack* packet back to source node
    - Checkpoint node divides the forwarding path into two streams:
      - Upstream: receive two *Ack* packets
      - Downstream: receive one *Ack* packet
  - **Timeout**
    - Node sets a timer for receiving an *Ack* packet after forwarding data packet
    - Forwarding misbehavior detection:
      - Node does not receive *Ack* before its timer expires
    - **Response**:
      - Generate an *Alarm* packet to prosecute the next node for its forwarding misbehavior
      - Forward the *Alarm* packet back to the source node
    - Timeout Setup
      - $T^{\zeta}_{ETT} = \alpha \cdot T^{\zeta}_{ETT} + (1 - \alpha) \cdot T_{ETT,k-1}$, $\zeta \in (C, S)$
      - $T_{ETT,k-1} = (T_{R,Ack} - T_{F,data}) / H_{k-1}$
      - $T^{\zeta} = T^{\zeta}_{ETT} \cdot H_k + H_k \cdot \mathcal{E}$
  - **Retransmission**
    - Node retransmits a cached data packet to the next node after forwarding an *Alarm* packet to source node
    - Condition:
      - Node does not receive an *Ack* or *Alarm* packet before its timer expires



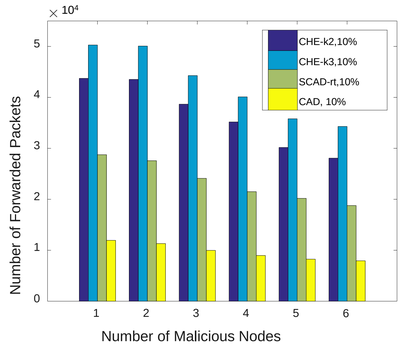
A forwarding path with a single checkpoint node in a network, where a black dot is a checkpoint node and the red dots are malicious nodes.

Performance Evaluation

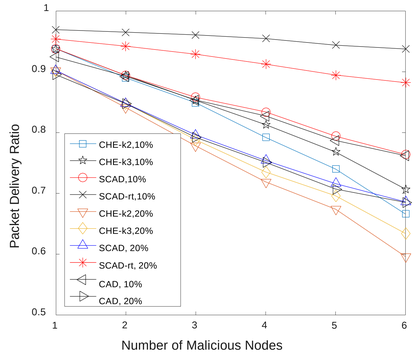
Detection Rate



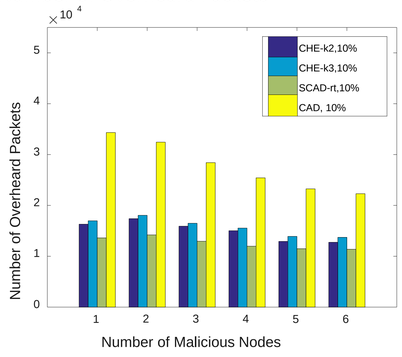
Number of Forwarded Packets



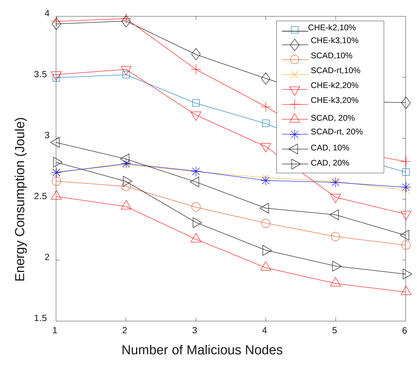
Packet Delivery Ratio



Number of Overheard Packets



Energy Consumption



Conclusion

- Efficiently detect the forwarding misbehaviors of malicious nodes and improve detection rate
- Efficiently reduce false detection and successful drop rate
- Achieve more than 90% packet delivery ratio with less energy consumption

References

1. B. Yu and B. Xiao, "Detecting Selective Forwarding Attacks in Wireless Sensor Networks," in IEEE IPDPS, 2006.
2. B. Xiao, B. Xu, and C. Gao, "CHEMAS: Identify Suspect Nodes in Selective Forwarding Attacks," Journal of Parallel and Distributed Computing, vol. 67, no. 11, pp. 1218-1230, 2007
3. D. M. Shila, C. Yu, and T. Anjali, "Mitigating Selective Forwarding Attacks with a Channel-Aware Approach in WMNs," IEEE Trans. On Wireless Communications, vol. 9, no. 5, pp. 1661-1675, 2010

T²WISTOR: TTU Wireless Mobile Networking Laboratory