The Effects of Denial-of-Service Attacks on Secure Time-Critical Communications in the Smart Grid

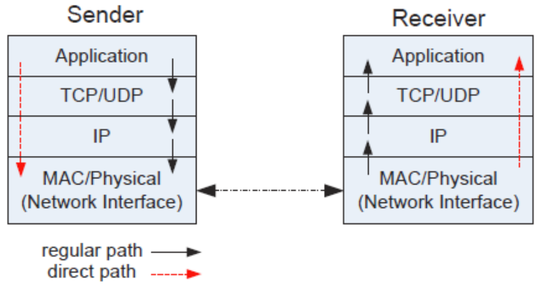
Fengli Zhang*, Qinghua Li*, Chase Ross*, Jing Yang^, Jia Di*, Juan Balda^, Alan Mantooth^
*Dept. of Computer Science and Computer Engineering, ^Dept. of Electrical Engineering, University of Arkansas

Introduction

- According to IEC 61850, many smart grid communications require messages to be delivered in a very short time
  - Trip messages and sample values applied to the transmission level: 3 ms
  - Interlocking messages applied to the distribution level: 10 ms
- Time-critical communications are vulnerable to denial-of-service (DoS) attacks
  - Flooding attack: Attacker floods many messages to the target network/machine
- We conduct systematic, experimental study about how DoS attacks affect message delivery delays

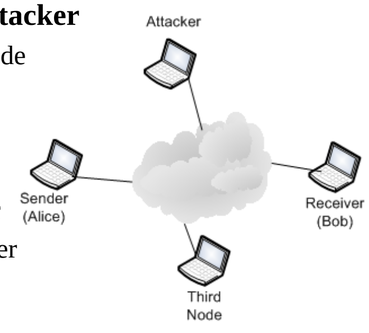
Background: Message Delivery Delay

- Delay: the elapsed time from when a message is generated by the sender application to when the message is received by the receiver application
  - Processing time at the sender's protocol stack
  - Network delay
  - Processing time at the receiver's protocol stack



Approach

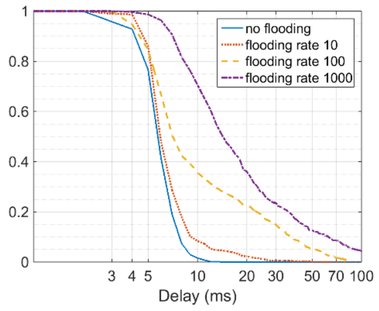
- Time-critical communications between **Sender** and **Receiver**
- Flooding attacks launched by **Attacker**
  - Network-layer flooding to a third node
  - Network-layer broadcast flooding
  - Network-layer flooding to sender
  - Network-layer flooding to receiver
  - Application-layer flooding to sender
  - Application-layer flooding to receiver



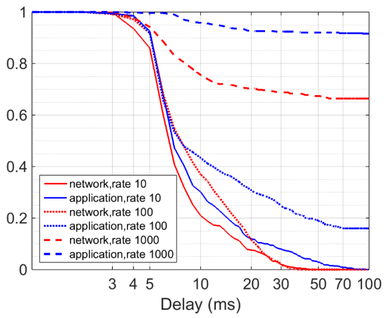
Experiment Results

Experiment on Wireless Networks

- **Deployment settings**
  - WLAN: Netgear N150 access point and 4 laptops
- **Effects of flooding attacks against Raw MAC communication signed with RSA** (complementary cumulative distributed function of delays is plotted)

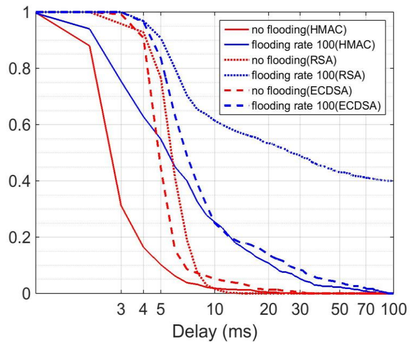


Application-layer flooding to receiver



Comparison of network-layer and application-layer flooding

  - Without flooding attacks, almost 100% of messages can be delivered in 10 ms.
  - With flooding, the delay increases as the flooding rate increases.
  - Application-layer flooding induces longer message delivery delays than network-layer flooding.
- **Delays with different authentication schemes RSA, ECDSA and HMAC**

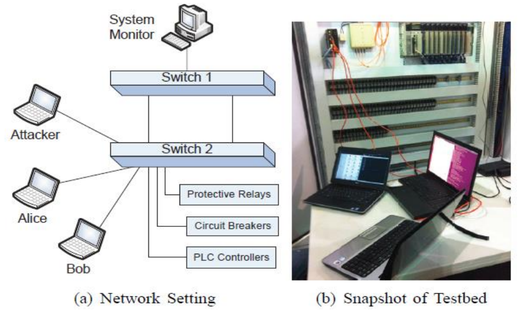


  - Without flooding attacks, the delay of RSA is the highest and the delay of HMAC is the shortest
  - With flooding attacks, messages with RSA are the most vulnerable and messages with HMAC are the most robust
  - Verifying RSA signature consumes the most CPU cycles

Experiment Results (Cont.)

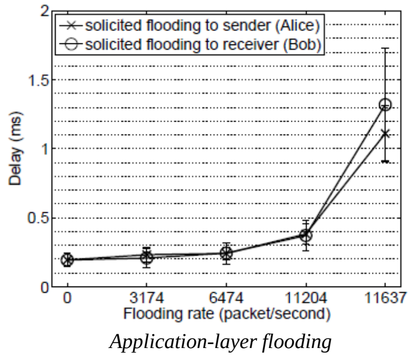
Experiment on Wired Networks

- Deployed to a real power system network – NCREPT (The National Center for Reliable Electric Power Transmission)



(a) Network Setting (b) Snapshot of Testbed

- Effects of flooding attacks on Raw MAC communications



Application-layer flooding

  - Flooding attacks can increase message delays

Conclusions and Future Work

Conclusions

- Flooding attacks can significantly increase the delay of time-critical messages.
- Wired network has better tolerance but still vulnerable.

Future Work

- Assess the rick of stealthy DoS attacks
- Design protection measures to mitigate DoS attacks