MAKING NETWORKS ROBUST TO COMPONENT FAILURE

A Dissertation Outline presented by Daniel Gyllstrom
University of Massachusetts Amherst USA
Advisor: Jim Kurose

2/8/13

Thesis Problem Statement

How can networks -- the Internet and networked cyber-physical systems -- be made more robust to component failure?

We address the following problem in this thesis: “how can networks including the Internet and networked cyber-physical systems be made more robust to component failure?”

3 Component Failure Problems

Specifically, this thesis considers 3 separate but related problems:
(1) node failure in traditional networks such as the Internet,
(2) the failure of sensors measuring the health of the electric power grid, and
(3) link failures in a smart grid communication network used to disseminate sensor measurements.

3 Component Failure Problems

1. node (router) failure in traditional network

Specifically, this thesis considers 3 separate but related problems:
(1) node failure in traditional networks such as the Internet,
(2) the failure of sensors measuring the health of the electric power grid, and
(3) link failures in a smart grid communication network used to disseminate sensor measurements.

3 Component Failure Problems

1. node (router) failure in traditional network
2. failure of critical smart grid sensors

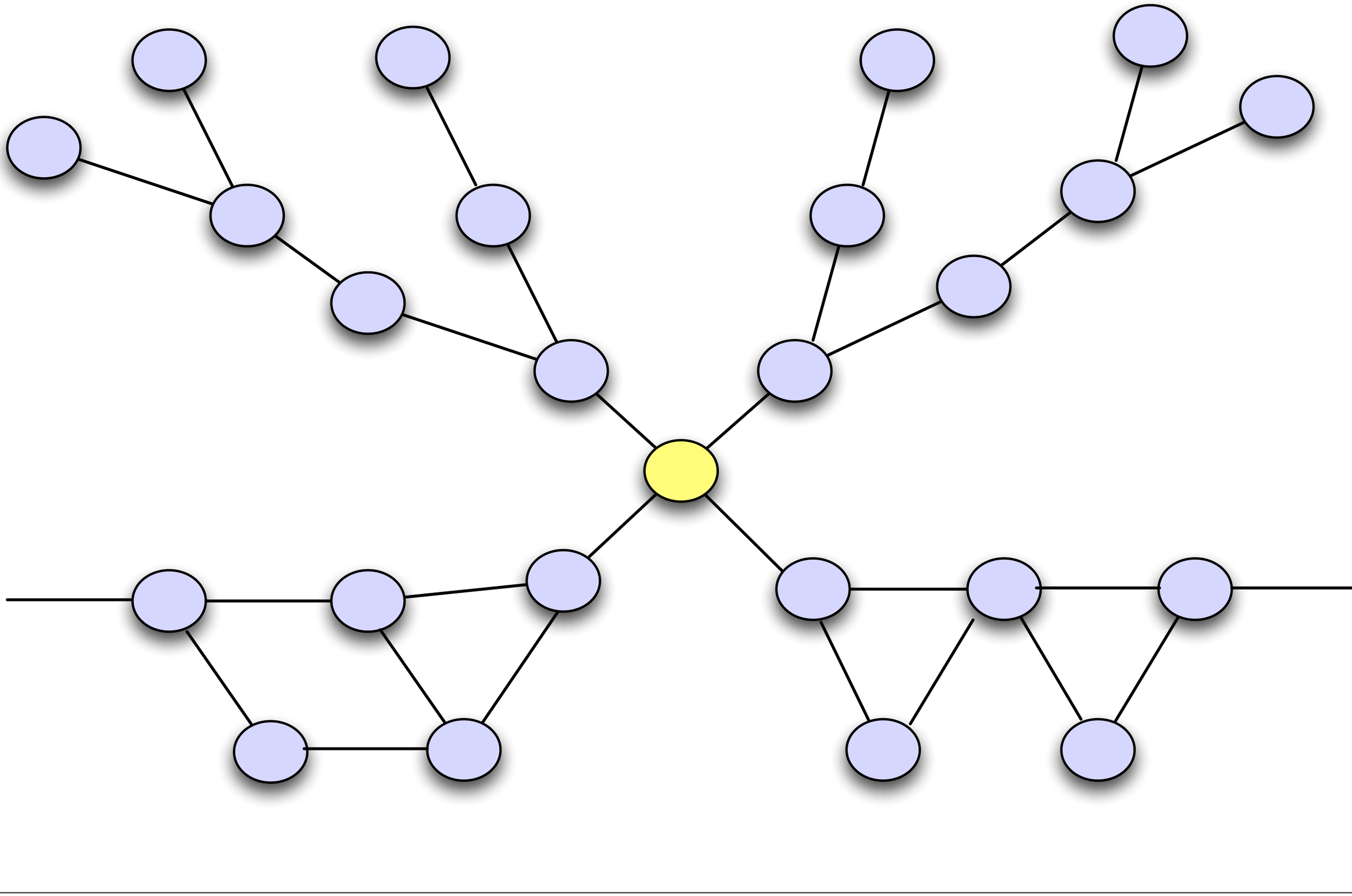
Specifically, this thesis considers 3 separate but related problems:
(1) node failure in traditional networks such as the Internet,
(2) the failure of sensors measuring the health of the electric power grid, and
(3) link failures in a smart grid communication network used to disseminate sensor measurements.

3 Component Failure Problems

1. node (router) failure in traditional network
2. failure of critical smart grid sensors
3. link failures in a smart grid communication network

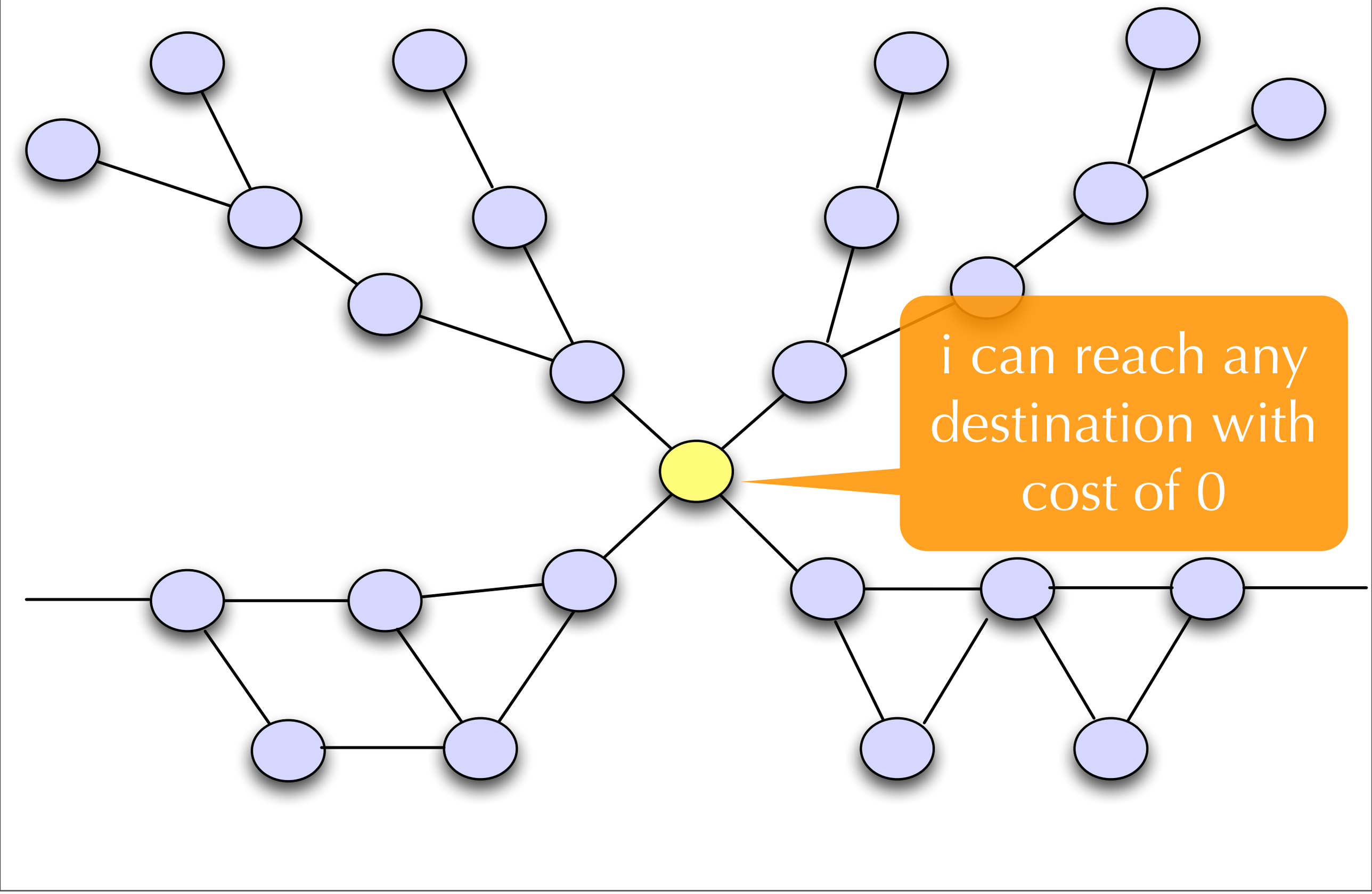
Specifically, this thesis considers 3 separate but related problems:
(1) node failure in traditional networks such as the Internet,
(2) the failure of sensors measuring the health of the electric power grid, and
(3) link failures in a smart grid communication network used to disseminate sensor measurements.

Ch 1: Network Router Failure



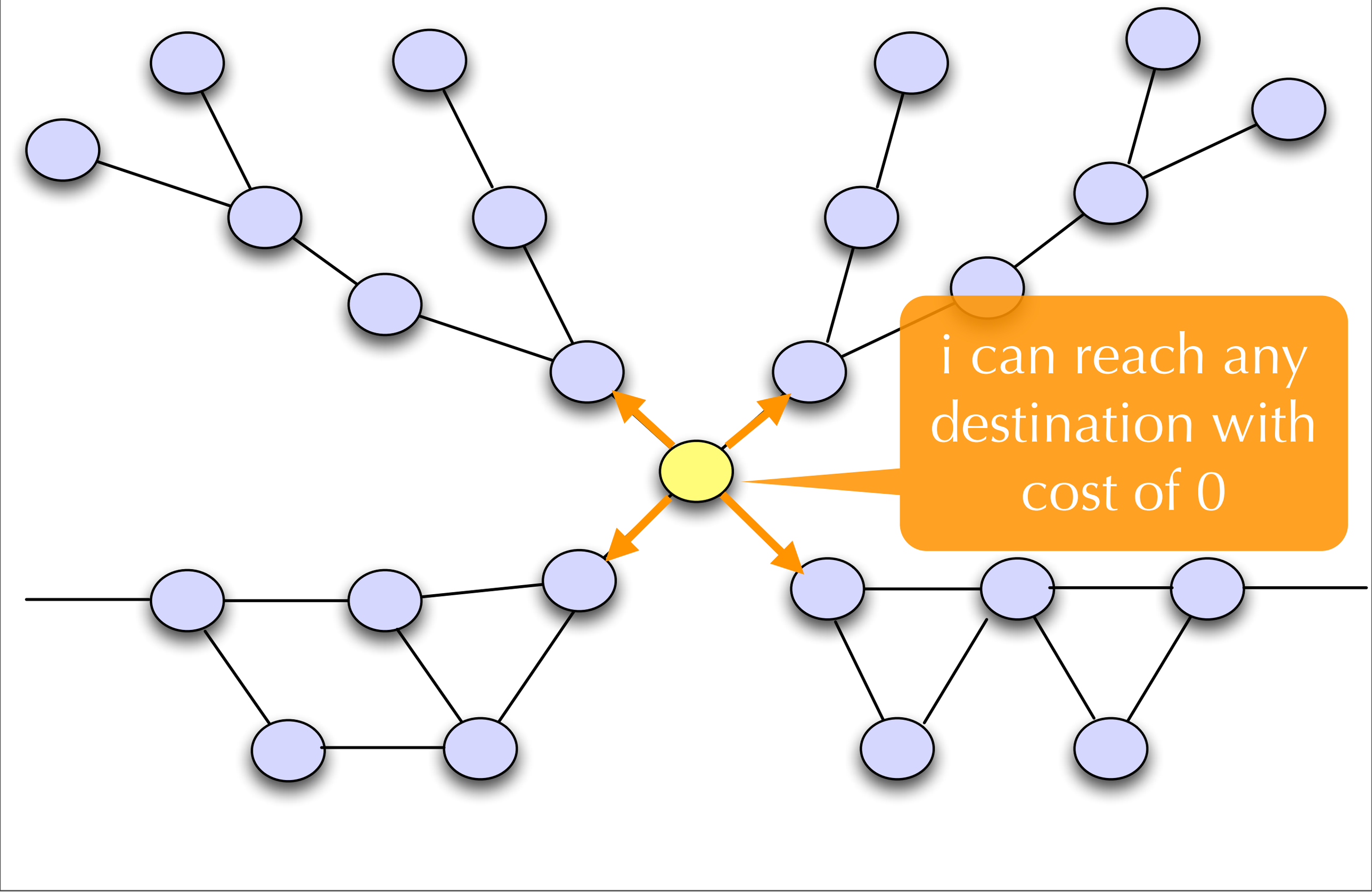
The first problem we consider arises in the context of distributed network algorithms, where a malicious or misconfigured node injects and spreads incorrect routing state throughout the network. Consider this example network of routers running the distance vector algorithm. Here the yellow router is compromised and falsely announces that is can reach any destination with a cost of 0. this false routing state propagates network-wide (as shown by the orange arrows). This causes many network routers to incorrectly route via the compromised node. This type of false state can degrade the performance of the network or render it unusable.

Ch 1: Network Router Failure



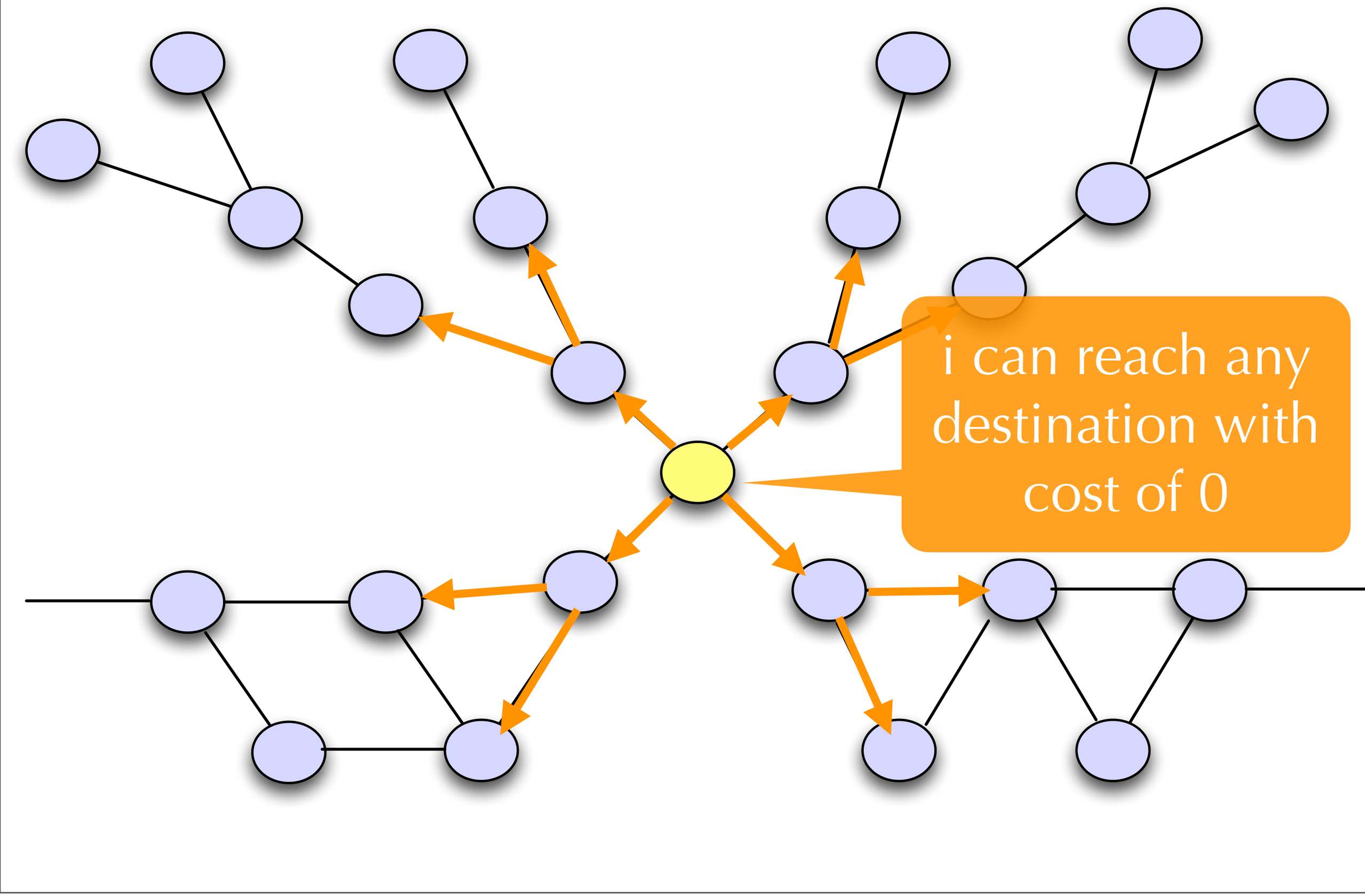
The first problem we consider arises in the context of distributed network algorithms, where a malicious or misconfigured node injects and spreads incorrect routing state throughout the network. Consider this example network of routers running the distance vector algorithm. Here the yellow router is compromised and falsely announces that is can reach any destination with a cost of 0. this false routing state propagates network-wide (as shown by the orange arrows). This causes many network routers to incorrectly route via the compromised node. This type of false state can degrade the performance of the network or render it unusable.

Ch 1: Network Router Failure



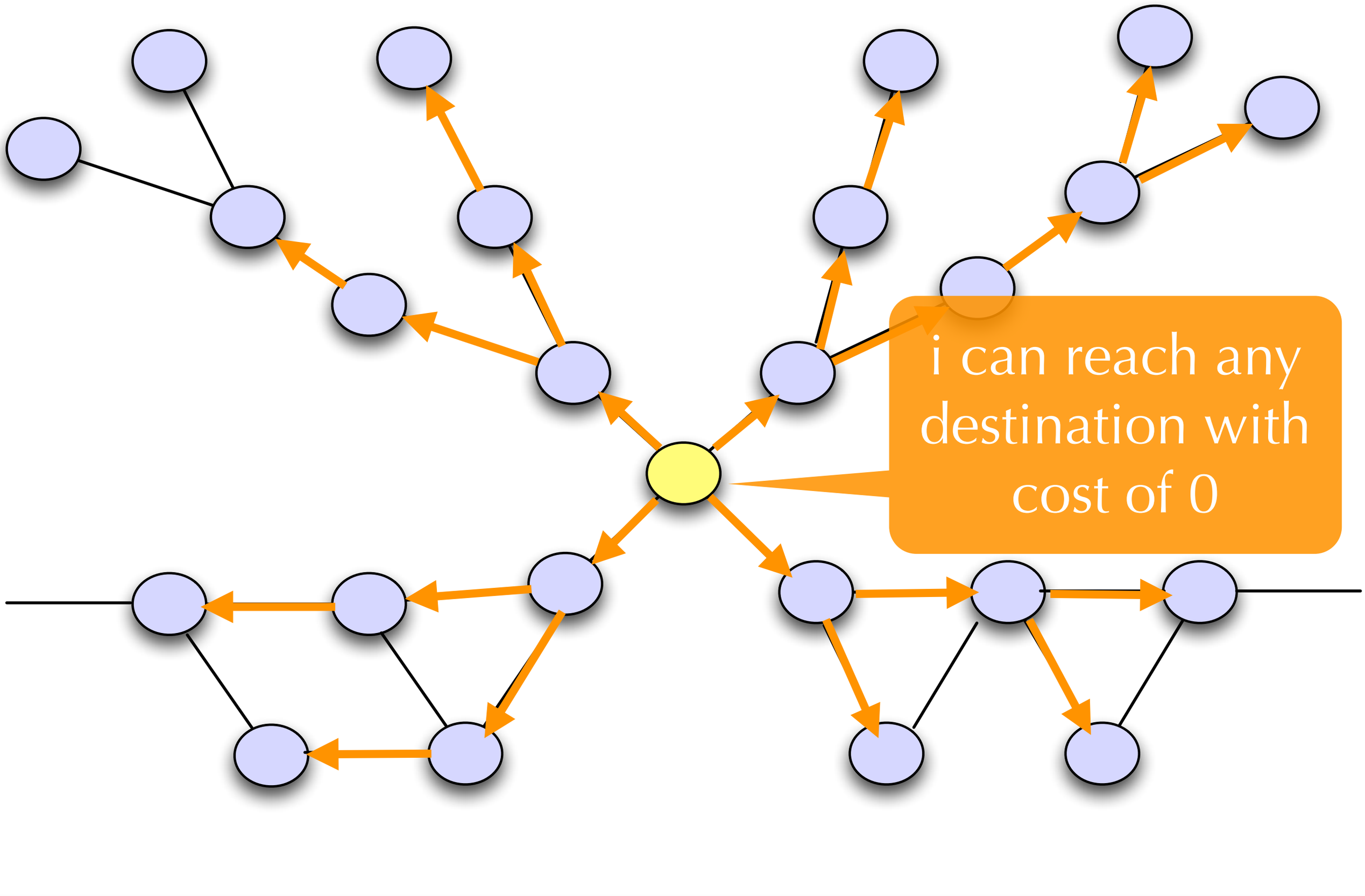
The first problem we consider arises in the context of distributed network algorithms, where a malicious or misconfigured node injects and spreads incorrect routing state throughout the network. Consider this example network of routers running the distance vector algorithm. Here the yellow router is compromised and falsely announces that is can reach any destination with a cost of 0. this false routing state propagates network-wide (as shown by the orange arrows). This causes many network routers to incorrectly route via the compromised node. This type of false state can degrade the performance of the network or render it unusable.

Ch 1: Network Router Failure



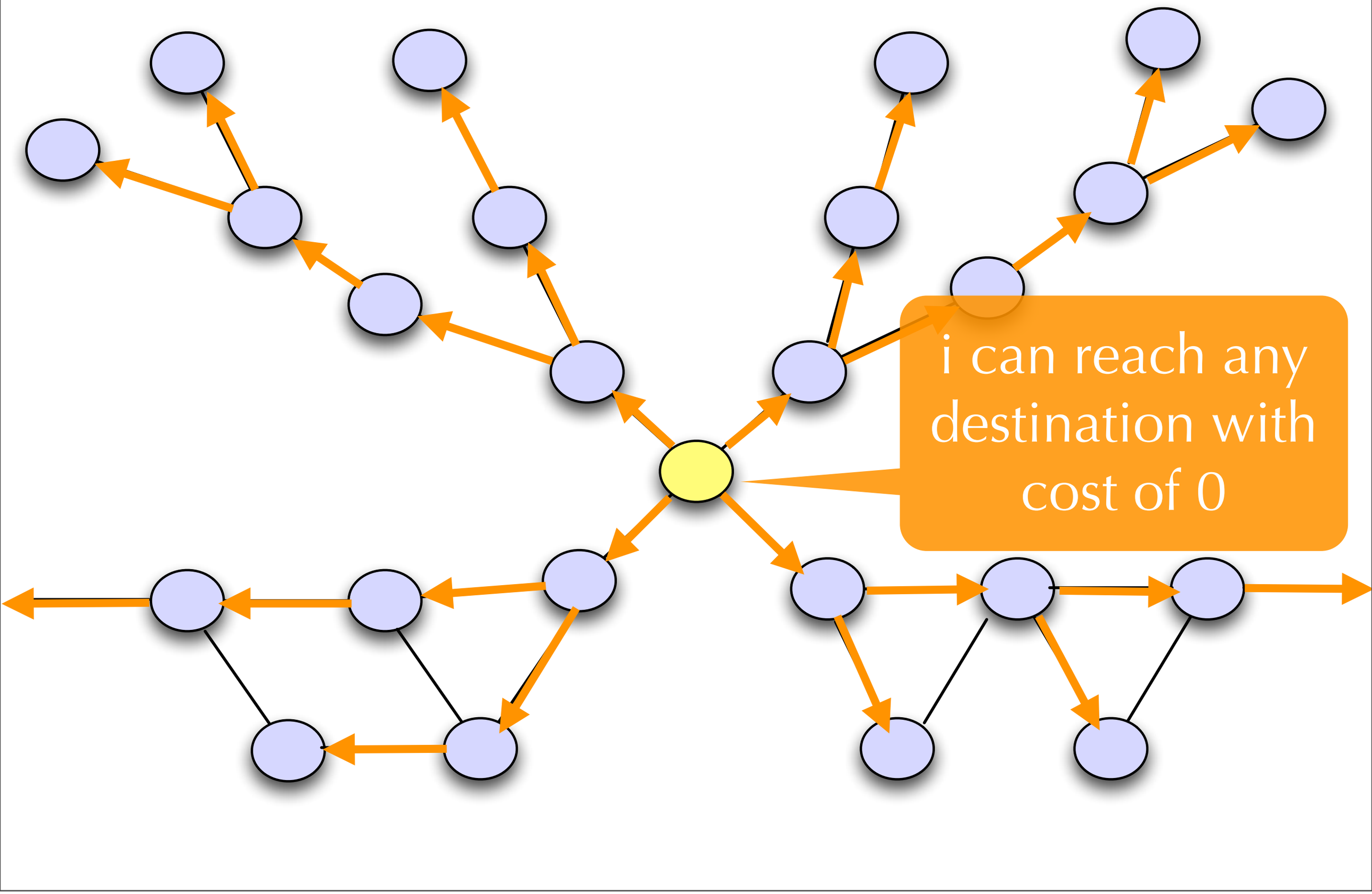
The first problem we consider arises in the context of distributed network algorithms, where a malicious or misconfigured node injects and spreads incorrect routing state throughout the network. Consider this example network of routers running the distance vector algorithm. Here the yellow router is compromised and falsely announces that is can reach any destination with a cost of 0. this false routing state propagates network-wide (as shown by the orange arrows). This causes many network routers to incorrectly route via the compromised node. This type of false state can degrade the performance of the network or render it unusable.

Ch 1: Network Router Failure



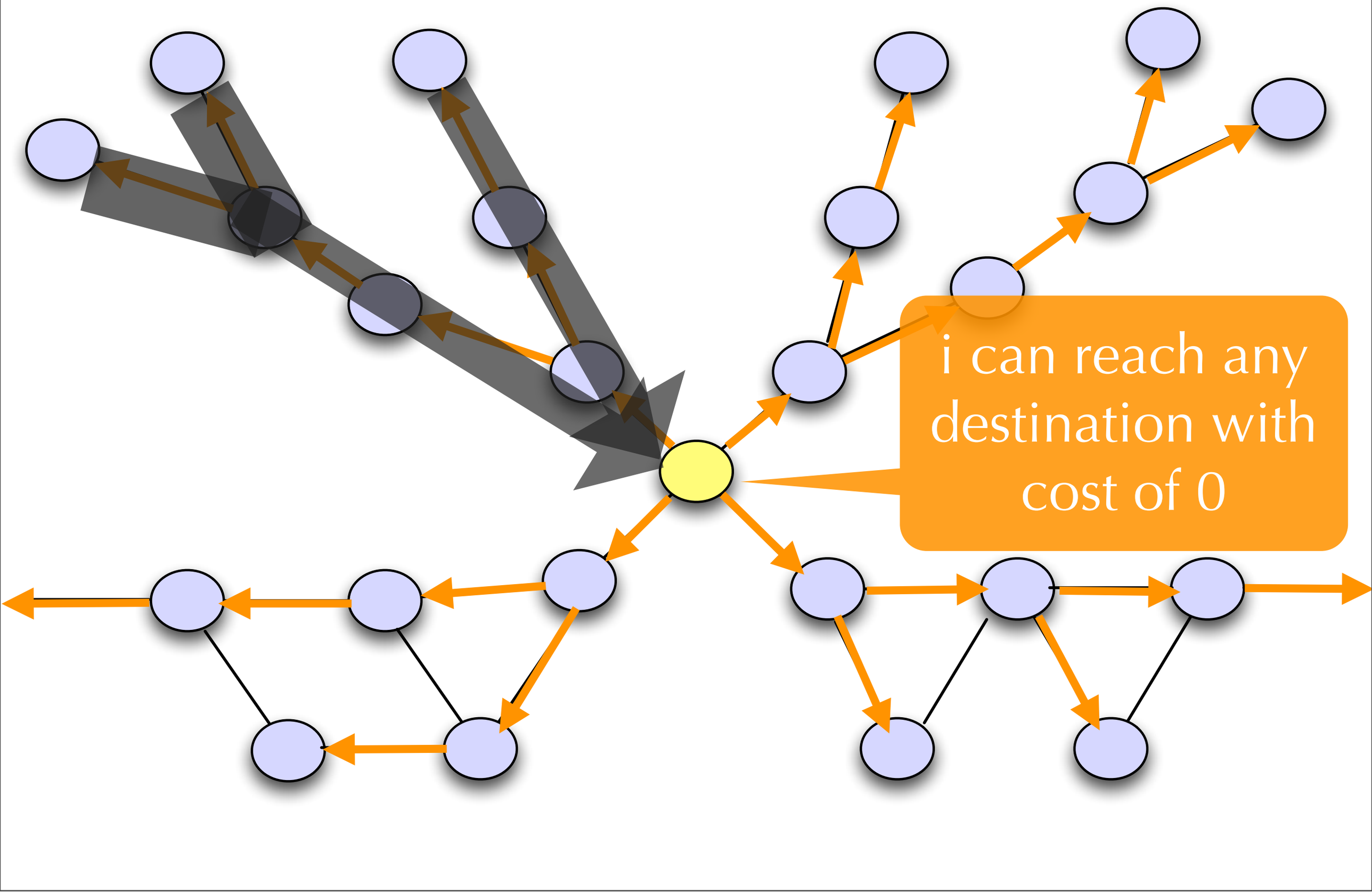
The first problem we consider arises in the context of distributed network algorithms, where a malicious or misconfigured node injects and spreads incorrect routing state throughout the network. Consider this example network of routers running the distance vector algorithm. Here the yellow router is compromised and falsely announces that is can reach any destination with a cost of 0. this false routing state propagates network-wide (as shown by the orange arrows). This causes many network routers to incorrectly route via the compromised node. This type of false state can degrade the performance of the network or render it unusable.

Ch 1: Network Router Failure



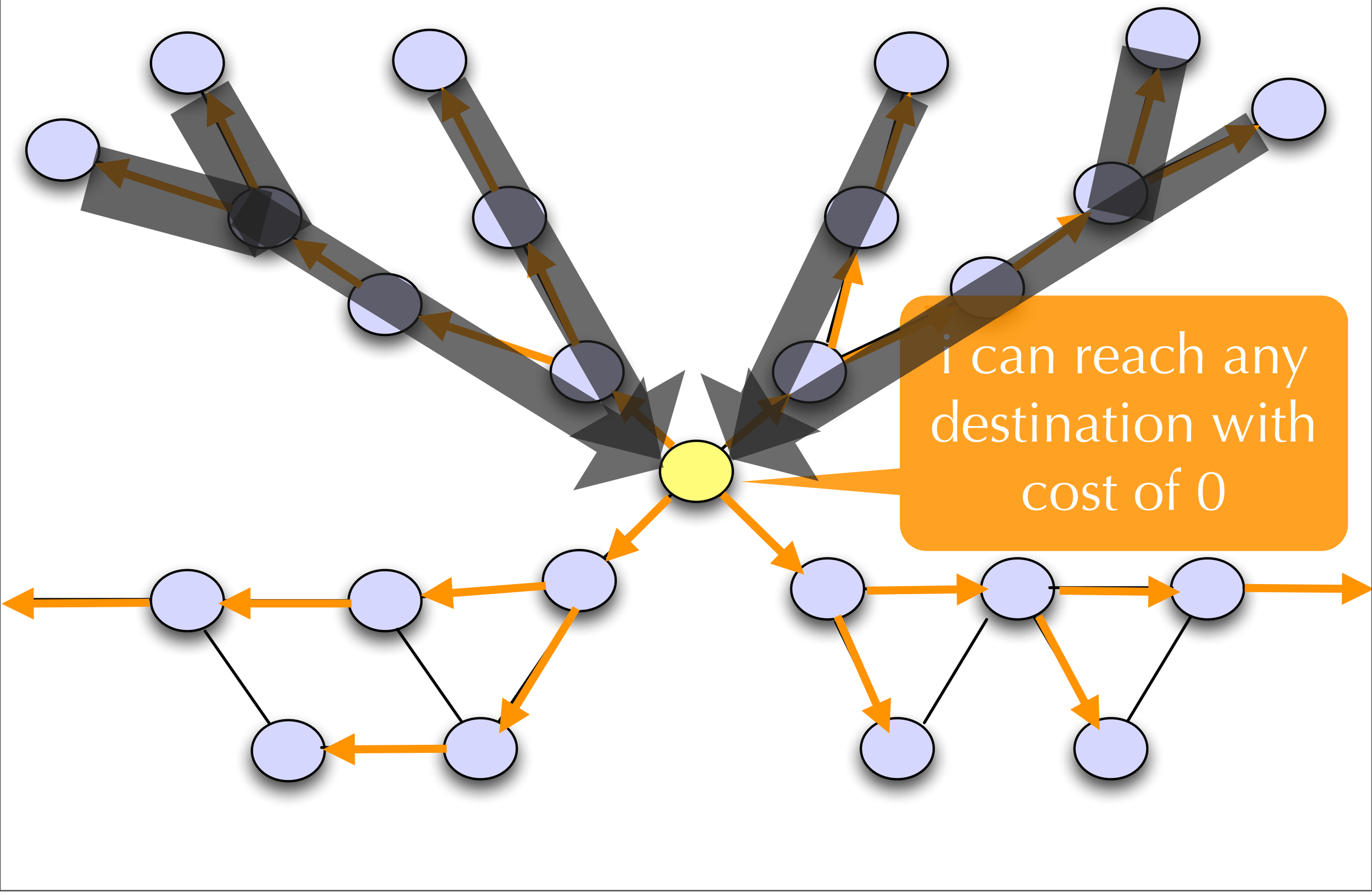
The first problem we consider arises in the context of distributed network algorithms, where a malicious or misconfigured node injects and spreads incorrect routing state throughout the network. Consider this example network of routers running the distance vector algorithm. Here the yellow router is compromised and falsely announces that is can reach any destination with a cost of 0. this false routing state propagates network-wide (as shown by the orange arrows). This causes many network routers to incorrectly route via the compromised node. This type of false state can degrade the performance of the network or render it unusable.

Ch 1: Network Router Failure



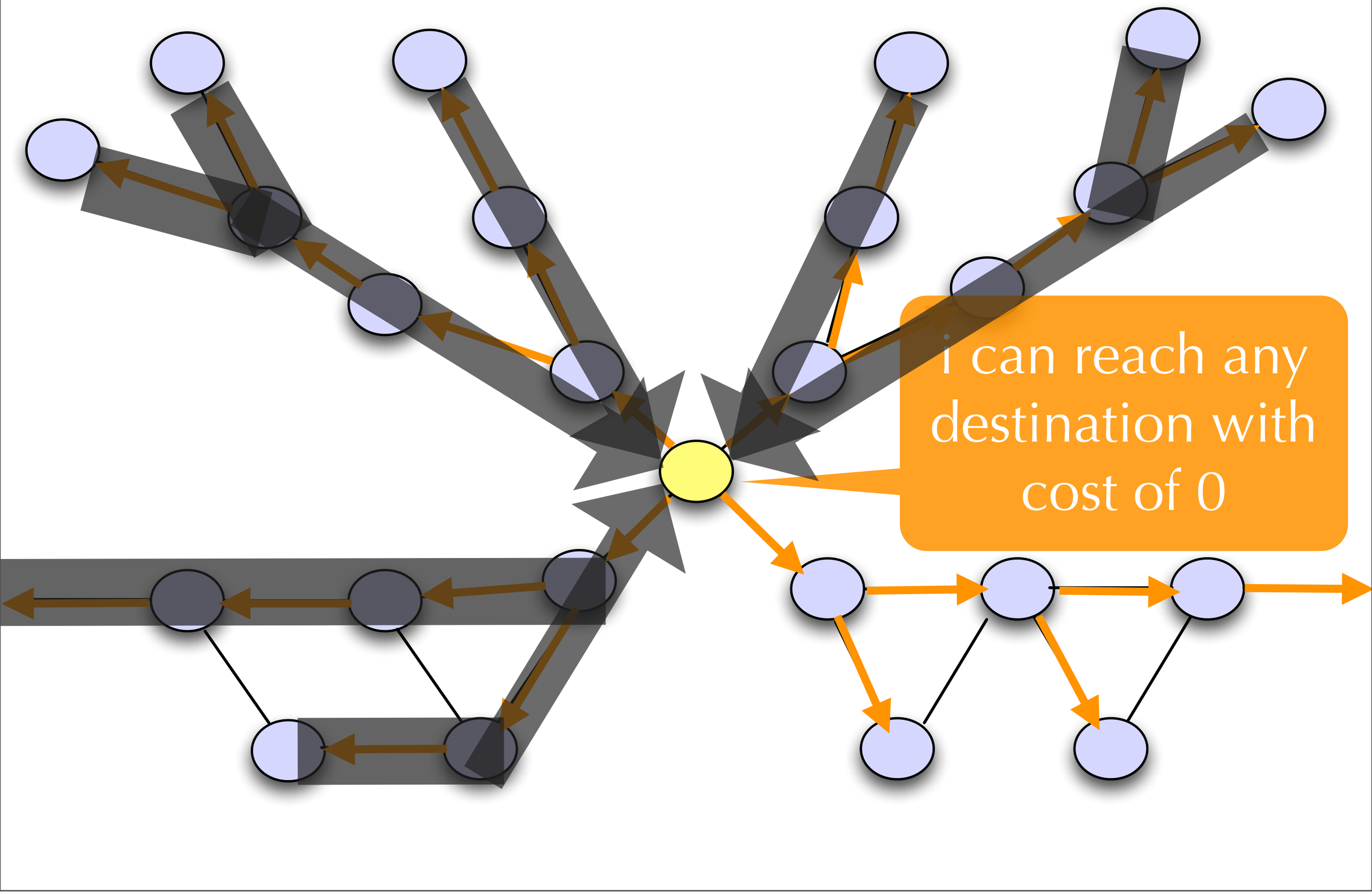
The first problem we consider arises in the context of distributed network algorithms, where a malicious or misconfigured node injects and spreads incorrect routing state throughout the network. Consider this example network of routers running the distance vector algorithm. Here the yellow router is compromised and falsely announces that is can reach any destination with a cost of 0. this false routing state propagates network-wide (as shown by the orange arrows). This causes many network routers to incorrectly route via the compromised node. This type of false state can degrade the performance of the network or render it unusable.

Ch 1: Network Router Failure



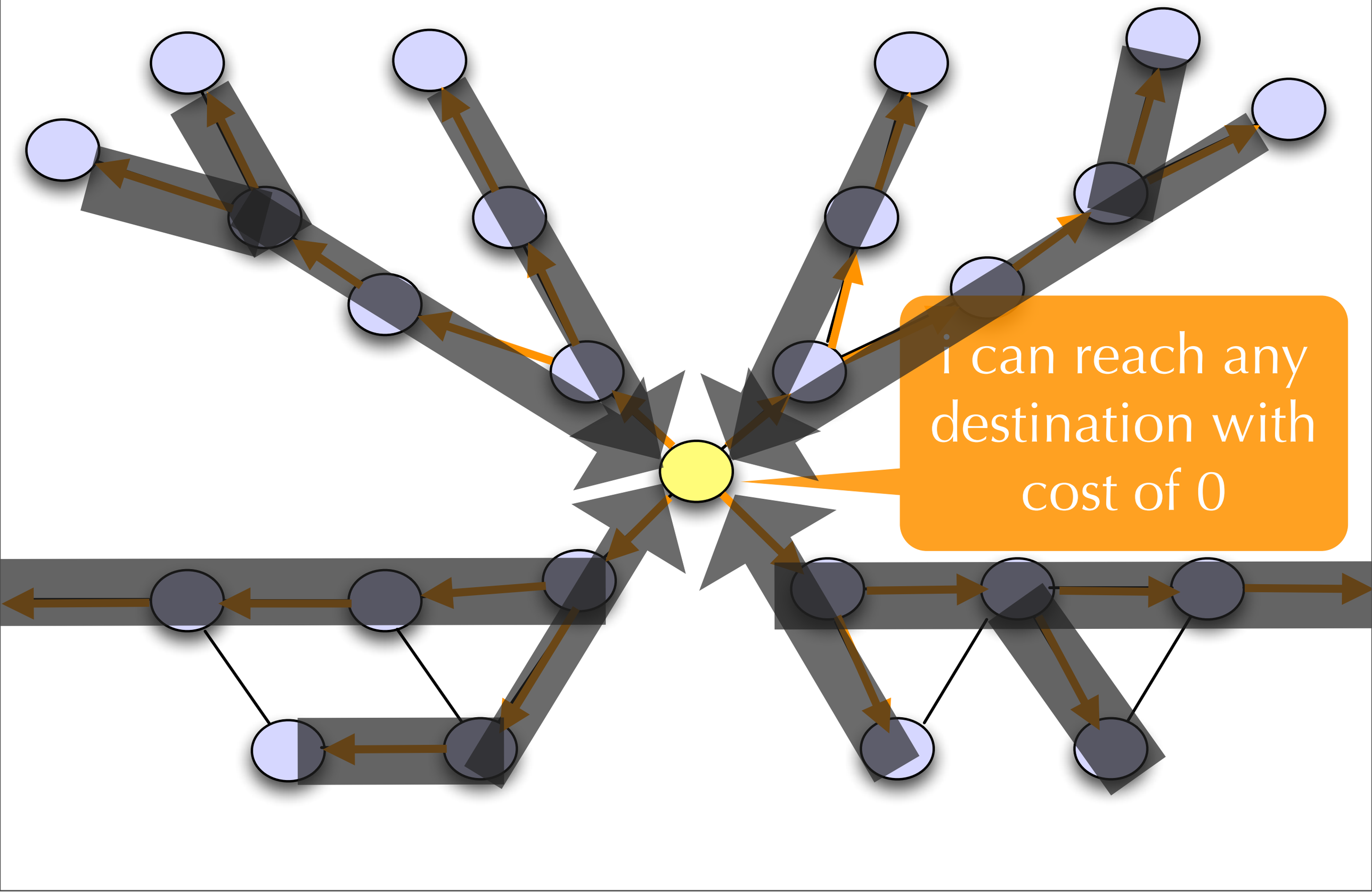
The first problem we consider arises in the context of distributed network algorithms, where a malicious or misconfigured node injects and spreads incorrect routing state throughout the network. Consider this example network of routers running the distance vector algorithm. Here the yellow router is compromised and falsely announces that is can reach any destination with a cost of 0. this false routing state propagates network-wide (as shown by the orange arrows). This causes many network routers to incorrectly route via the compromised node. This type of false state can degrade the performance of the network or render it unusable.

Ch 1: Network Router Failure



The first problem we consider arises in the context of distributed network algorithms, where a malicious or misconfigured node injects and spreads incorrect routing state throughout the network. Consider this example network of routers running the distance vector algorithm. Here the yellow router is compromised and falsely announces that is can reach any destination with a cost of 0. this false routing state propagates network-wide (as shown by the orange arrows). This causes many network routers to incorrectly route via the compromised node. This type of false state can degrade the performance of the network or render it unusable.

Ch 1: Network Router Failure



The first problem we consider arises in the context of distributed network algorithms, where a malicious or misconfigured node injects and spreads incorrect routing state throughout the network. Consider this example network of routers running the distance vector algorithm. Here the yellow router is compromised and falsely announces that is can reach any destination with a cost of 0. this false routing state propagates network-wide (as shown by the orange arrows). This causes many network routers to incorrectly route via the compromised node. This type of false state can degrade the performance of the network or render it unusable.

April 25, 1997 7:00 PM PDT

Router glitch cuts Net access

By CNET News.com Staff
Staff Writer, CNET News

Related Stories

Net blackout hits some regions
April 25, 1997

Software blamed for AOL blackout
February 5, 1997

WorldNet service restored
November 9, 1996

Web gets an Olympian workout
July 13, 1996

What started out as a router glitch at a small Internet service provider in Virginia today triggered a major outage in Internet access across the country, lasting more than two hours in some places.

The problem started this morning at 8:30 a.m. PT when MAI Network Services, an ISP headquartered in a McLean, Virginia, unwittingly passed some bad router information from one of its customers onto Sprint, one of the largest Internet backbone operators in North America. Because Sprint's backbone is used by so many other smaller ISPs, the router problem was echoed, causing temporary network outages across the country and, perhaps, internationally.

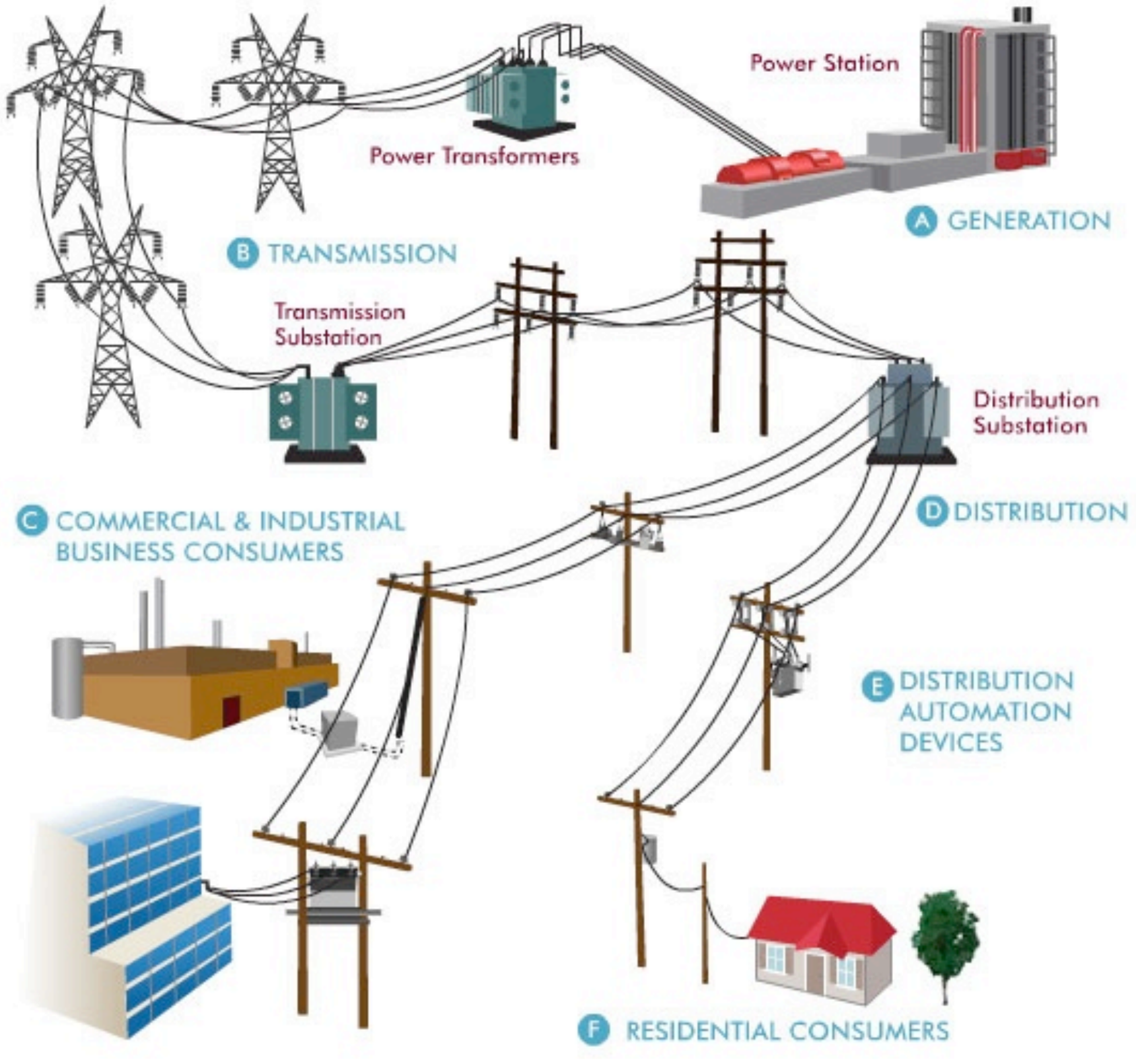
The outage underscored the fragility of the infrastructure that underlies the global network and how easily a problem with one small ISP can be amplified throughout the Internet. Even so, the Net displayed a remarkable resilience that seems to disprove its doomsayers, who have predicted that the network is on the verge of collapse.

"This particular thing was a confluence of two or three things happening--human error, bug, and some policy problems--that all came together on the same day," said Jack Rickard, publisher of *BoardWatch* magazine.

"There are probably a hundred guys in back rooms keeping this stuff together, just barely," Ricard said of the Internet.

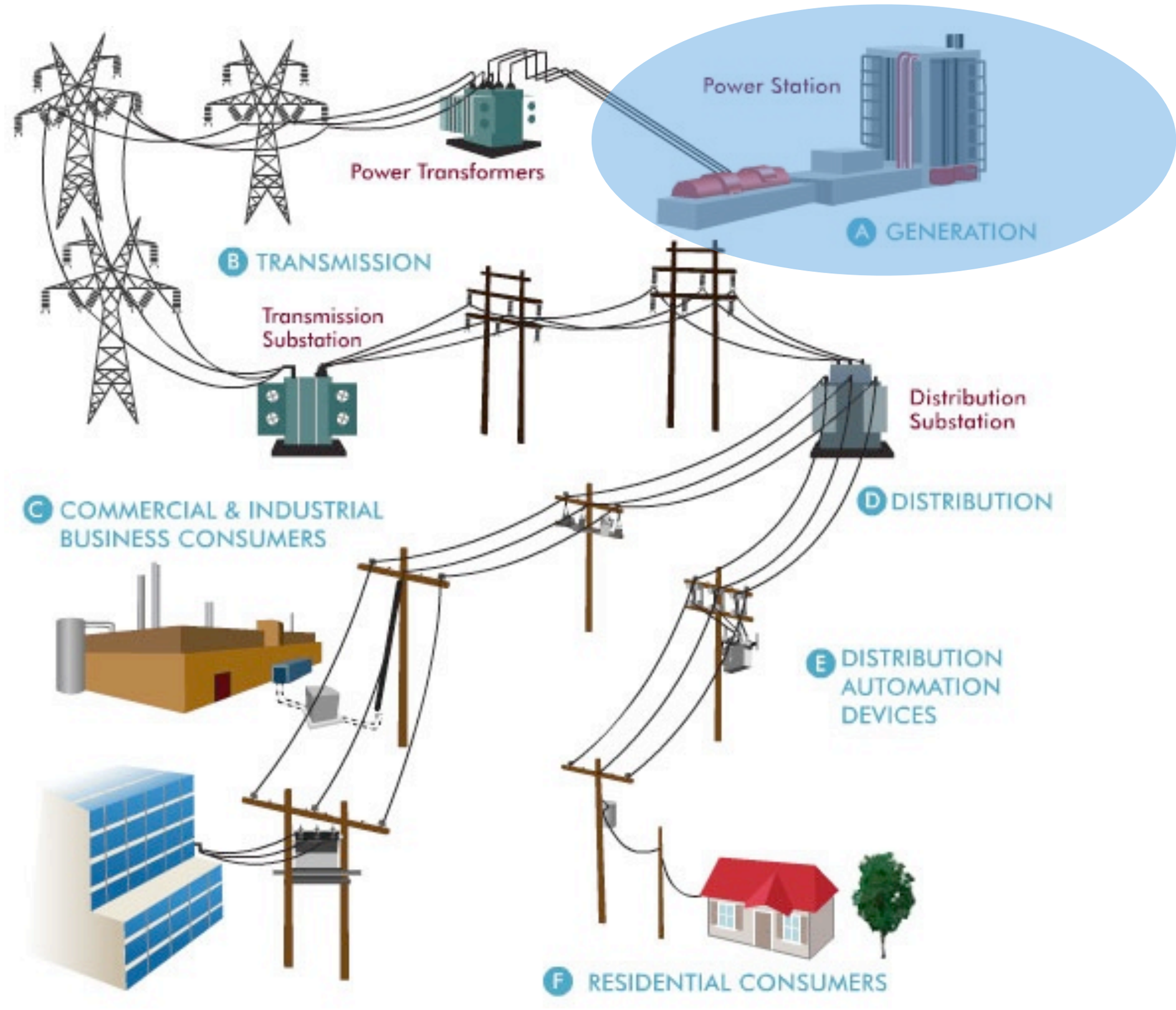
One such case arose in 1997, when a significant portion of Internet traffic was routed through a single misconfigured router that had spread false routing state to several Internet routers. As a result, a large portion of the Internet became inoperable for several hours.

Smart Grid Definition



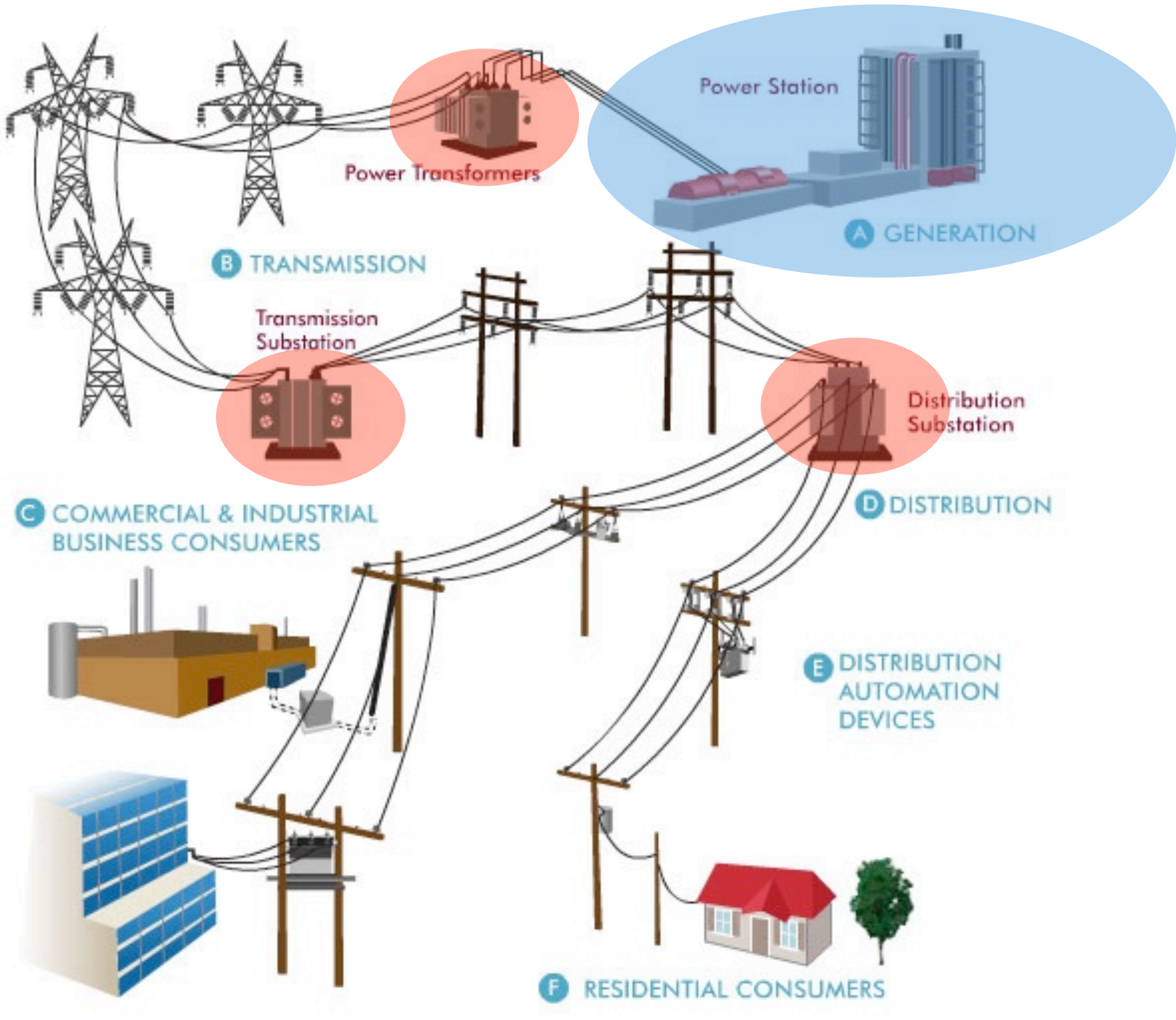
The second two problems we consider concern the electric power grid and what is termed the “smart grid”. An electric power grid consists of a set of buses - power generation centers, electric substations, or aggregation points of electrical loads - and transmission lines connecting those buses. We refer to modern and future electric power grids that automate power grid operations using sensors and wide-area communication as the smart grid.

Smart Grid Definition



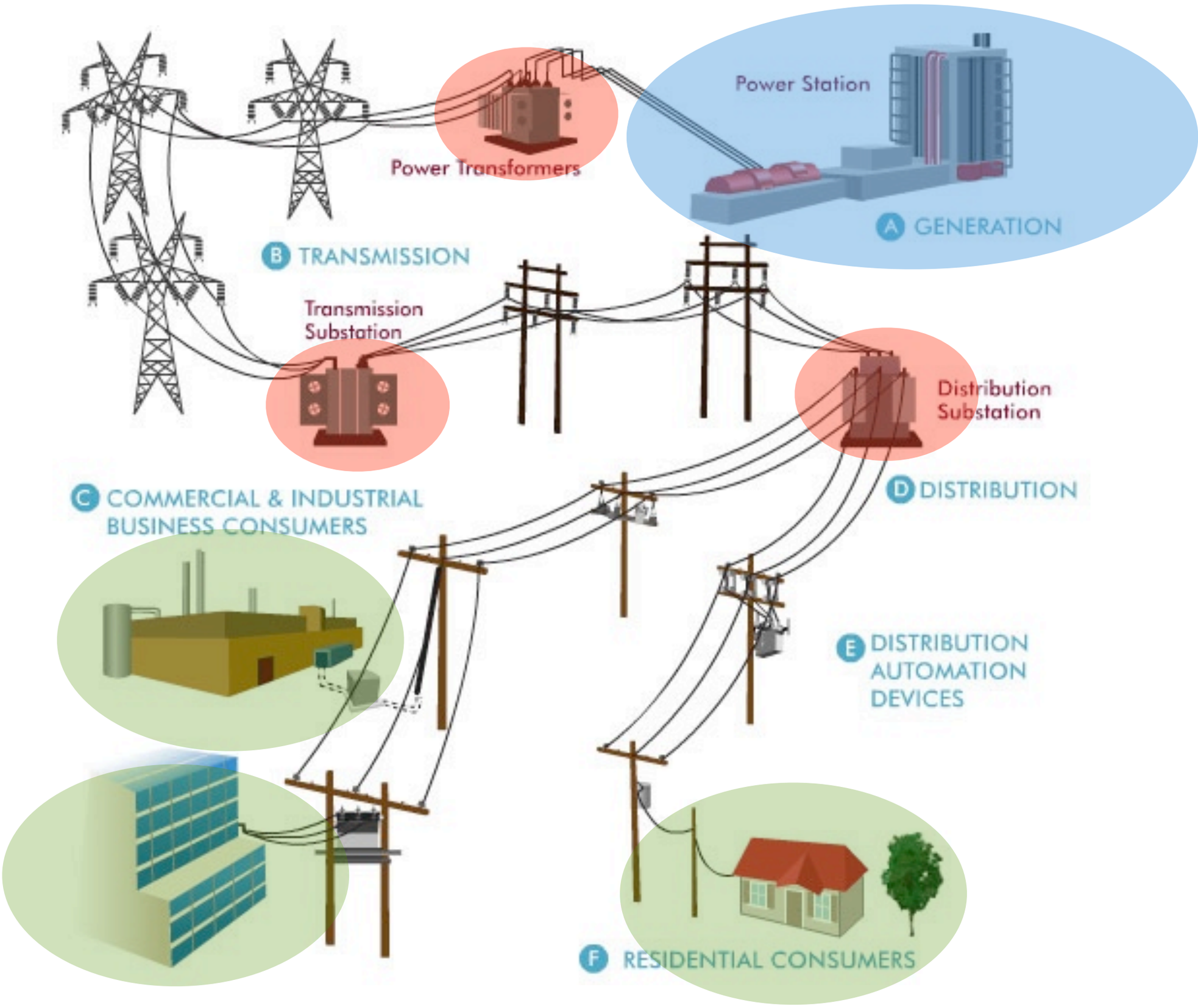
The second two problems we consider concern the electric power grid and what is termed the “smart grid”. An electric power grid consists of a set of buses - power generation centers, electric substations, or aggregation points of electrical loads - and transmission lines connecting those buses. We refer to modern and future electric power grids that automate power grid operations using sensors and wide-area communication as the smart grid.

Smart Grid Definition



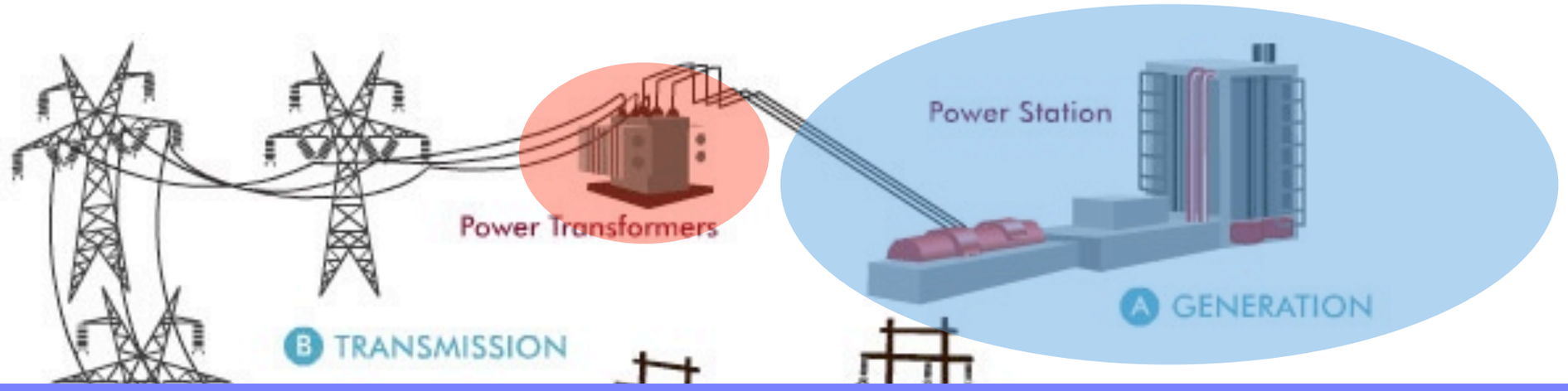
The second two problems we consider concern the electric power grid and what is termed the “smart grid”. An electric power grid consists of a set of buses - power generation centers, electric substations, or aggregation points of electrical loads - and transmission lines connecting those buses. We refer to modern and future electric power grids that automate power grid operations using sensors and wide-area communication as the smart grid.

Smart Grid Definition



The second two problems we consider concern the electric power grid and what is termed the “smart grid”. An electric power grid consists of a set of buses - power generation centers, electric substations, or aggregation points of electrical loads - and transmission lines connecting those buses. We refer to modern and future electric power grids that automate power grid operations using sensors and wide-area communication as the smart grid.

Smart Grid Definition



in power grid reliability is #1 priority + deploying smart grid sensors is key to improving grid reliability

The second two problems we consider concern the electric power grid and what is termed the “smart grid”. An electric power grid consists of a set of buses - power generation centers, electric substations, or aggregation points of electrical loads - and transmission lines connecting those buses. We refer to modern and future electric power grids that automate power grid operations using sensors and wide-area communication as the smart grid.

PMU: Smart Grid Sensor

- high frequency voltage and current measurements
  - measures the “pulse” of the power grid

Phasor Measurement Units, or PMUs, is the sensor currently being deployed on power grids worldwide to help better manage and operate the power grid. PMUs measure voltage and current at electrical buses and transmission lines at a high sampling rate. In this way PMUs can measure the instantaneous health of the power grid. The last 2 parts of this thesis consider problems related to PMUs.

Ch 2+3: Smart Grid Failures

- Ch 2: PMU sensor failure
- Ch 3: link failures in communication network used to disseminate PMU measurements

In the 2nd part of this thesis we look at the failure of the PMU sensors themselves. While in the third and final section of this thesis we look at the failure of communication links in the network used to disseminate critical PMU sensor data. Either of these failures can cause critical errors in smart grid applications used to control, operate, and manage a power grid.

Ch 2+3: Smart Grid Failures

- Ch 2: PMU sensor failure
- Ch 3: link failures in communication network used to disseminate PMU measurements

these failures can cause critical errors in smart grid applications used to operate the grid

In the 2nd part of this thesis we look at the failure of the PMU sensors themselves. While in the third and final section of this thesis we look at the failure of communication links in the network used to disseminate critical PMU sensor data. Either of these failures can cause critical errors in smart grid applications used to control, operate, and manage a power grid.

theguardian

India blackouts leave 700 million without power

Power cuts plunge 20 of India's 28 states into darkness as energy suppliers fail to meet growing demand

Helen Pidd in Delhi
The Guardian, Tuesday 31 July 2012 10.48 EDT

More than 700 million people in India have been left without power in the world's worst blackout of recent times, leading to fears that protests and even riots could follow if the country's electricity supply continues to fail to meet growing demand.

Twenty of India's 28 states were hit by power cuts, along with the capital, New Delhi, when three of the country's five electricity grids failed at lunchtime.

As engineers struggled for hours to fix the problem, hundreds of trains failed, leaving passengers stranded along thousands of miles of track from Kashmir in the north to Nagaland on the eastern border with Burma.

Traffic lights went out, causing jams in New Delhi, Kolkata and other cities. Surgical operations were cancelled across the country, with nurses at one hospital just outside Delhi having to operate life-saving equipment manually when back-up generators failed.

In the worst case, these component failures can lead to a cascade of power grid failures like the recent 2012 power grid failures in India where an estimated 700 million people were affected. I want to emphasize that PMUs were and are not currently being used in India and thus are not to blame for this failure. However, blackouts of this magnitude will be possible when PMUs are widely deployed.

Automated Recovery Is Needed

- automated recovery needed to reduce
  - short-term disruption
  - increase long-term network survivability

Recovering quickly from the component failures just discussed are vital to both reducing short-term disruption and increasing long-term network survivability. In this thesis, we design algorithms that make networks robust to component failure.

Automated Recovery Is Needed

- automated recovery needed to reduce
  - short-term disruption
  - increase long-term network survivability

thesis designs algorithms to make networks robust to these component failures

Recovering quickly from the component failures just discussed are vital to both reducing short-term disruption and increasing long-term network survivability. In this thesis, we design algorithms that make networks robust to component failure.

Unifying The 3 Subproblems

- each problem considers network robustness in the face of component failure
- our solutions
  - on-demand recovery for distributed network algorithms
  - preplanned recovery for smart grid apps where reliability is key

the 3 problems we address all consider the failure of network components and our solutions aim to improve the robustness of these networks through automated recovery. We propose
(1) on-demand recovery algorithms for distributed network algorithms that optimize for control message overhead and convergence time, and
(2) preplanned approaches to recovery for electric power grid applications, where reliability is key.

Talk Outline

Here is the outline of this talk

Talk Outline

- thesis introduction

Here is the outline of this talk

Talk Outline

- thesis introduction
- background on electric power grid + smart grid

Here is the outline of this talk

Talk Outline

- thesis introduction
- background on electric power grid + smart grid
- placement of smart grid sensors to enable measurement error detection

Here is the outline of this talk

Talk Outline

- thesis introduction
- background on electric power grid + smart grid
- placement of smart grid sensors to enable measurement error detection
- recovery from failed communication links in a smart grid

Here is the outline of this talk

Talk Outline

- thesis introduction
- background on electric power grid + smart grid
- placement of smart grid sensors to enable measurement error detection
- recovery from failed communication links in a smart grid
- recovery from malicious nodes injecting false routing state

Here is the outline of this talk

Talk Outline

- thesis introduction
- background on electric power grid + smart grid
- placement of smart grid sensors to enable measurement error detection
- recovery from failed communication links in a smart grid
- recovery from malicious nodes injecting false routing state
- outline for future work and conclusions

Here is the outline of this talk

Talk Outline

- thesis introduction
- background on electric power grid + smart grid
- placement of smart grid sensors to enable measurement error detection
- recovery from failed communication links in a smart grid
- recovery from malicious nodes injecting false routing state
- outline for future work and conclusions

the technical chapters highlighted in blue are complete.

Talk Outline

- theme of thesis and problem description
- background on electric power grid + smart grid
- placement of smart grid sensors to enable measurement error detection
- recovery from failed communication links in a smart grid
- recovery from malicious nodes injecting false routing state
- outline for future work and conclusions

"recovery from failed communication links in a smart grid" marks work in progress.

Talk Outline

- theme of thesis and problem description
- background on electric power grid + smart grid
- recovery from failed communication links in a smart grid
- placement of smart grid sensors to enable measurement error detection
- recovery from malicious nodes injecting false routing state
- conclusions and outline for future work

Thesis Timeline: Completed Work

Thesis Timeline: Completed Work

- Ch 1: "Recovery from False Routing State in Distributed Routing Algorithms"
  - published in *IFIP Networking 2010 Conference*
  - chapter is done

unless the committee has suggestions

Thesis Timeline: Completed Work

- Ch 1: "Recovery from False Routing State in Distributed Routing Algorithms"
  - published in *IFIP Networking 2010 Conference*
  - chapter is done
- Ch 2: "PMU Sensor Placement for Measurement Error Detection in the Smart Grid"
  - published in *e-Energy 2012*
  - chapter is done

unless the committee has suggestions

Thesis Timeline: Work in Progress

- Ch. 3: "Recovery from Link Failures in Smart Grid Communication Network"
  - problem well-defined
  - algorithms, implementation, analysis, and evaluation yet to be completed

Thesis Timeline: Work In Progress

Thesis Timeline: Work In Progress

- Ch. 3 milestones

Thesis Timeline: Work In Progress

- Ch. 3 milestones
  - implement FAILED-LINK using POX Openflow controller

Thesis Timeline: Work In Progress

- Ch. 3 milestones
  - implement FAILED-LINK using POX Openflow controller
  - test + profile FAILED-LINK

Thesis Timeline: Work In Progress

- Ch. 3 milestones
  - implement FAILED-LINK using POX Openflow controller
  - test + profile FAILED-LINK
  - implement MIN-FLOWS, MIN-SINKS, + MIN-CONTROL using POX Openflow controller

Thesis Timeline: Work In Progress

- Ch. 3 milestones
  - implement FAILED-LINK using POX Openflow controller
  - test + profile FAILED-LINK
  - implement MIN-FLOWS, MIN-SINKS, + MIN-CONTROL using POX Openflow controller
  - complexity analysis

Thesis Timeline: Work In Progress

- Ch. 3 milestones
  - implement FAILED-LINK using POX Openflow controller
  - test + profile FAILED-LINK
  - implement MIN-FLOWS, MIN-SINKS, + MIN-CONTROL using POX Openflow controller
  - complexity analysis
  - simulation-based study of FAILED-LINK, MIN-FLOWS, MIN-SINKS, MIN-CONTROL

Thesis Timeline: Work In Progress

- Ch. 3 milestones
  - implement FAILED-LINK using POX Openflow controller 3 weeks - Feb
  - test + profile FAILED-LINK
  - implement MIN-FLOWS, MIN-SINKS, + MIN-CONTROL using POX Openflow controller
  - complexity analysis
  - simulation-based study of FAILED-LINK, MIN-FLOWS, MIN-SINKS, MIN-CONTROL

Thesis Timeline: Work In Progress

- Ch. 3 milestones
  - implement FAILED-LINK using POX Openflow controller 3 weeks - Feb
  - test + profile FAILED-LINK 2 weeks - March
  - implement MIN-FLOWS, MIN-SINKS, + MIN-CONTROL using POX Openflow controller
  - complexity analysis
  - simulation-based study of FAILED-LINK, MIN-FLOWS, MIN-SINKS, MIN-CONTROL

Thesis Timeline: Work In Progress

- Ch. 3 milestones
  - implement FAILED-LINK using POX Openflow controller 3 weeks - Feb
  - test + profile FAILED-LINK 2 weeks - March
  - implement MIN-FLOWS, MIN-SINKS, + MIN-CONTROL using POX Openflo 4 weeks - May
  - complexity analysis
  - simulation-based study of FAILED-LINK, MIN-FLOWS, MIN-SINKS, MIN-CONTROL

Thesis Timeline: Work In Progress

- Ch. 3 milestones
  - implement FAILED-LINK using POX Openflow controller — 3 weeks - Feb
  - test + profile FAILED-LINK — 2 weeks - March
  - implement MIN-FLOWS, MIN-SINKS, + MIN-CONTROL using POX Openflow — 4 weeks - May
  - complexity analysis — 2 weeks - May
  - simulation-based study of FAILED-LINK, MIN-FLOWS, MIN-SINKS, MIN-CONTROL

Thesis Timeline: Work In Progress

- Ch. 3 milestones
  - implement FAILED-LINK using POX Openflow controller — 3 weeks - Feb
  - test + profile FAILED-LINK — 2 weeks - March
  - implement MIN-FLOWS, MIN-SINKS, + MIN-CONTROL using POX Openflo — 4 weeks - May
  - complexity analysis — 2 weeks - May
  - simulation-based study of FAILED-LINK, MIN-FLOWS, MIN-SINKS, MIN-CONTROL — 3 weeks - June

Thesis Summary

- consider failure of network components
  - router spreading false routing state
  - smart grid sensor measurement error
  - link failures in smart grid communication network
- proposed algorithms for automated recovery

Backup Slides

(Ch 1) Network Router Failure

- network router fails and spread false routing state
  - bad network performance
  - unusable network

The first problem we consider arises in the context of distributed network algorithms. Here we have a network of routers running a distributed routing algorithm such as distance vector. We consider the problem where a malicious or misconfigured node injects and spreads incorrect routing state throughout the network. Such false state can degrade the performance of the network or render it unusable.