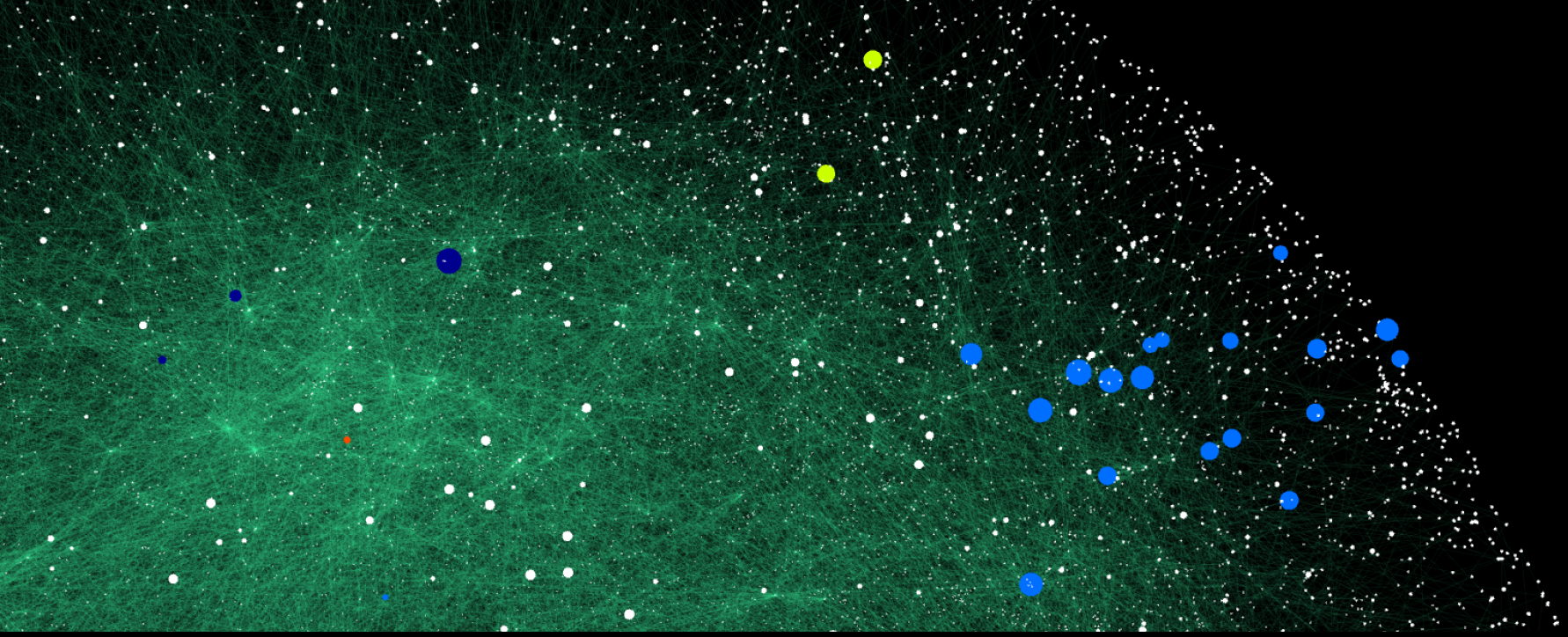


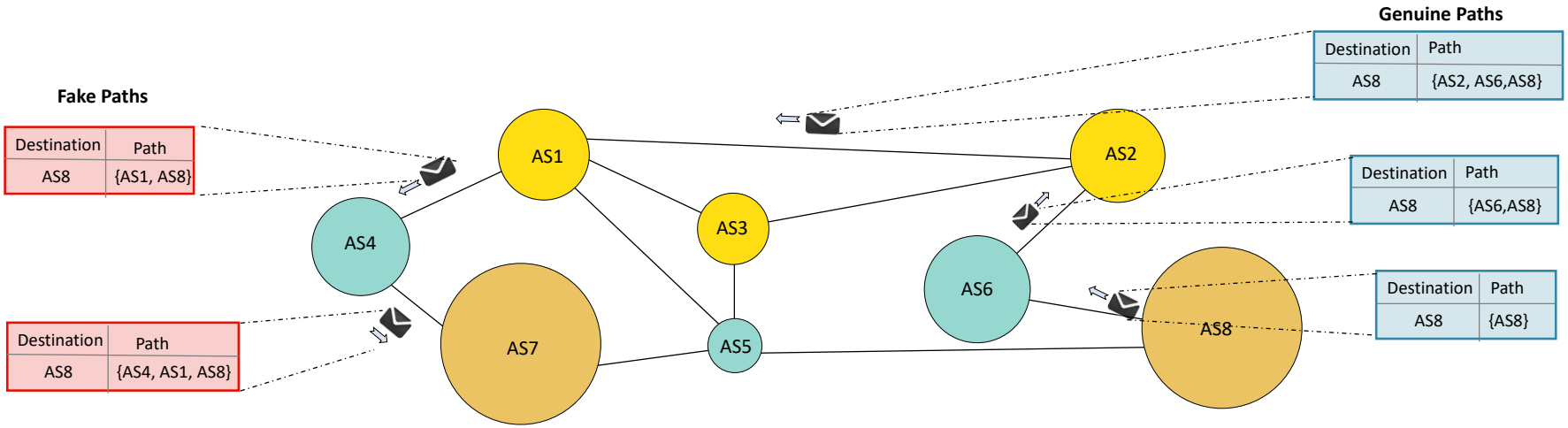
Shortest Path Finding in Incomplete Networks: Implications for BGP Security

Maksim Kitsak, Ph.D.

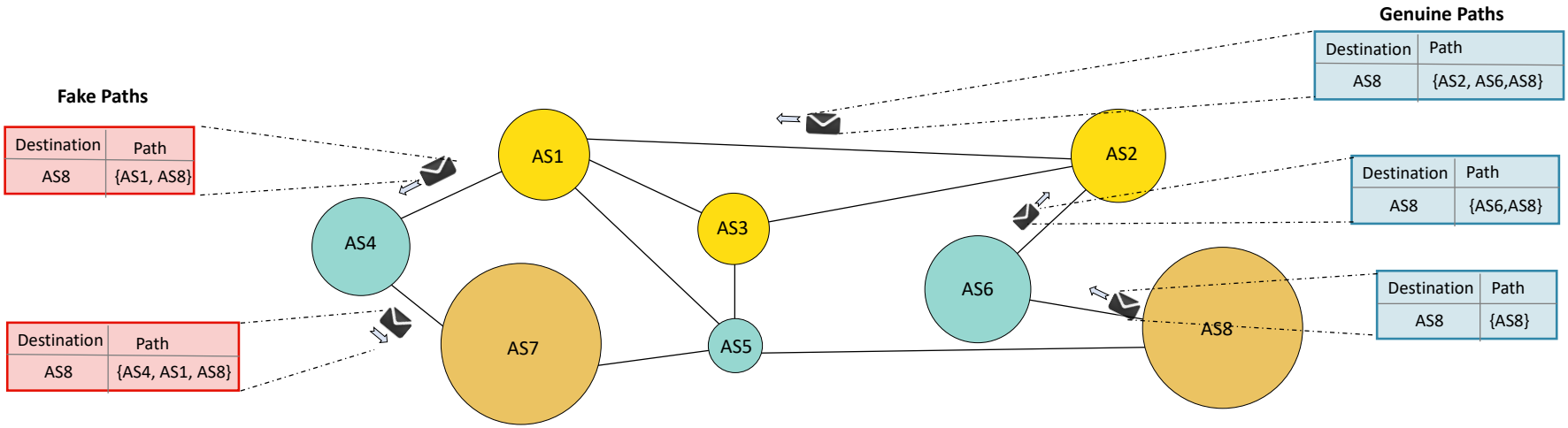
Electrical Engineering, Mathematics and Computer Science
Delft University of Technology

SimulaMet, October 13, 2021

Problem: No rigorous integrity checks for BGP updates



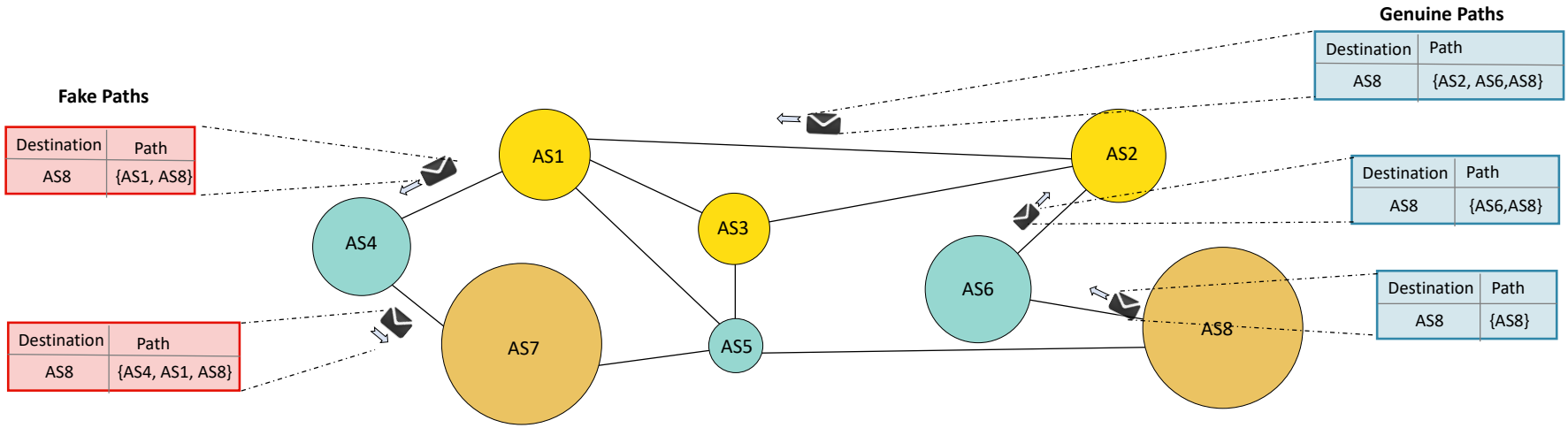
Problem: No rigorous integrity checks for BGP updates



BGP prefix hijack:

AS claims ownership of IP prefixes or claims it may provide transit to a “popular” IP prefix.

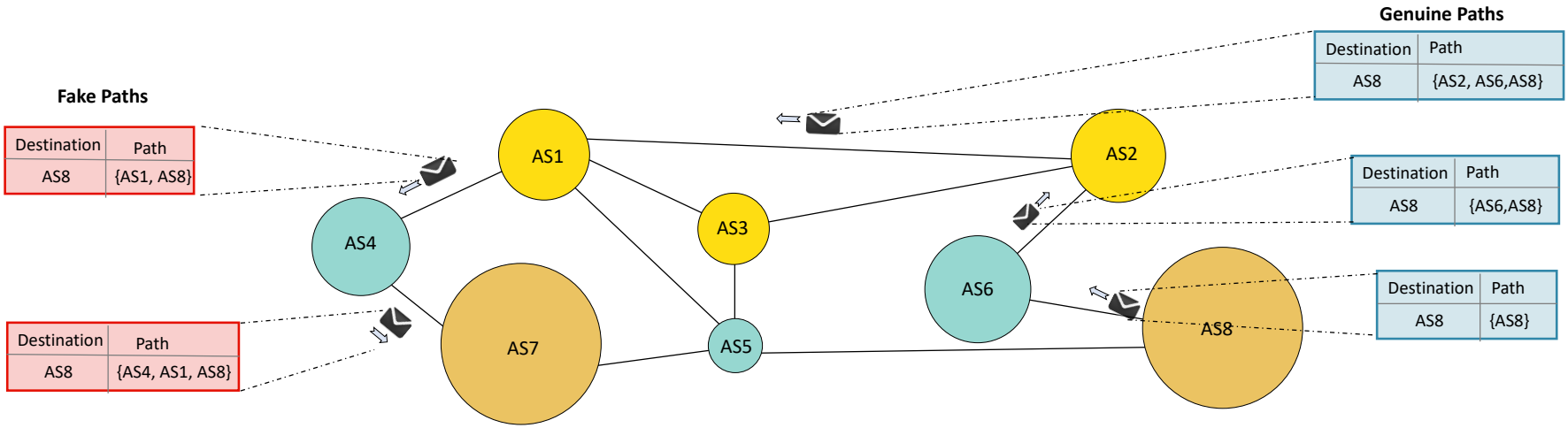
Problem: No rigorous integrity checks for BGP updates



BGP prefix hijack:
AS claims ownership of IP prefixes or claims it may provide transit to a “popular” IP prefix.

Example: 2018 Google “hijack” story
MainOne is the leading connectivity provider AS in West Africa.
MainOne announced it is directly connected to Google AS.
MainOne “tricked” China Telecom into accepting new path to Google AS.
Significant portion of Internet Google traffic was rerouted through China Telecom and crashed against the Chinese (Great) Firewall.

Problem: No rigorous integrity checks for BGP updates



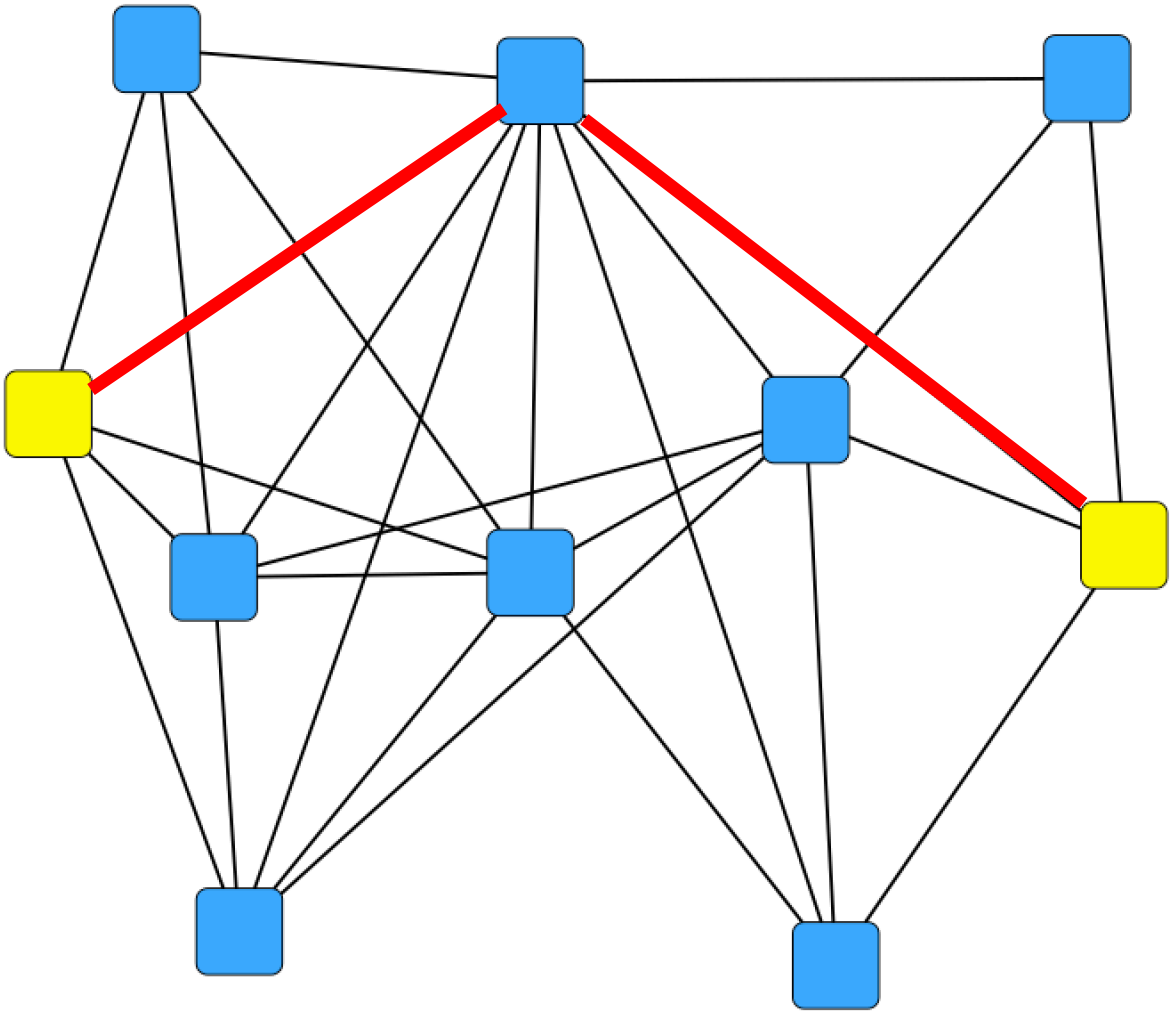
BGP prefix hijack:
AS claims ownership of IP prefixes or claims it may provide transit to a "popular" IP prefix.

Example: 2018 Google "hijack" story
MainOne is the leading connectivity provider AS in West Africa.
MainOne announced it is directly connected to Google AS.
MainOne "tricked" China Telecom into accepting new path to Google AS.
Significant portion of Internet Google traffic was rerouted through China Telecom and crashed against the Chinese (Great) Firewall.

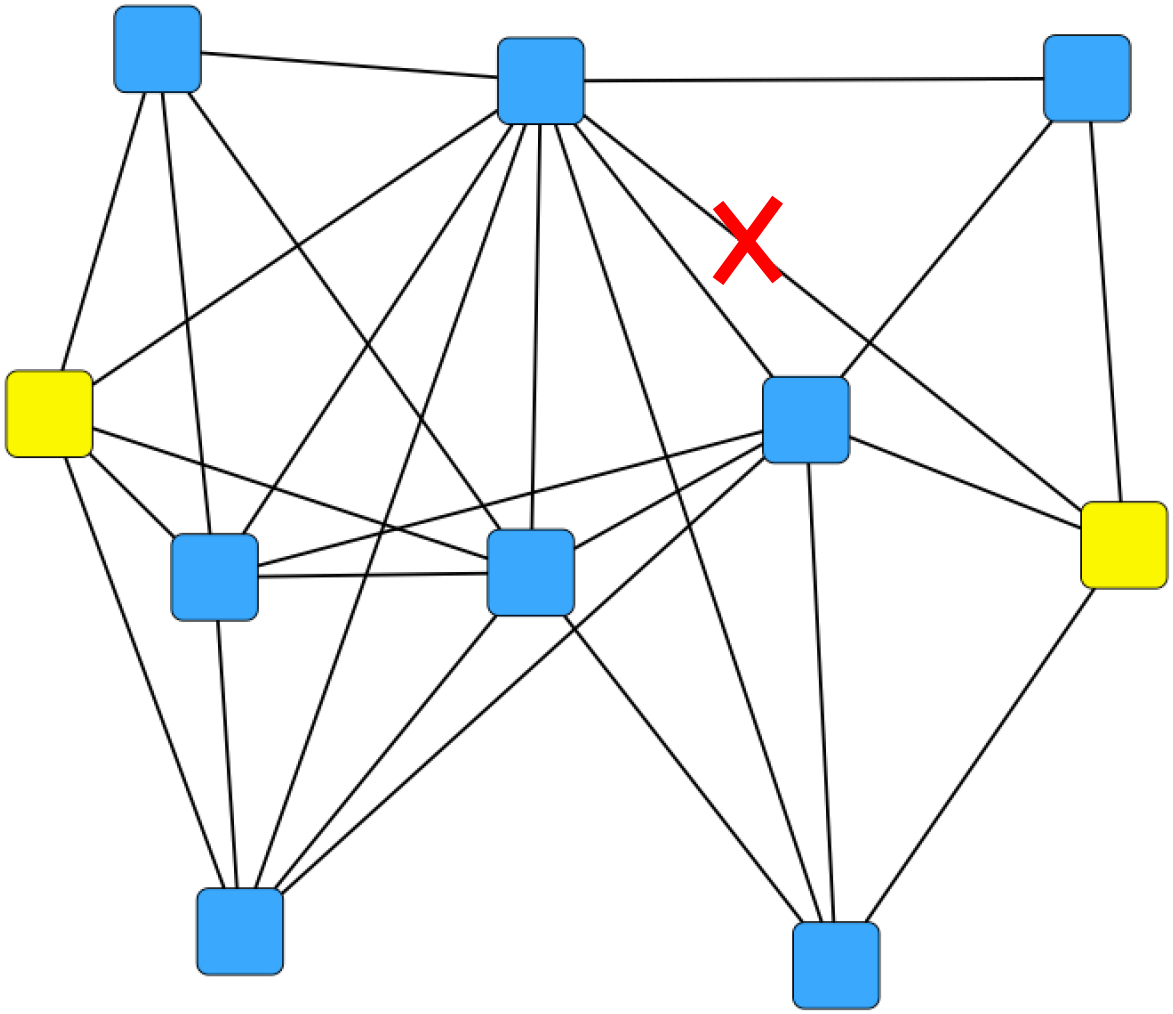
Q: Can ASes reliably validate BGP paths?
Extremely hard problem due to e.g., the private nature of ASes, complexity of Internet measurements, highly-dynamic nature of Internet etc.

Can graph theory help? What if communication paths are shortest?

Shortest path is the smallest sequence of nodes/links from *A* to *B*

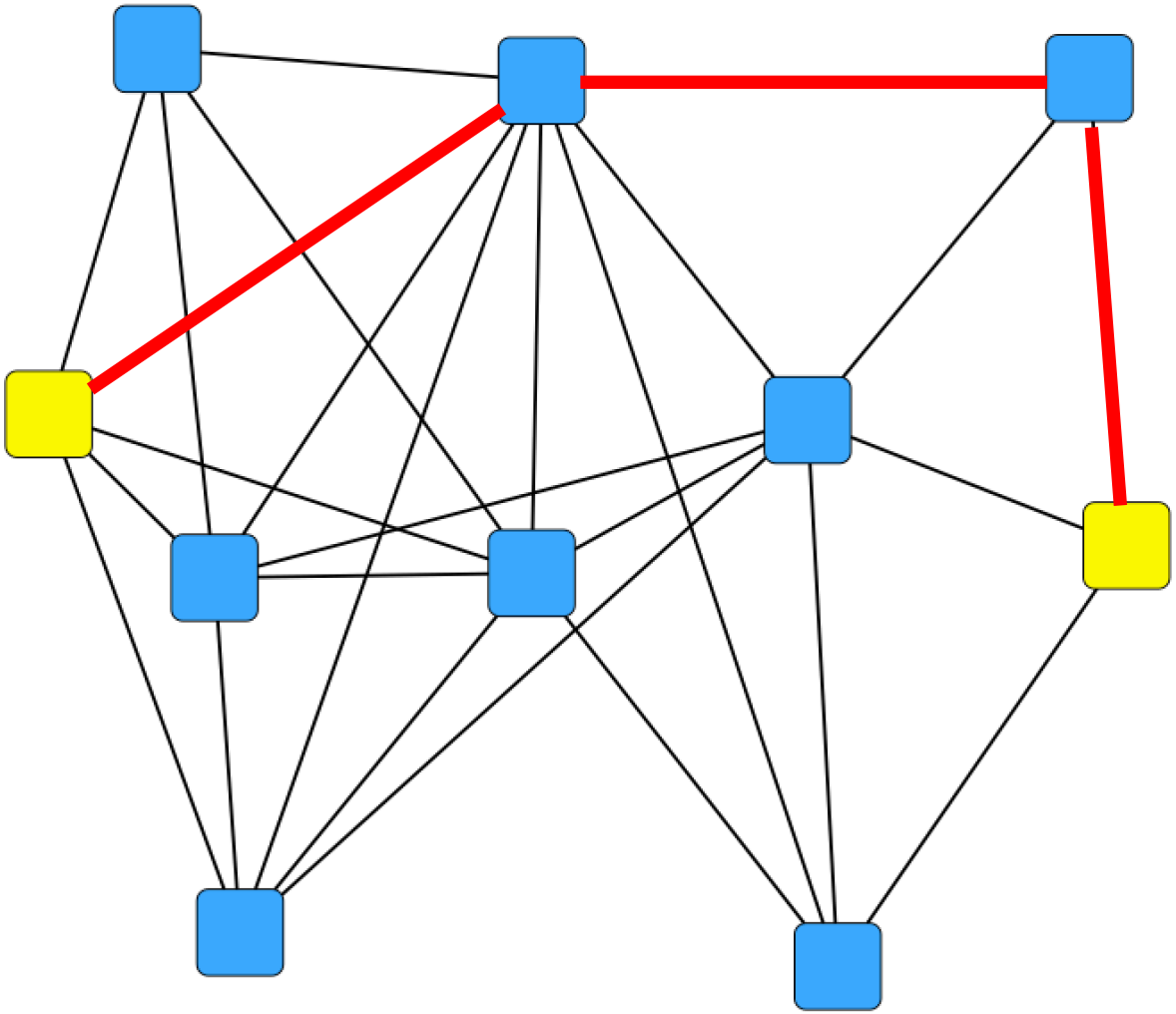


Shortest paths are FRAGILE!



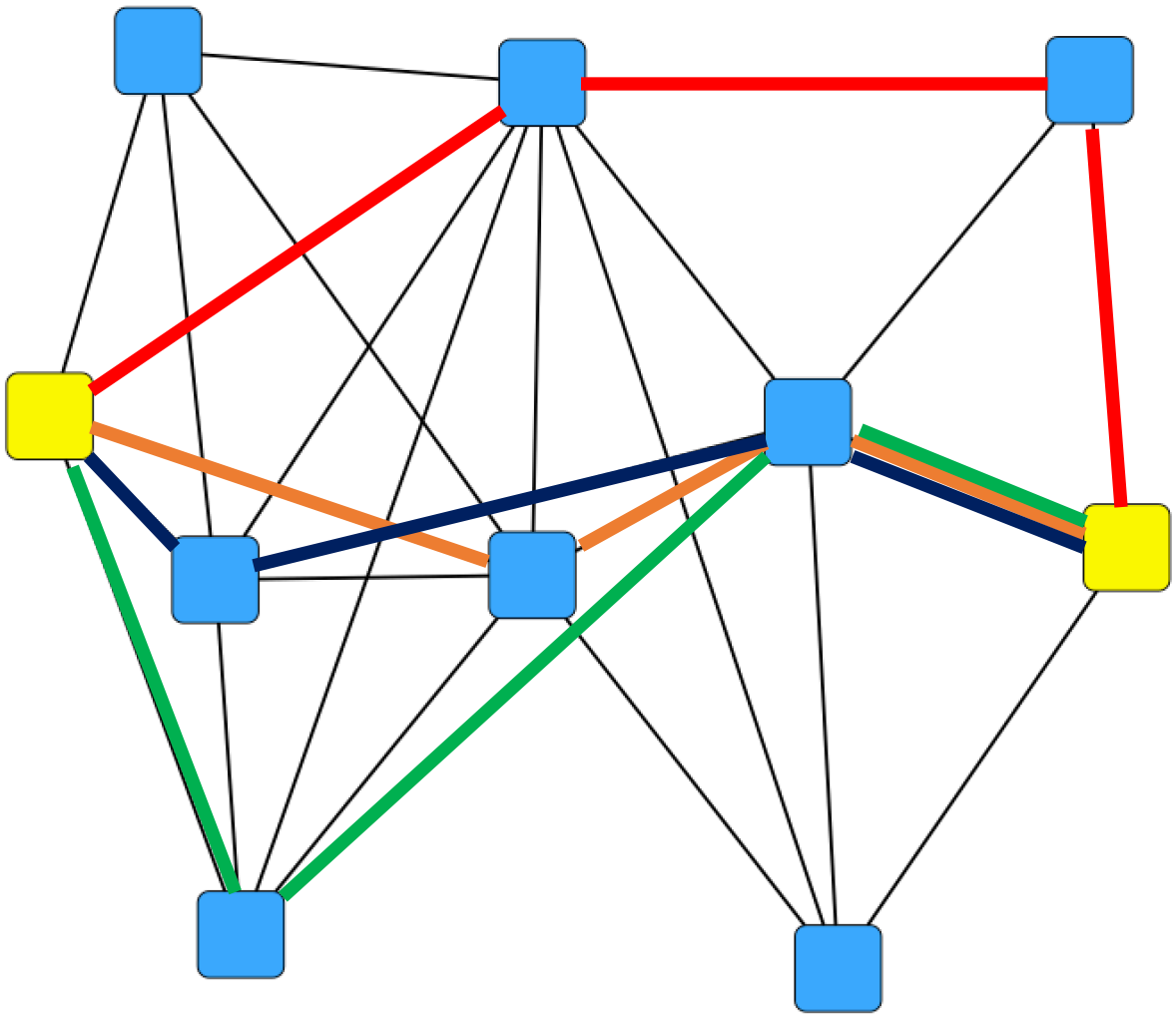
Let us remove a single link from the network….

Shortest paths are FRAGILE!



The shortest path is longer and passes different nodes.

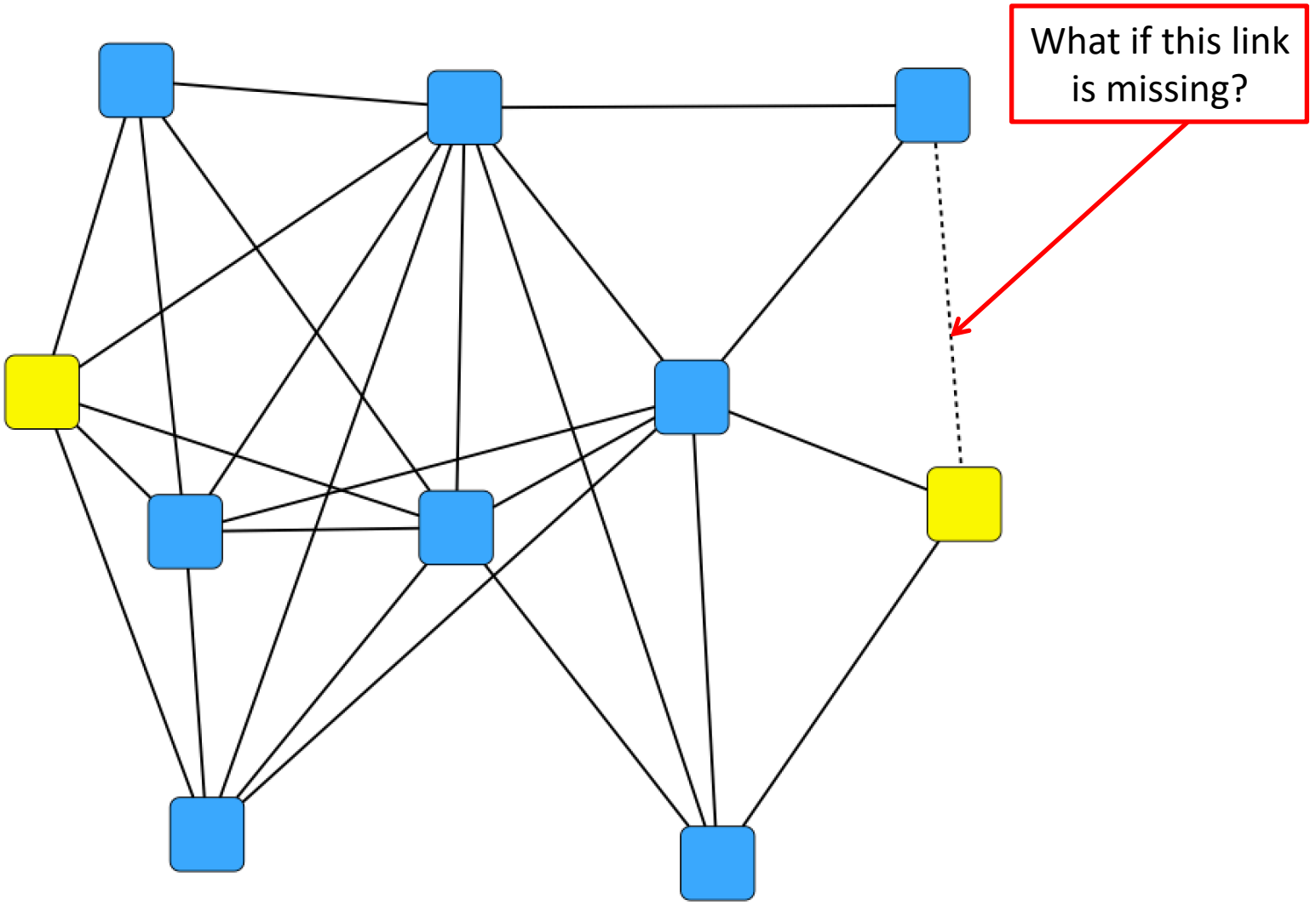
Shortest paths are FRAGILE!



Now there are several paths that use different sets of nodes!

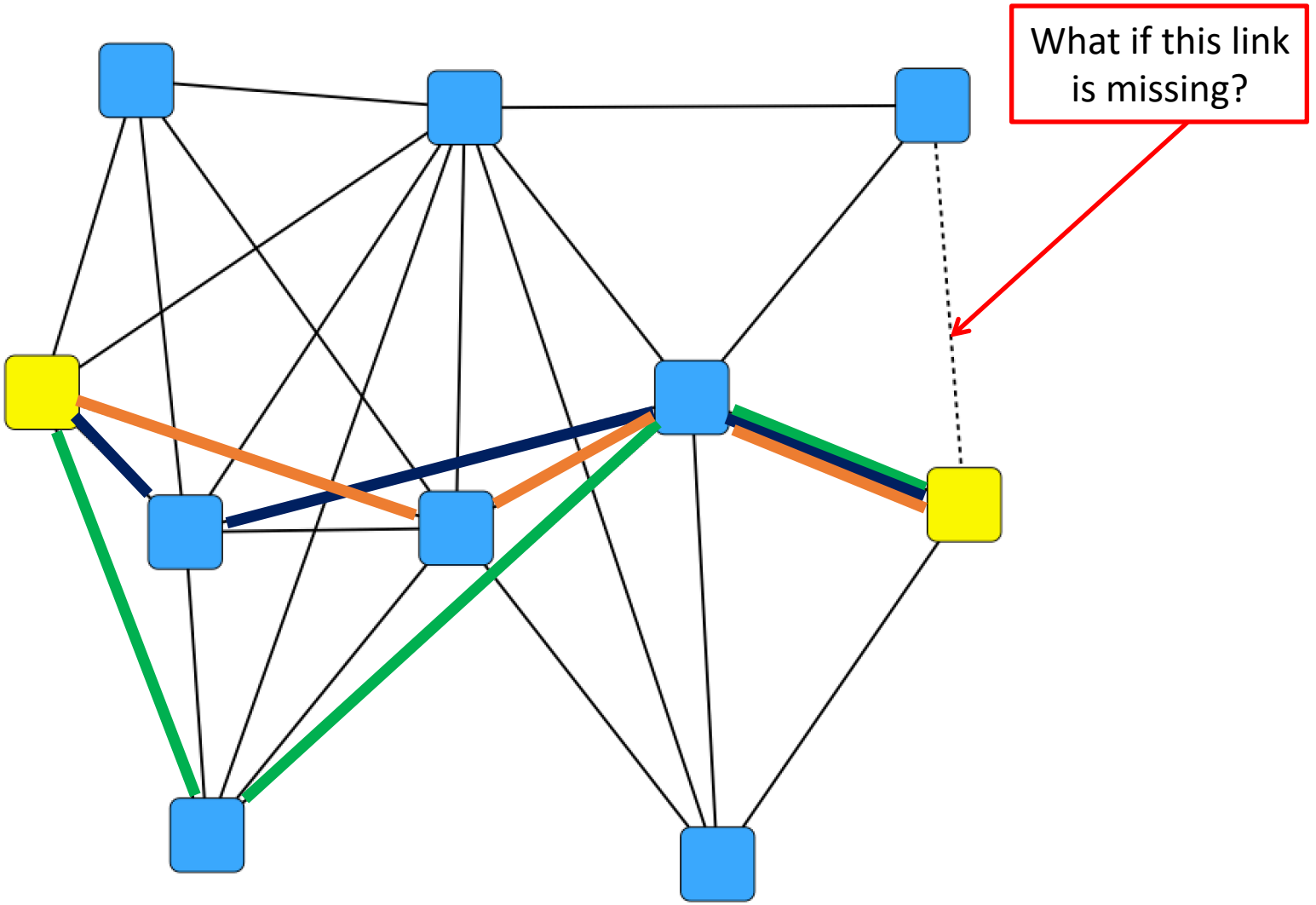
Shortest paths are hard to identify!

Real networks are not fully known (missing links, spurious links)



Shortest paths are hard to identify in incomplete networks

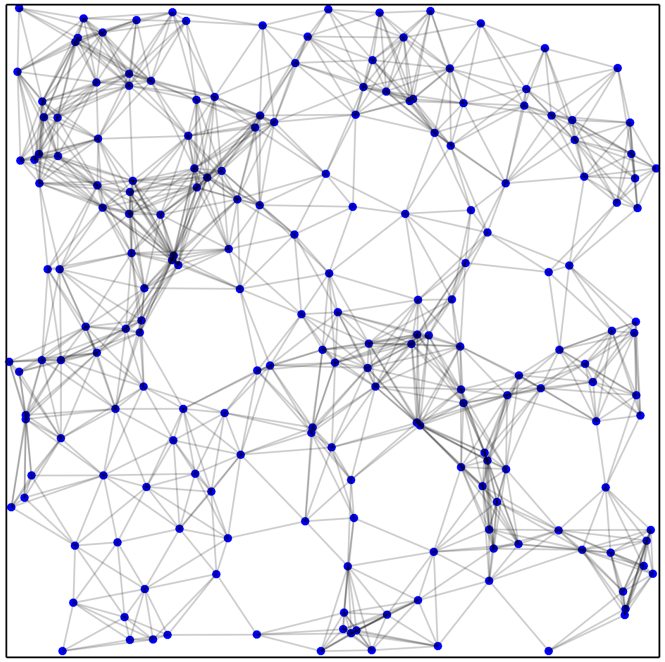
Not all paths are observed!



Shortest paths are not as hard in geometric networks

Random Geometric Graph:

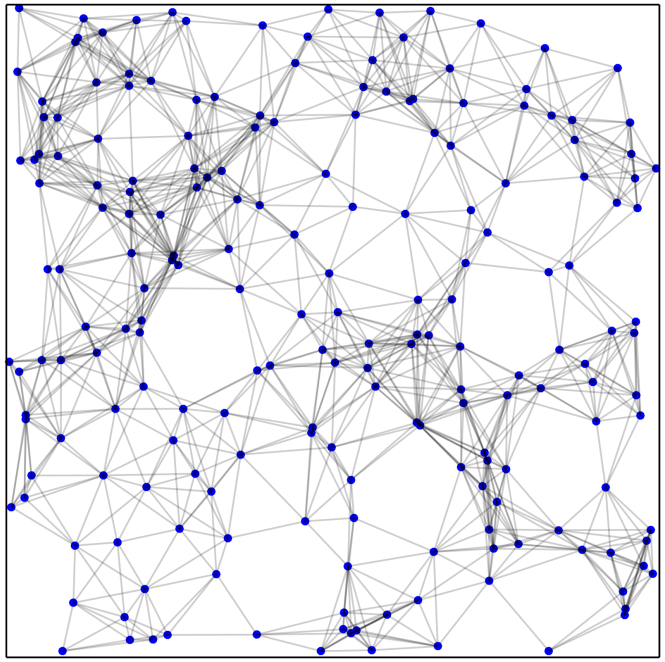
points are connected if distance does not exceed threshold

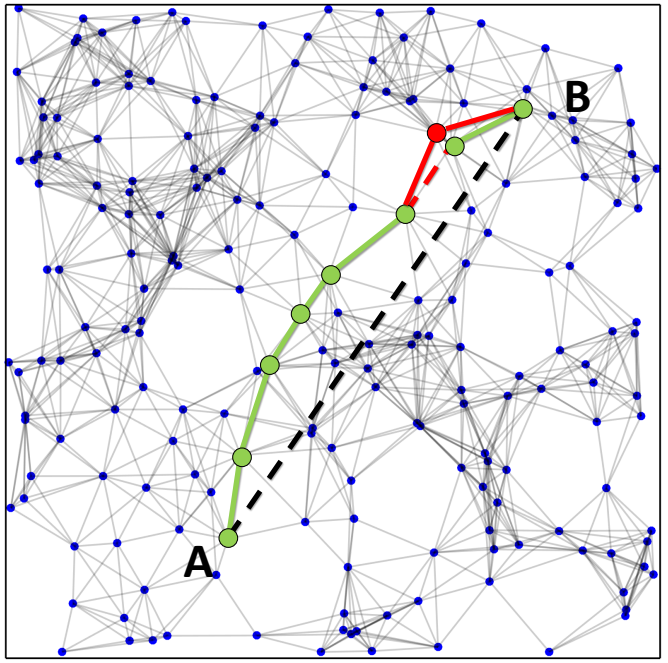


Shortest paths are not as hard in geometric networks

Random Geometric Graph:

points are connected if distance does not exceed threshold





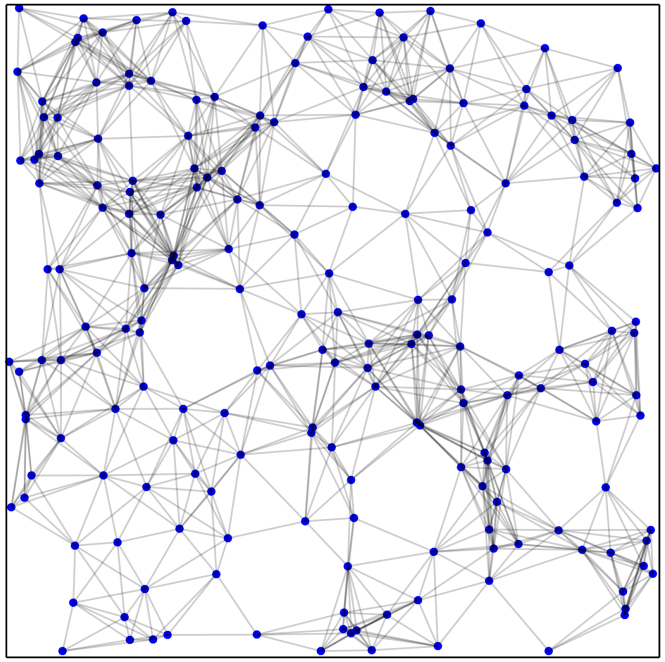
Shortest paths in RGGs are close to geodesic curves!

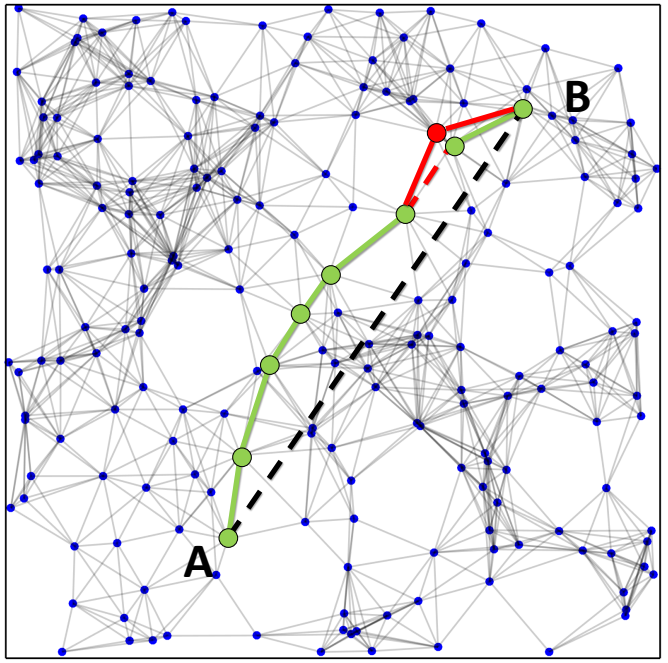
J. Dıaz (2016), A. P. Kartun-Giles (2019)

Shortest paths are not as hard in geometric networks

Random Geometric Graph:

points are connected if distance does not exceed threshold





Shortest paths in RGGs are close to geodesic curves!

J. Dıaz (2016), A. P. Kartun-Giles (2019)

Finding shortest path nodes in geometric networks:

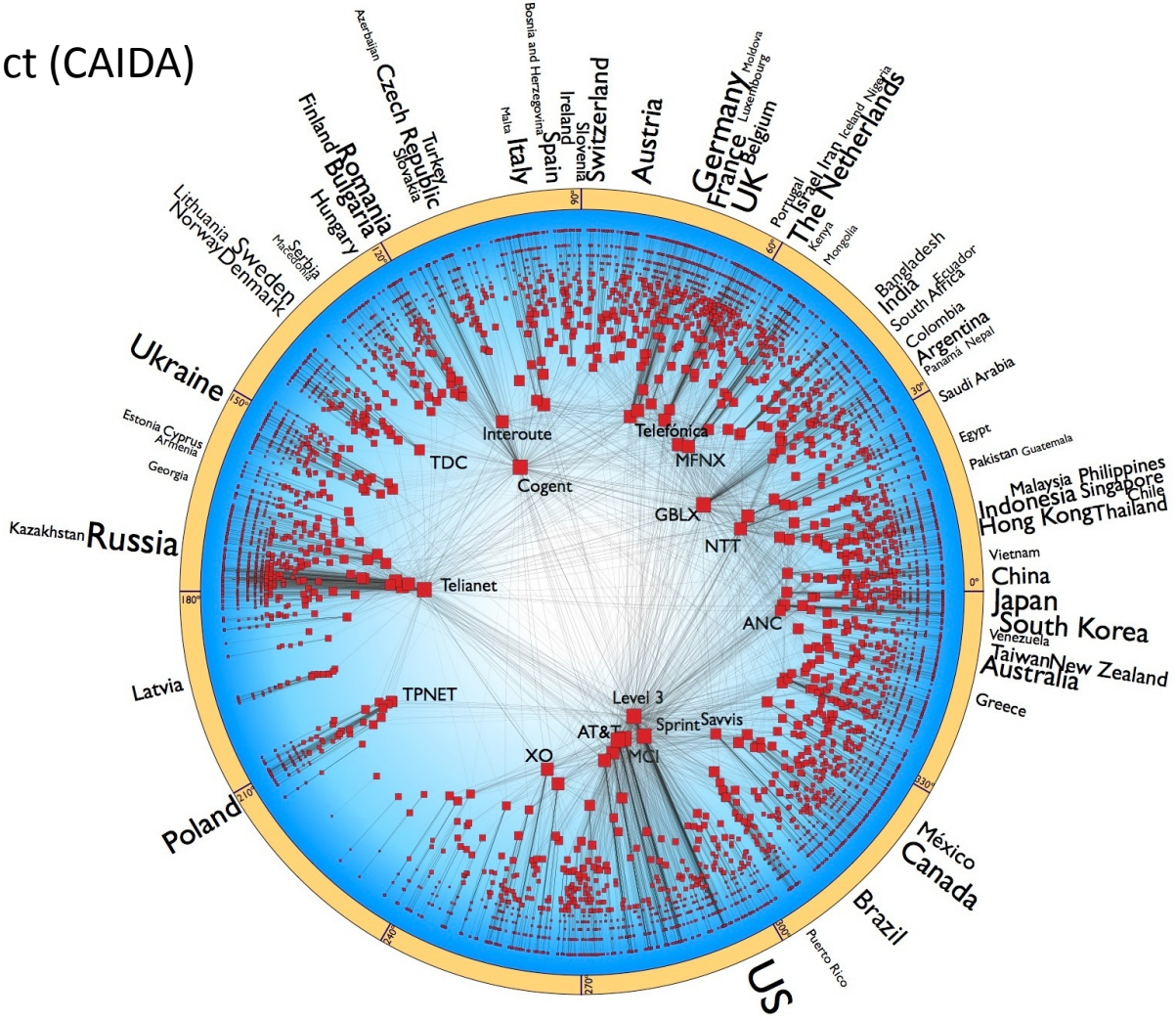
1) Find geodesic connecting shortest path endpoints

2) Rank nodes based on distance to geodesic:

The closer the node the higher is the chance it belongs to the shortest path.

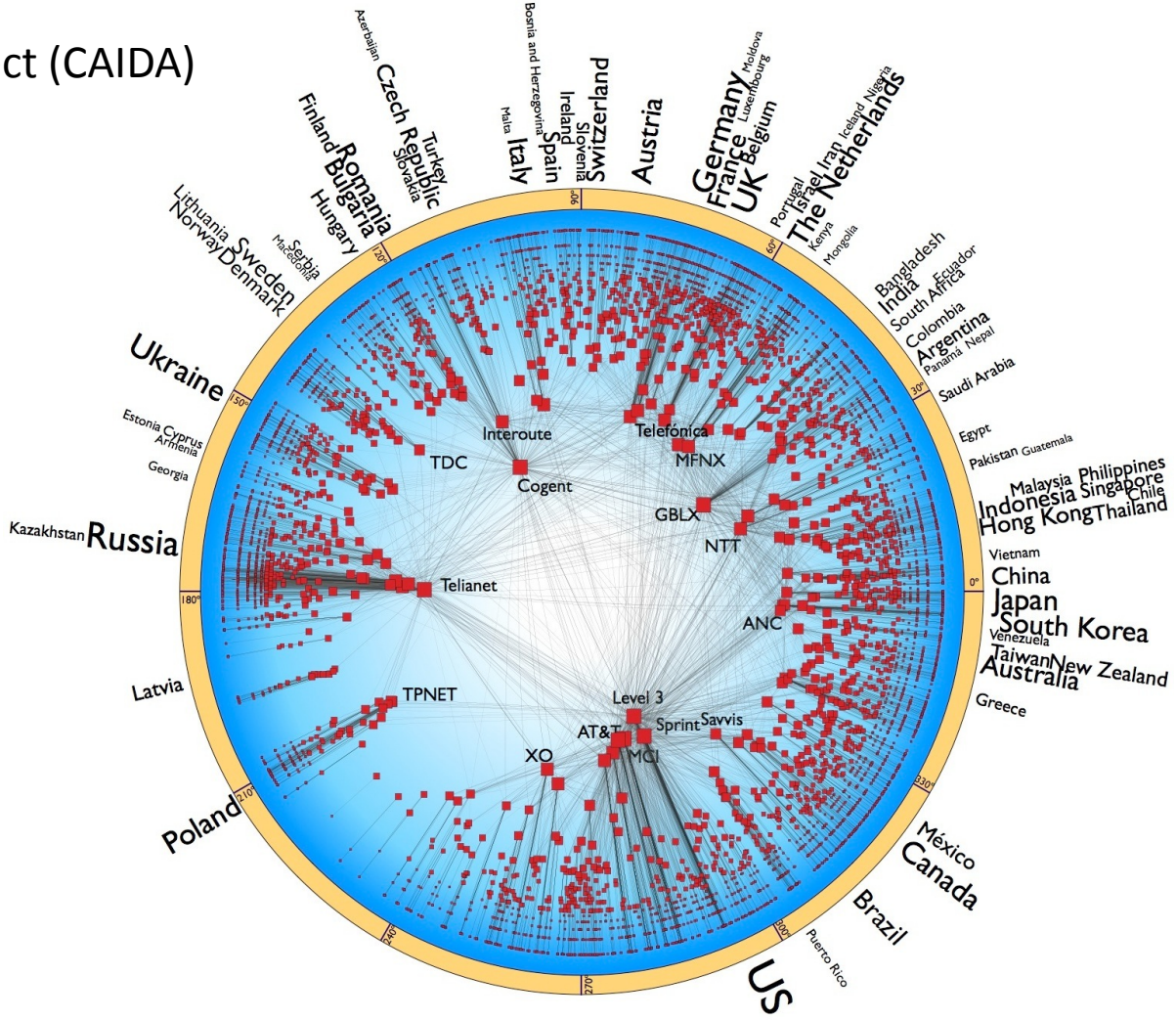
AS Internet is effectively hyperbolic

AS topology from
the Archipelago project (CAIDA)



AS Internet is effectively hyperbolic

AS topology from
the Archipelago project (CAIDA)

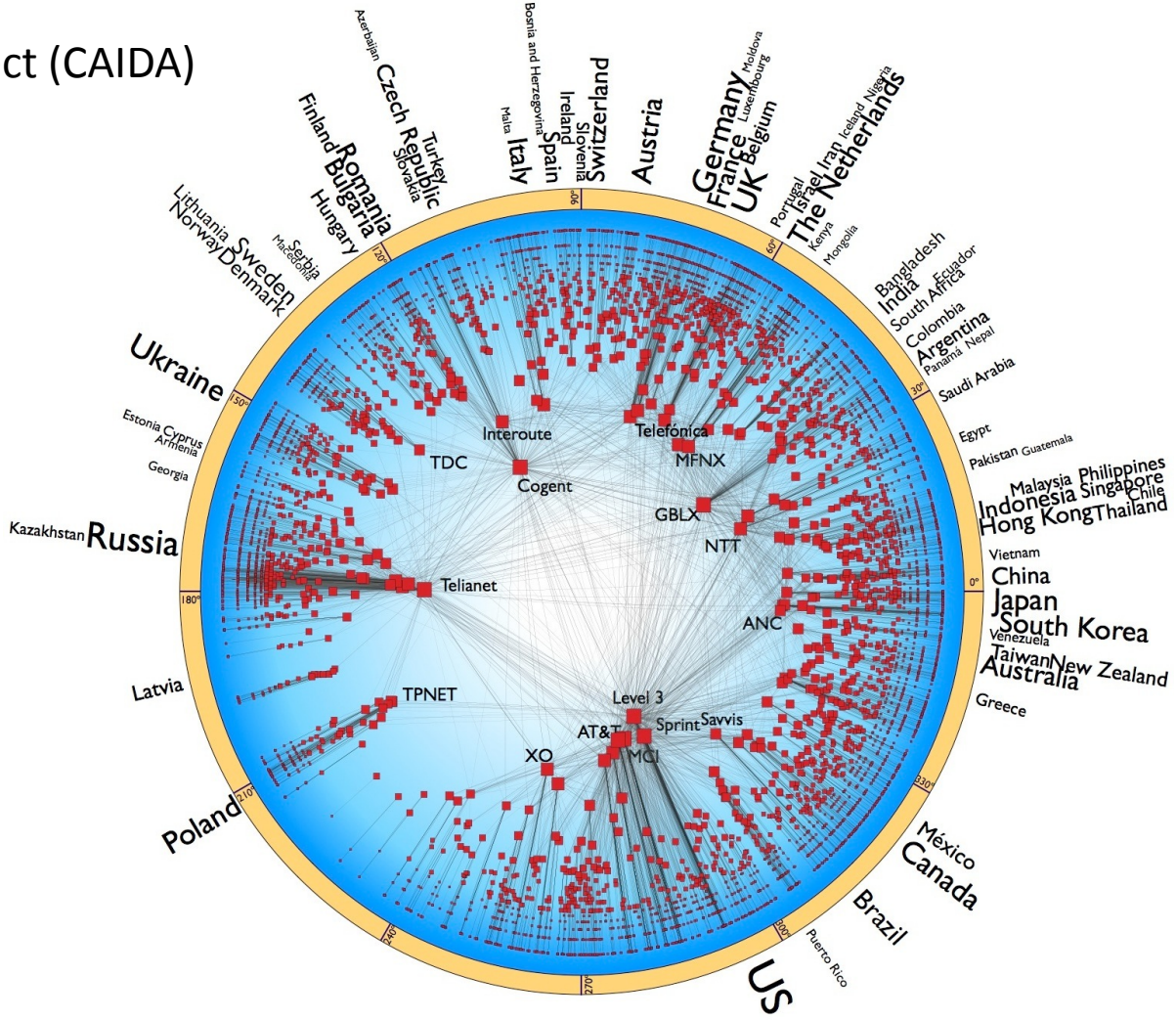


Map obtained using unsupervised ML methods by M. Boguñá, F. Papadopoulos, and D. Krioukov in 2010

Purpose: geometric greedy routing as an alternative to BGP

AS Internet is effectively hyperbolic

AS topology from
the Archipelago project (CAIDA)

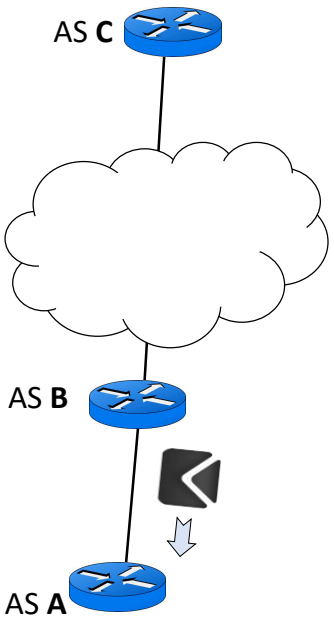


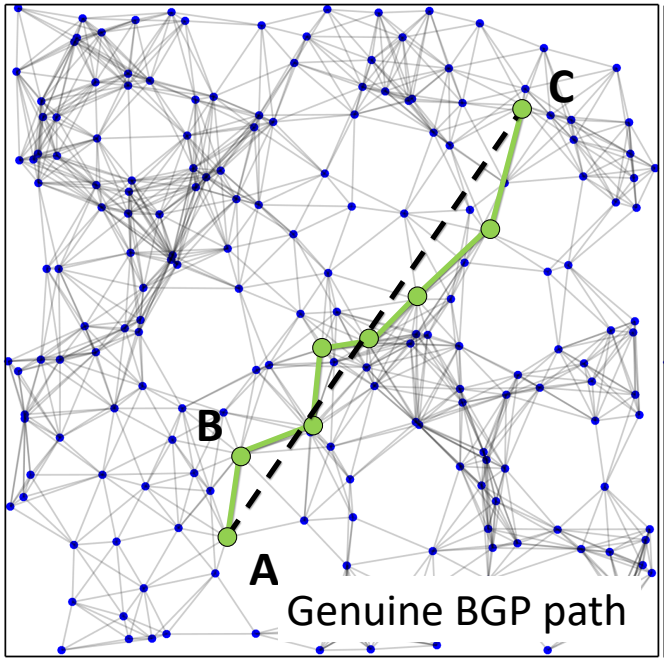
Map obtained using unsupervised ML methods by M. Boguñá, F. Papadopoulos, and D. Krioukov in 2010

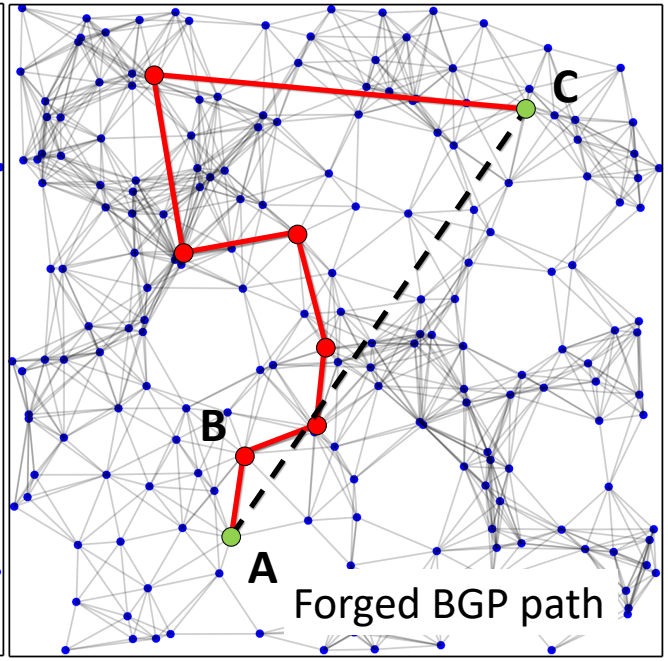
Purpose: geometric greedy routing as an alternative to BGP

The same (updated) map can be used to validate BGP paths.

Towards Geometric Path Validation





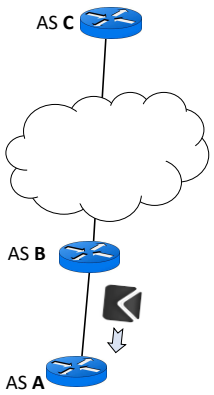


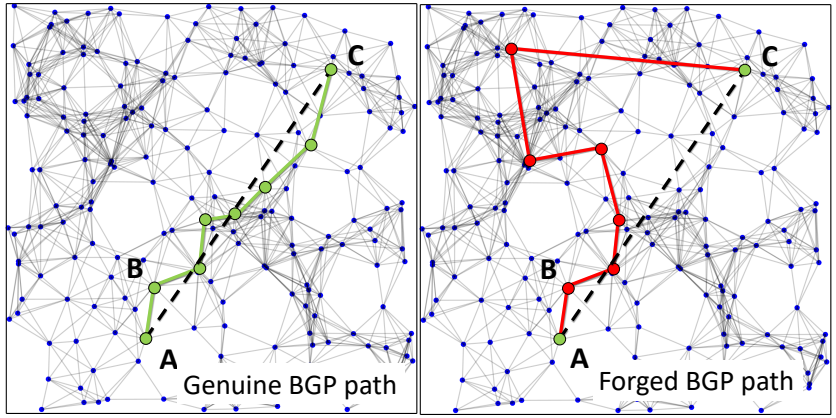
AS **A** can evaluate path geometric conformity and reject if needed.

Hyperbolic Internet mapping is highly robust to incomplete network data!

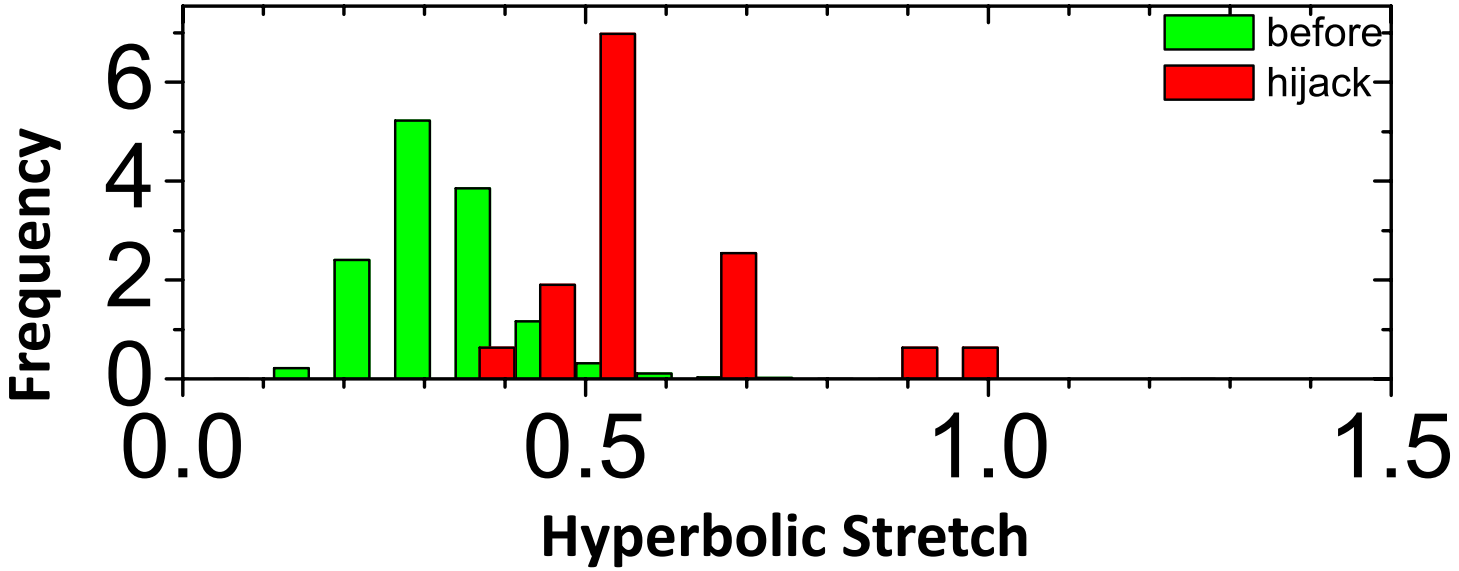
M. Kitsak et al, in preparation (2021)

Back to the Google hijack study



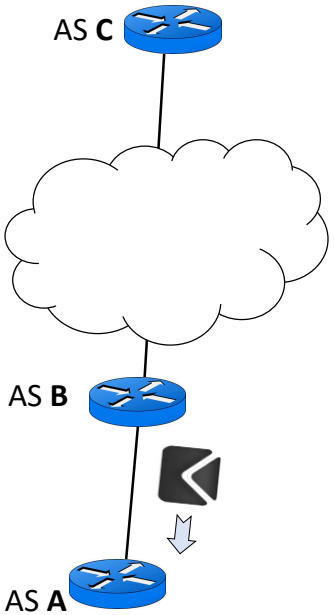


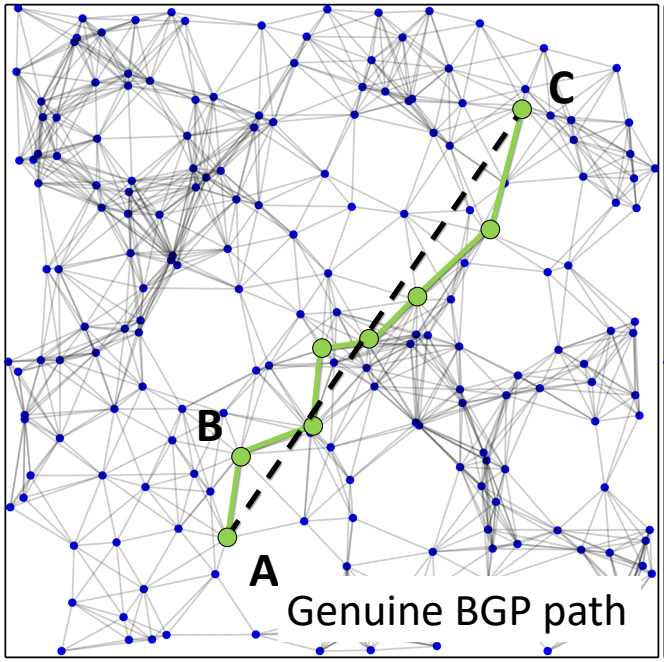
BGP paths before and during the hijack (by the BGPStream)

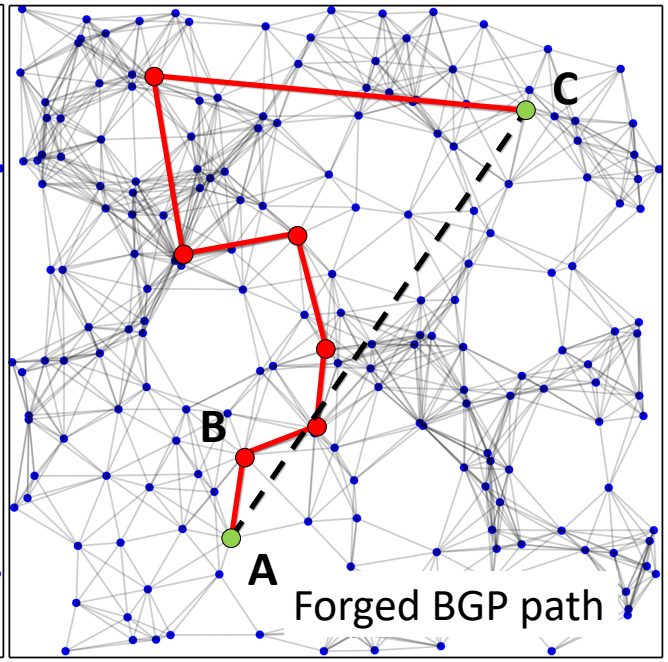


M. Kitsak et al, in preparation (2021)

Take home message







Machine Learning (Network Embedding) techniques may be used to design new and explainable methods to identify/forecast routing anomalies.

M. Kitsak et al, in preparation (2021)