Trust Management and Security in the Future Communication-Based "Smart" Electric Power Grid

Authors: Jose Fadul1, Kenneth Hopkinson,
Christopher Sheffield, James Moore and Todd Ande

44th Hawaii International Conference on Systems Sciences, 2011

Presenter: Wenjin Yan

Submitted in Partial Fulfillment of the Course Requirements for
ECEN 689: Cyber Security of the Smart Grid
Instructor: Dr. Deepa Kundur

Overview

- Introduction
- Motivation
- Reputation-based trust management
- Three scenarios
- Create the graph
- Assessment
- Summary
- References

Introduction

- New standards and initiatives are moving in the direction of a smarter grid.

- Smart meters Vs Protection, control & SCADA

- A realistic view of Smart Grid

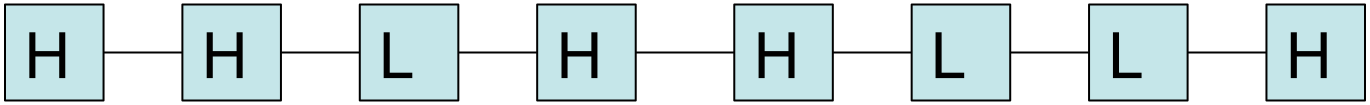
- Reputation-based trust management system

Motivation

- Cyber security risk

  -----IP spoofing, MITM, DOS, hijacking

- Idea of *Reputation-Based Trust*



H H L H H L L H

-----Share sensor readings;

-----Trust value: High/Low

- Make decision based on the trust value

  ----Mitigate some network vulnerabilities

Reputation-based trust

- Share information

  ---- voltage and current tolerance values

- Power lines loss

  ---- line impedance(constant)

- Binary values

  ---- 1: within tolerance

  0: not within tolerance

Trust Management

- Central Premise:

  ---- make better decisions

- Fundamental Algorithms:

  ---- Dijkstra’s shortest-paths

  Network flow

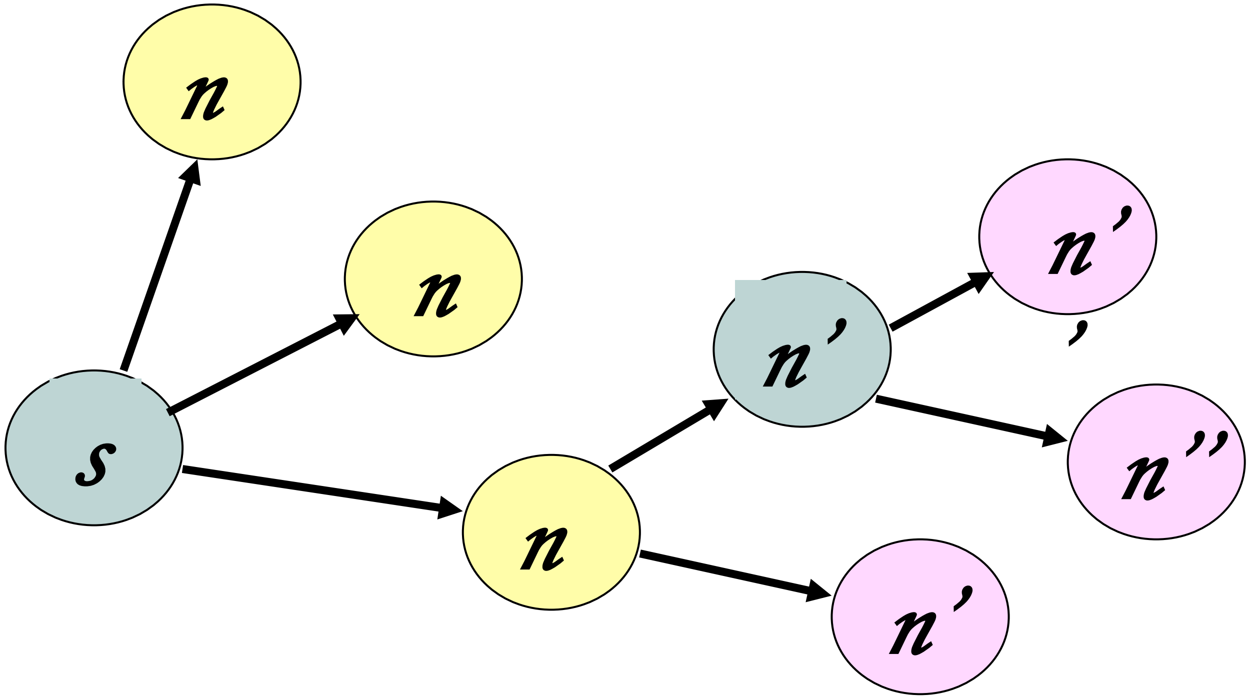
- TMS increase the level of complexity

  ----requires additional memory

  bandwidth

Dijkstra Algorithm

Find shortest paths from source s to all other destinations.

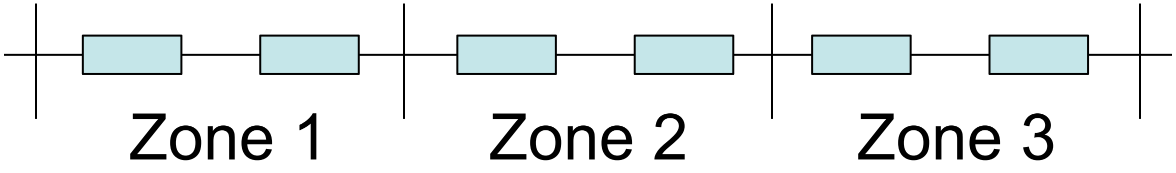


Conceived by Dutch computer scientist ----

Egsger Dijkstra, in 1956 and published in 1959.

Backup Protection

- Traditional Backup Protection System



---- a. Larger isolated region

b. no explicit intra-communication

- Agent-based design

---- communicate relay information

Benefits: a. Allow corrections to prevent false trip.

b. Smaller isolated region

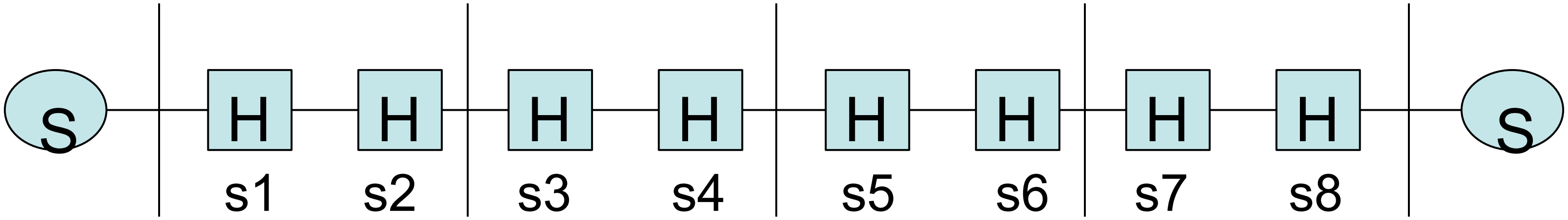
Drawback: same vulnerabilities in network

Three scenarios

Scenario 1: TMS does not interfere with primary relay-breaker protection functions.

Scenario 2: A shorted power grid containing trusted and untrusted sensor node/relays.

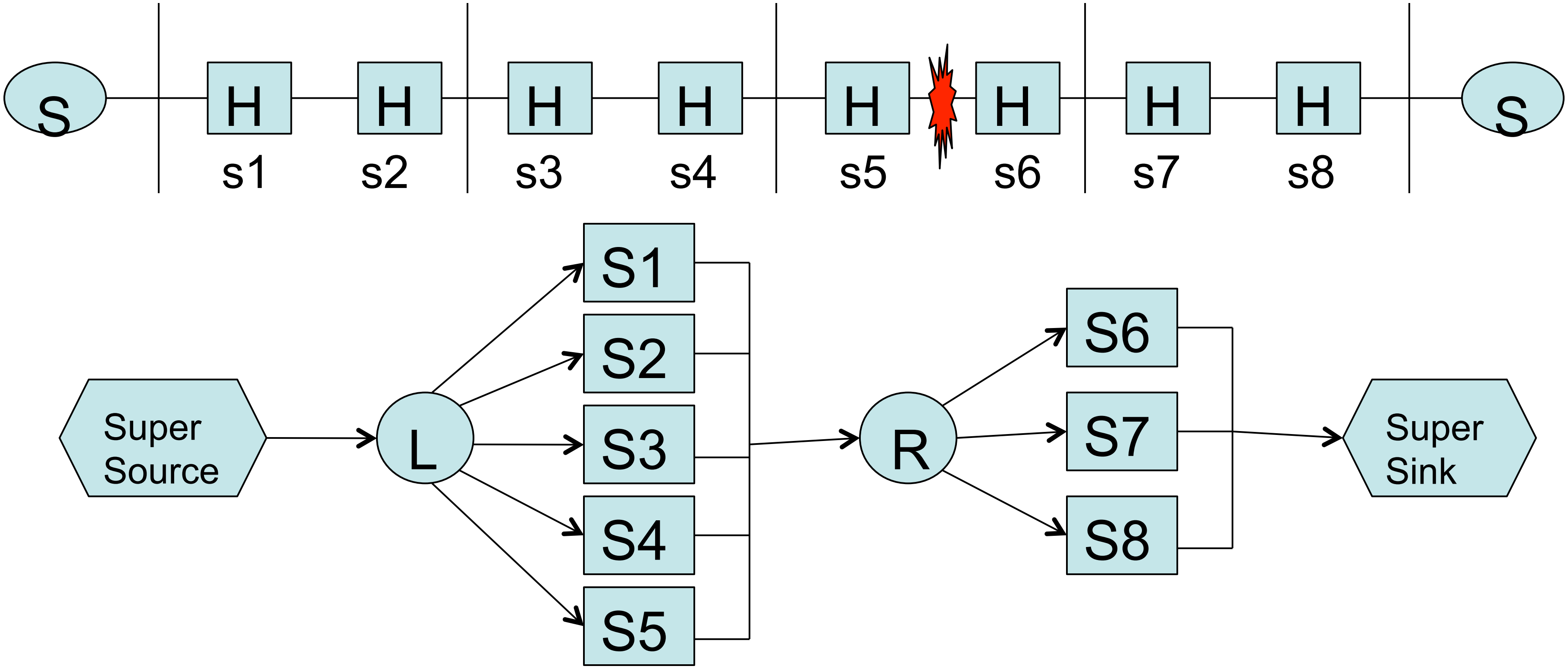
Scenario 3: A cyber attacker's attempt to cause a power outage by gaining unauthorized remote access of a single node/relay.



---- 2 generators & 8 sensor node/relays

High trust values equal 100

Scenario 1.1



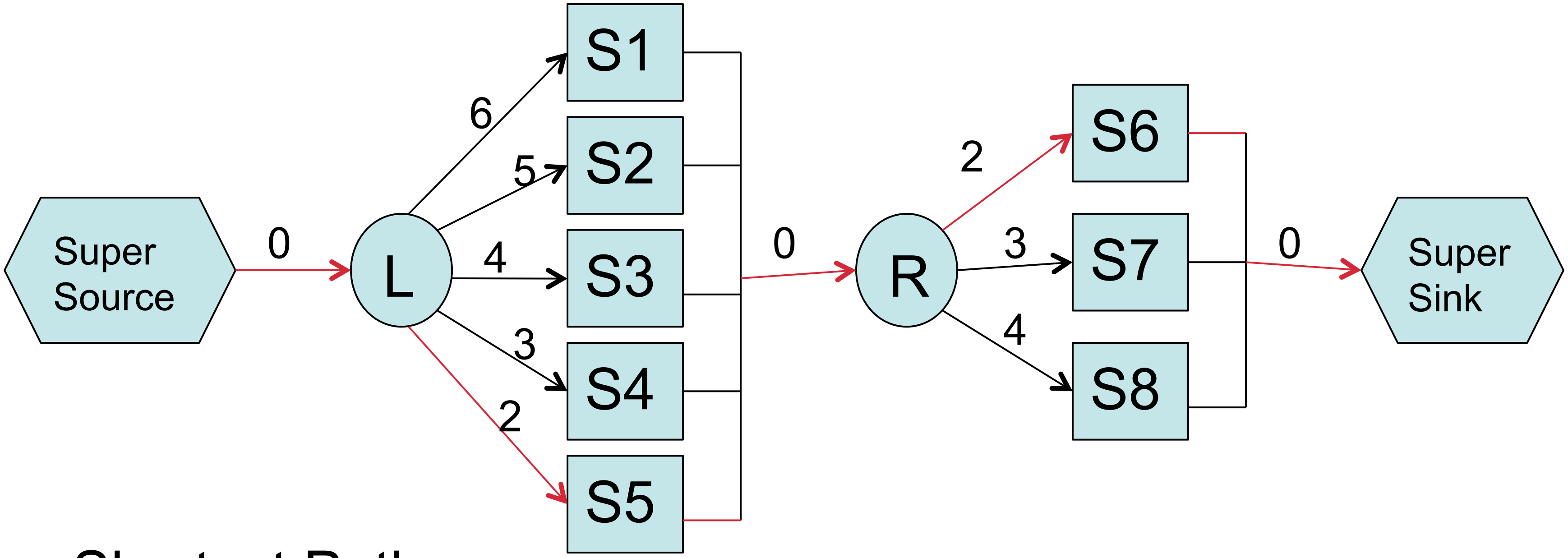
- Four fictitious nodes:

  a super source, super sink, left junction and right junction nodes.

Scenario 1.2

- The edge values for the generated graph:

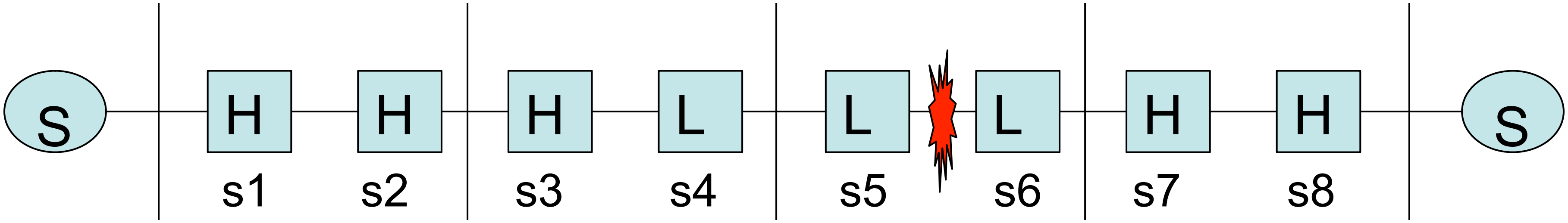
  ---- The edges entering a fictitious node: 0 ;
  The edges entering relay nodes: based on their
  distance from the fault and their assigned trust values.



- Shortest Path:

  ---- Node 5 and node 6 should open

Scenario 2.1



- Considered with lower trust values:

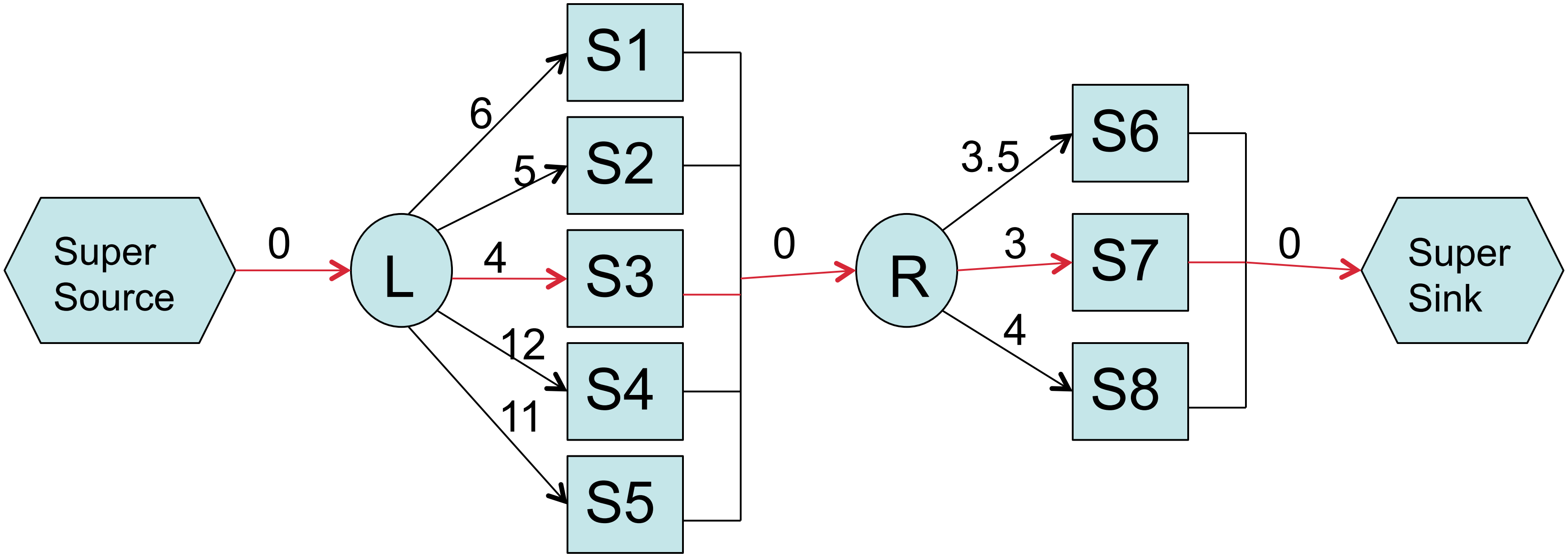
  ---- Sensor node/relays S4, S5 and S6:

  with trust value of 10%, 10% and 40%, respectively.

- High value: 100 ; S4 = 10 ; S5 = 10 ; S6 = 2.5.

- Lower trust values correspond with the higher edge cost

Scenario 2.2



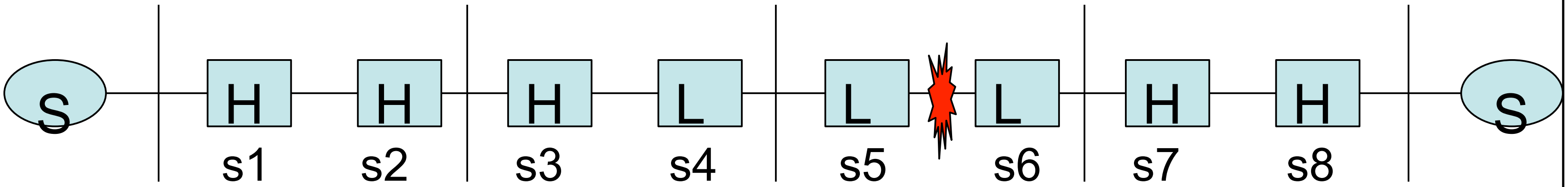
- Shortest Path:

  ---- Node 3 and node 7 should open

- Benefits:

  Minimizes the affected service area and the associated damages

Scenario 3.1



- Considered cyber threat associated with hijacking a sensor node/relay.

  ---- Trip: initiate a relay trip signal

- Hijacked node:

  ---- Considered trusted: confirm the trip signal internally.

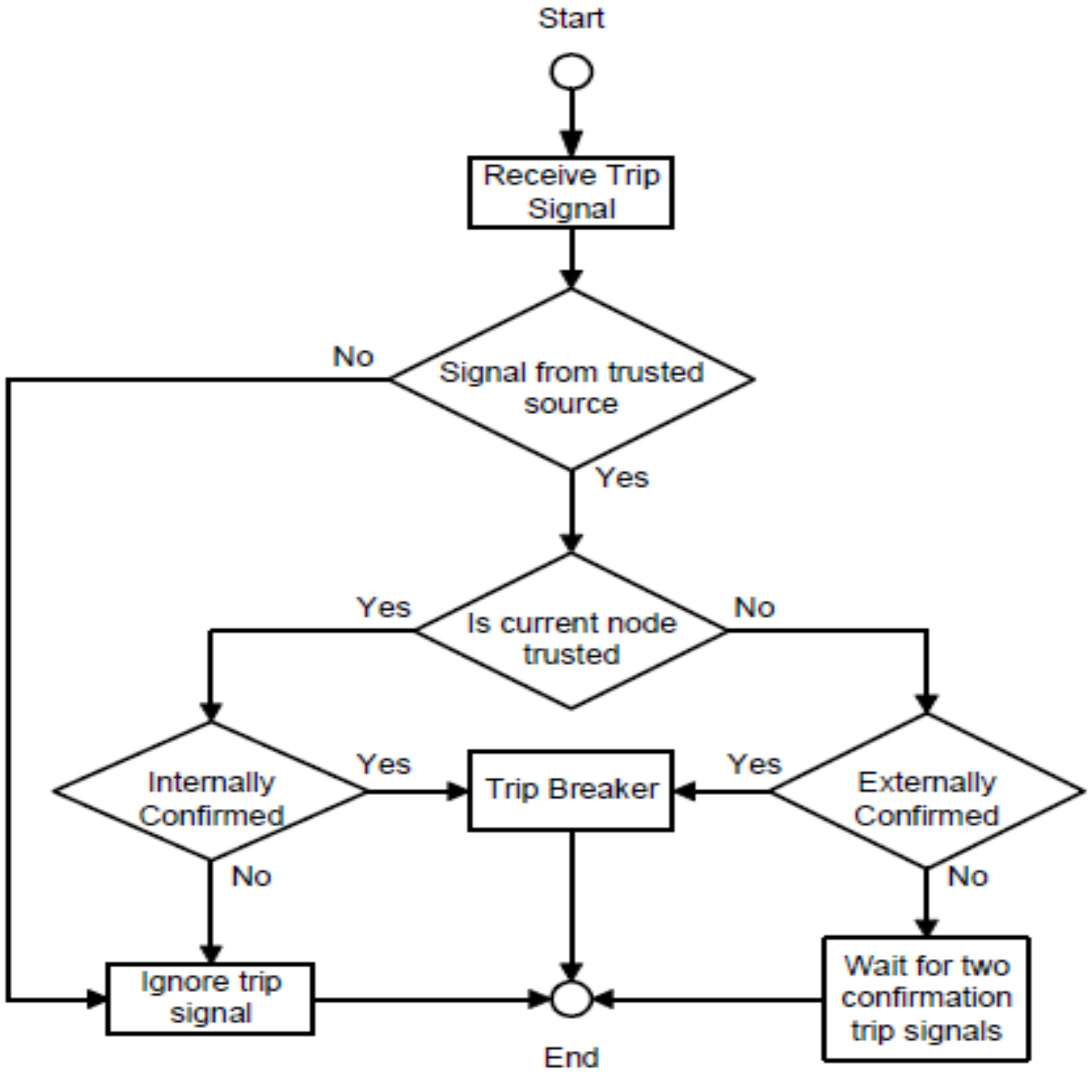
  ---- Not trusted: wait for confirmation from external trusted nodes.

  Unwarranted broadcast messages:

  indicate the presents of a cyber attacker;

  alert the power grid control center.

Scenario 3.2



[2]

Receive trip signal flowchart

Create the Graph

- Three requirements:

  1) the power grid topology,

  2) all sensor node/relays' trust values

  3) the location of the detected line fault.

- Requirement 1:

---- SCADA or a network discovery program: Static

- Requirement 2:

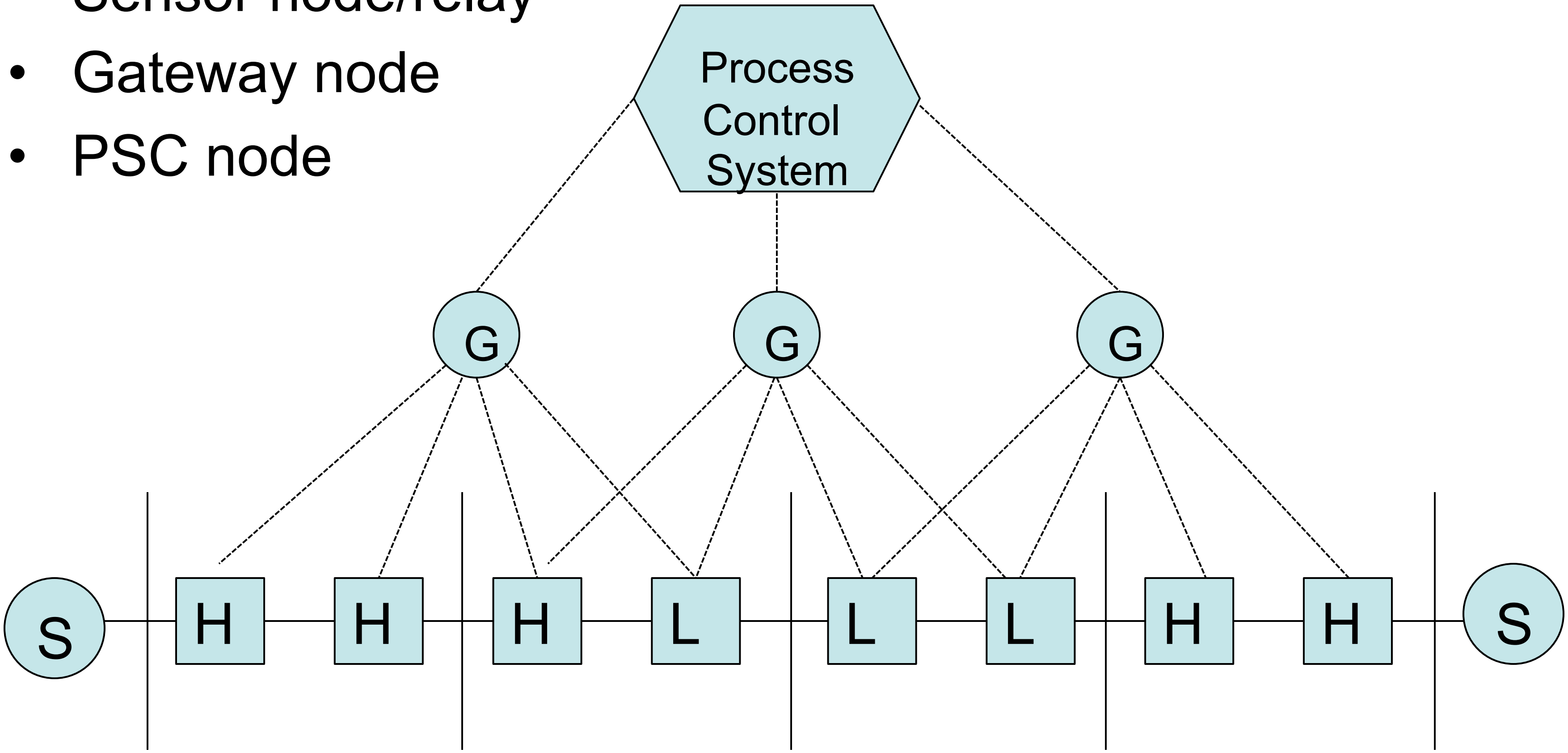
---- Simple Trust algorithm

- Requirement 3:

---- Sensor node/relays detecting the fault

Simple Trust algorithm

- Overlapping network neighborhoods
- Sensor node/relay
- Gateway node
- PSC node



Assessment

- Pros

  Logical & well organized

  Proposed a new way to mitigate vulnerabilities

  Related to practical protection problems

- Cons

  Untrusted values

  Details about tolerance

Summary

- The increased communication capabilities increase the power grids susceptibility to cyber attacks.

- The reputation based trust management

  ---- Mitigate cyber type attacks

  Improve backup protection system response time

- Further research is required before implementation.

Reference

[1] Wikipedia, http://en.wikipedia.org/wiki/Dijkstra's_algorithm

[2] J. Fadul, K. Hopkinson, C. Sheffield, J. Moore and T. Andel, "Trust Management and Security in the Future Communication-Based "Smart" Electric Power Grid," Proc. 44th Hawaii International Conference on Systems Sciences, 2011

[3] E. W. Dijkstra, "A Note on Two Problems in Connection with Graphs," Numerische Mathematik, vol.1,pp. 269-271, 1959.

[4] IEEE, IEEE 100: The authoritative dictionary of IEEE standards terms, 7th ed.: IEEE Press, 2000.

Thank you!!

Question?