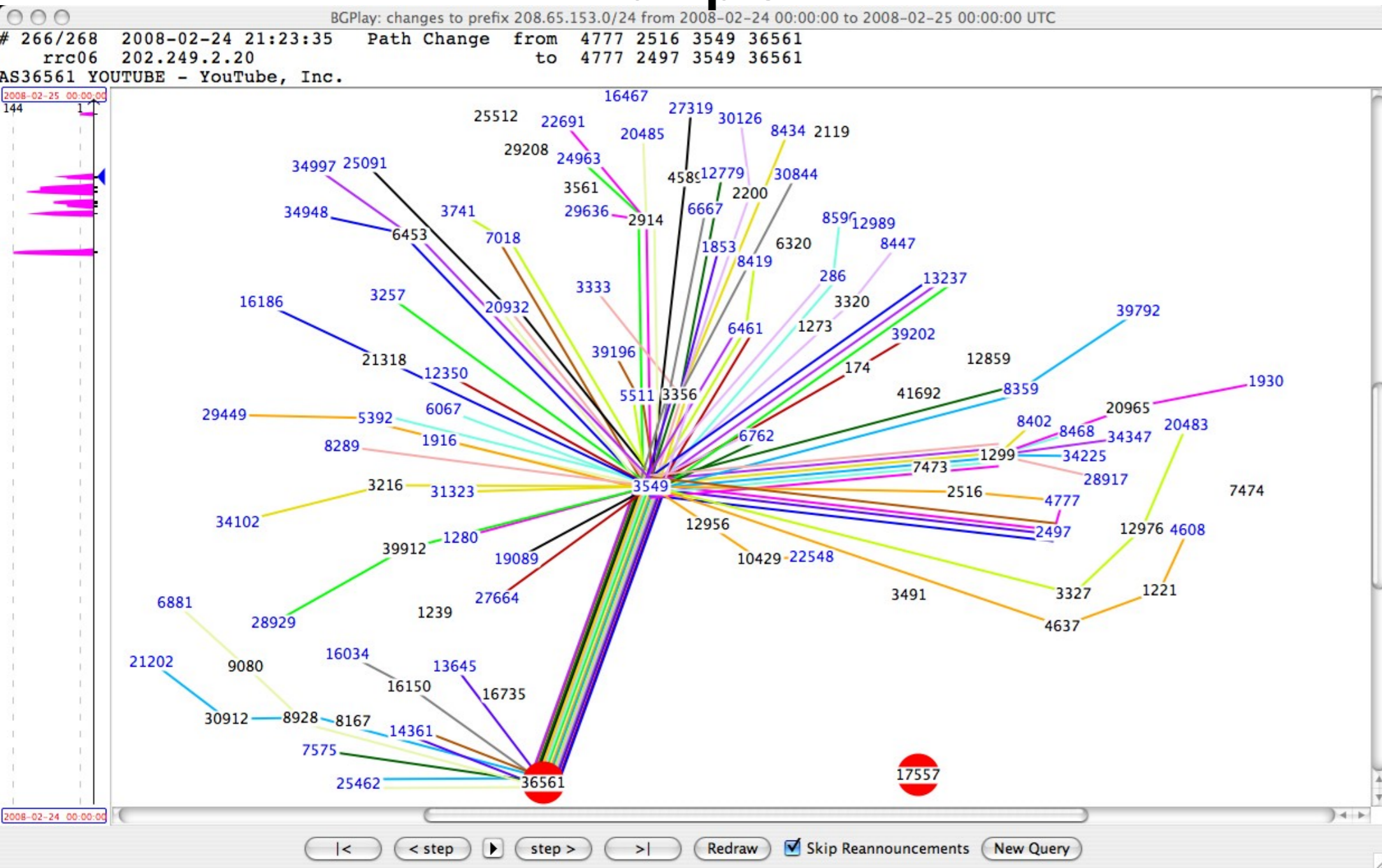


Stealthy IP Prefix Hijacking

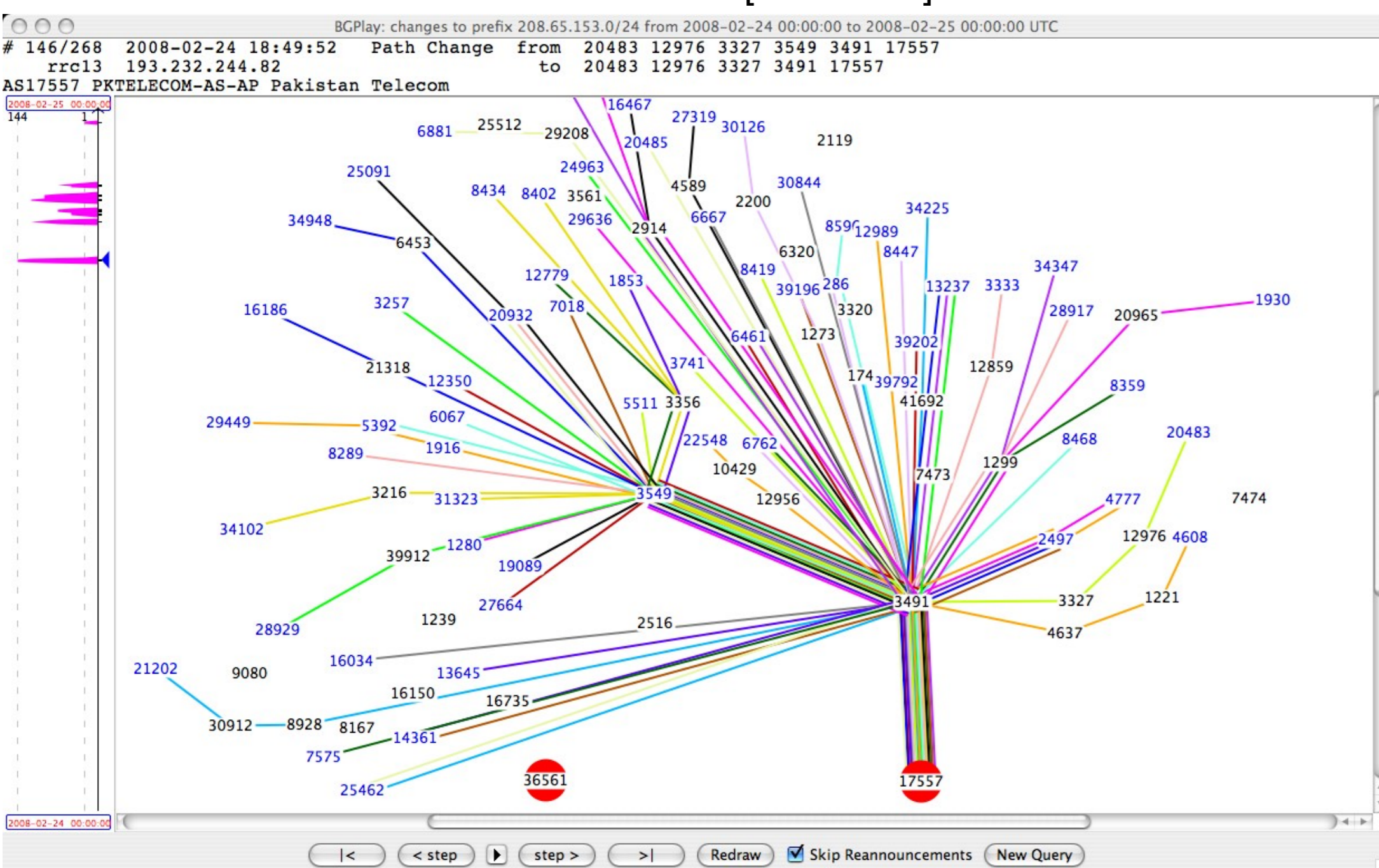
Christian McArthur & Mina S. Guirguis
Department of Computer Science, Texas State University-San Marcos

Prefix Hijacking: The YouTube / Pakistan Telecom Example



AS map under normal conditions [see above]. YouTube's prefix is routed via BGP to itself (AS 36561).

Pakistan Telecom begins announcing YouTube's prefix. The BGP announcement is inadvertently propagated to the Internet. Traffic destined for YouTube is sent to Pakistan Telecom [see below].



Source of AS Maps: <http://www.ripe.net/news/study-youtube-hijacking.html>

Even Worse!! Stealthy Prefix Hijacking

What if the attacker's goal is to impact a **smaller** number of ASes, so that

- (1) the attacker will not be overwhelmed by the amount of hijacked traffic,
- (2) the victim would not observe a sharp drop-off in its incoming traffic that would raise an alarm, and
- (3) the hijacking could be used to accomplish phishing, data recording or sniffing, or rerouting back to the victim.

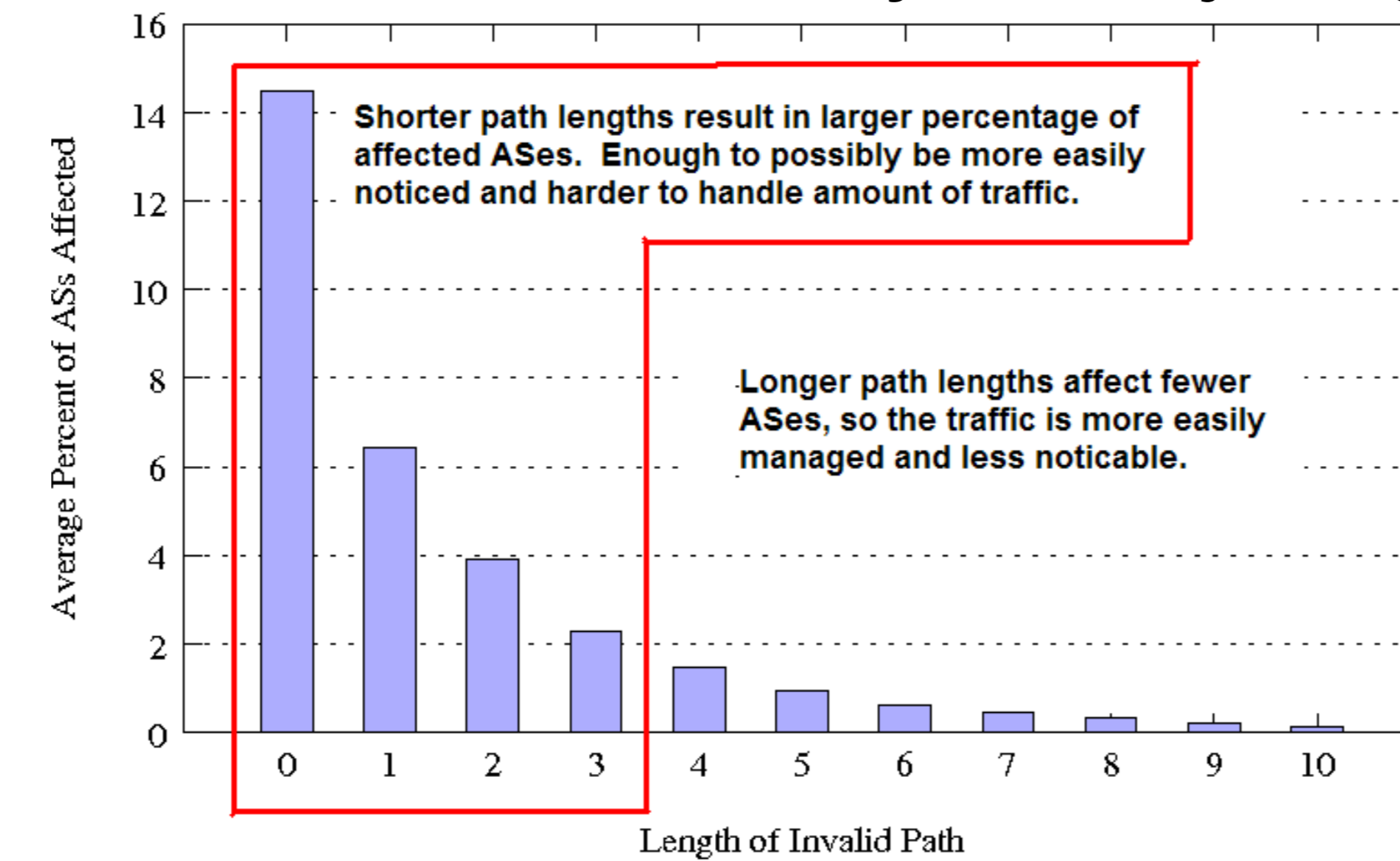
How to Perform a Stealthy Prefix Hijack

1. For a chosen victim, discover the AS tree where the victim is the root of the tree.
2. Determine which ASes in the tree you can peer with.
3. For each possible peer estimate the potential effects of the hijack with differing lengths of invalid paths.
4. Establish a peering relationship with the desired AS.
5. Temporarily announce an invalid BGP route, hijacking the victim's prefix, and analyze the amount of incoming traffic.
6. If the amount of traffic received is not desired (too much or too little), repeat step 5 with an invalid BGP route with a different length.
7. Once the amount traffic being received is desired, continue to announce the last route.

How to Determine the Effects of Prefix Hijacking

- BGP announcements from Routeviews accumulated.
- Data used to form AS trees for every prefix (250,000+).
- Each position in the tree was evaluated from a potential attacker's point of view.
- Determine the number of ASes affected by an attacker announcing BGP routes of various lengths.

Potential Effects of Stealthy Prefix Hijacking



Shorter path lengths result in larger percentage of affected ASes. Enough to possibly be more easily noticed and harder to handle amount of traffic.

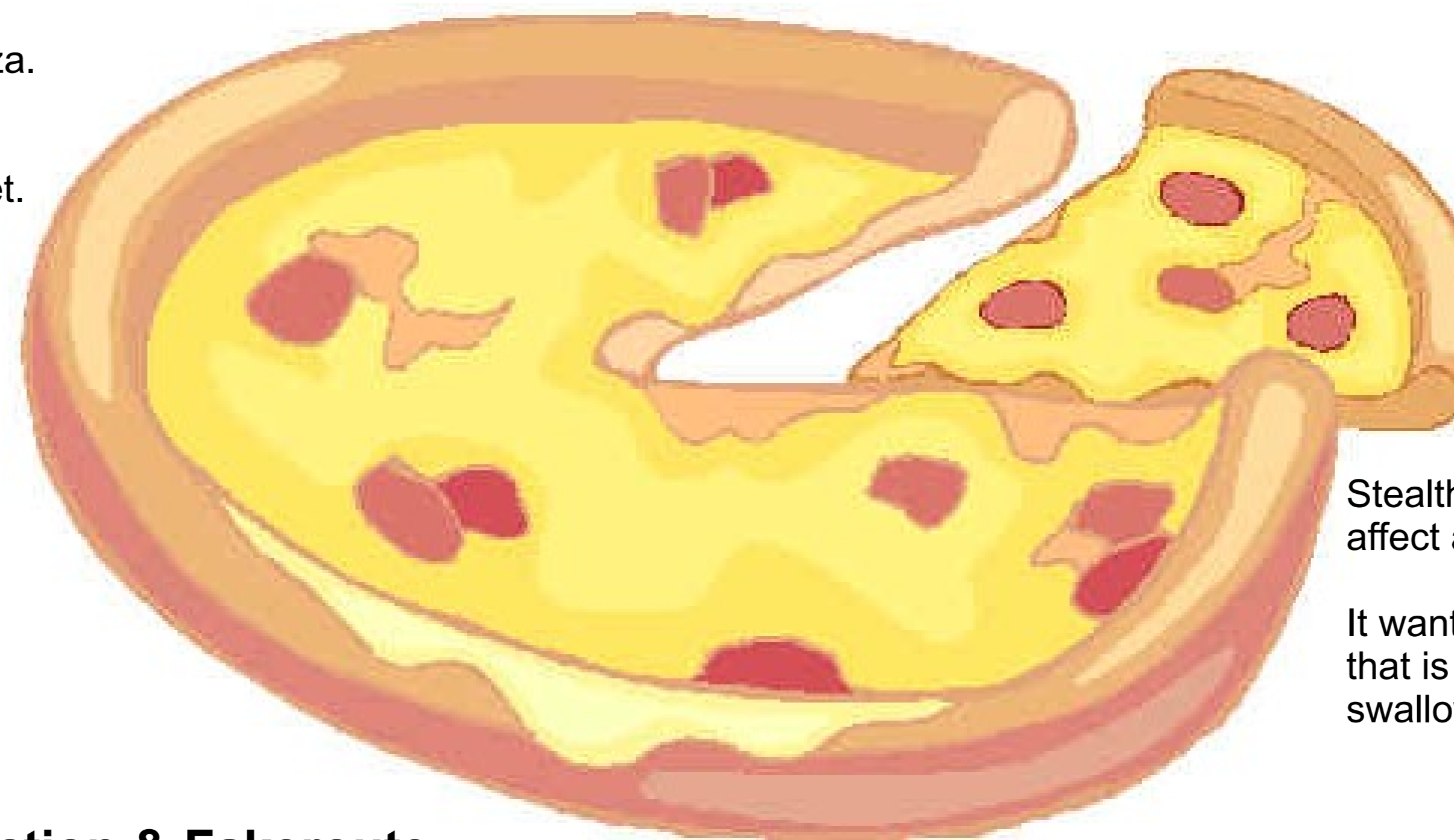
Longer path lengths affect fewer ASes, so the traffic is more easily managed and less noticable.

Don't Bite Off More Than You Can Chew

Think of the Internet as a big pizza.

Current prefix hijacking methods affects many ASes on the Internet.

These methods want the entire pizza for itself.

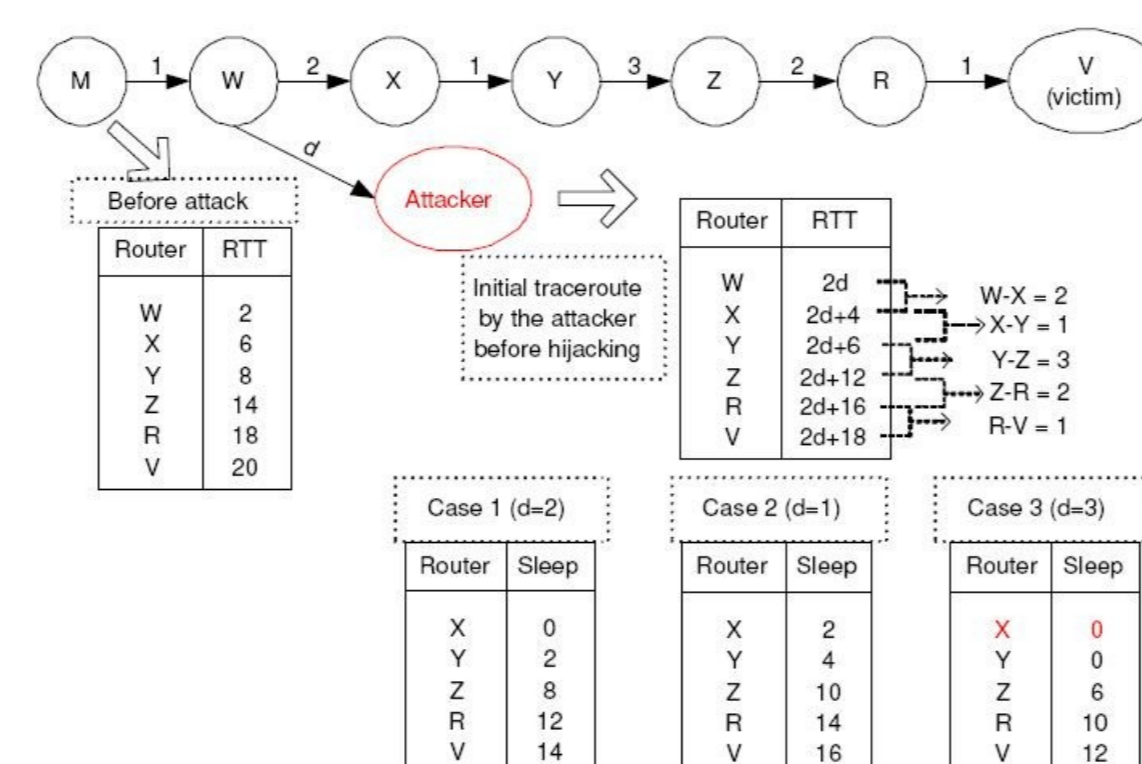


Stealthy prefix hijacking aims to affect a smaller number of ASes.

It wants a small slice of the pizza that is easier to manage and to swallow.

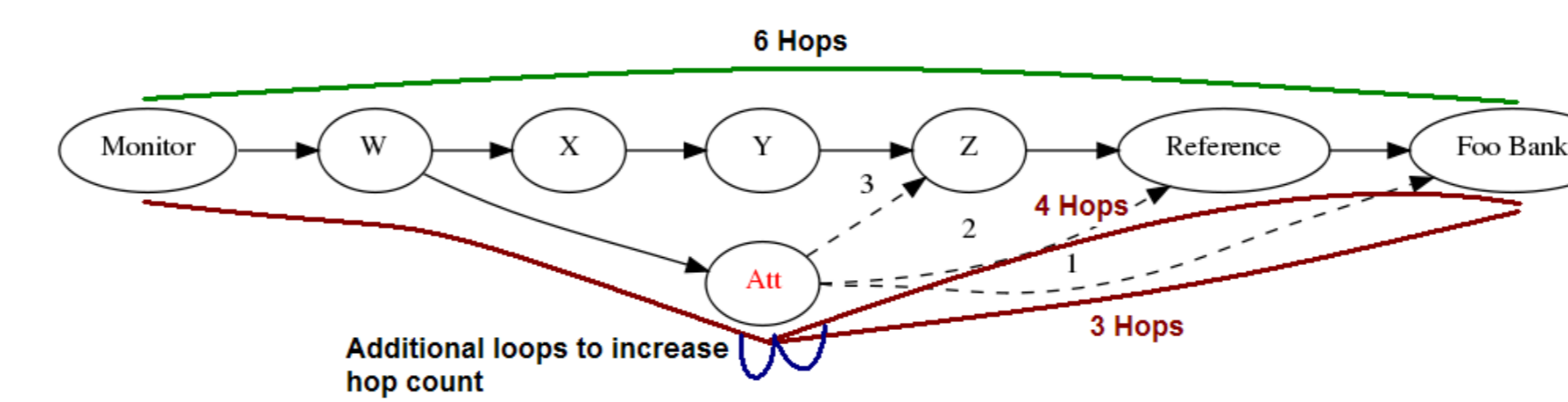
Defeating Detection & Fakeroute

- Current detection methods often rely on traceroute to detect hijacking attacks.
- We created "fakeroute" to intercept traceroute requests and falsify replies.
- Before the hijack, the attacker performs its own traceroute to discover:
 - IP Addresses and host names of routers to victim
 - Latencies and response times for each router.
- After the hijack, the attacker intercepts traceroute requests destined to the victim:
 - Forges replies with the relevant information for each router on the path to the victim.
 - Sends replies after a delay such that response times are accurate.



Change in Hop Count Detection

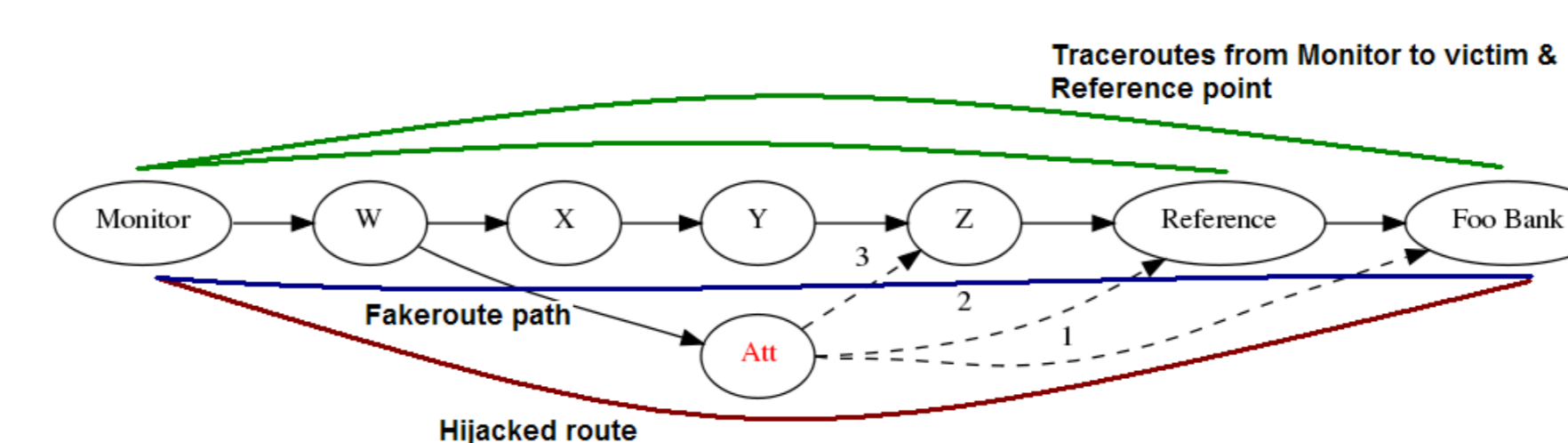
- Perform traceroute requests from monitor to victim.
- When a "significant" change in hop counts occur an alarm is raised.
- However, an attacker can use fakeroute to return a path back to the monitor causing no change in number of hops. [See figure below and "Falsifying Hop Count" in table at top right.]



Additional loops to increase hop count

Traceroute Path Disagreement

- Perform two traceroutes:
 - From Monitor to the possible victim.
 - From Monitor to a reference point.
 - Reference point should be close to the victim, but outside the victim's prefix.
- Compare the two routes. Significant differences between them raises an alarm.
- Using fakeroute, the attacker can return the original path. [See figure below and "Falsifying Entire Path" in table at top right.]



Hijacked route

Traceroute & BGP Paths Attack Scenario 2

	BGP Paths to the Victim (Foo Bank)
Before Attack	Monitor - W - X - Y - X - Z - Reference - Foo Bank
After Attack	Monitor - W - Attacker - Reference - Foo Bank

	Traceroute Paths to the Victim (Foo Bank)
Before Attack	Monitor - W - X - Y - X - Z - Reference - Foo Bank
After Attack	Monitor - W - Attacker - Reference - Foo Bank
Falsifying Hop Count	Monitor - W - Attacker - Attacker - Attacker - Reference - Foo Bank
Falsifying Entire Path	Monitor - W - X - Y - X - Z - Reference - Foo Bank

	Traceroute Paths to the Reference Point
Before Attack	Monitor - W - X - Y - X - Z - Reference
After Attack	Monitor - W - X - Y - X - Z - Reference

AS Traceroute

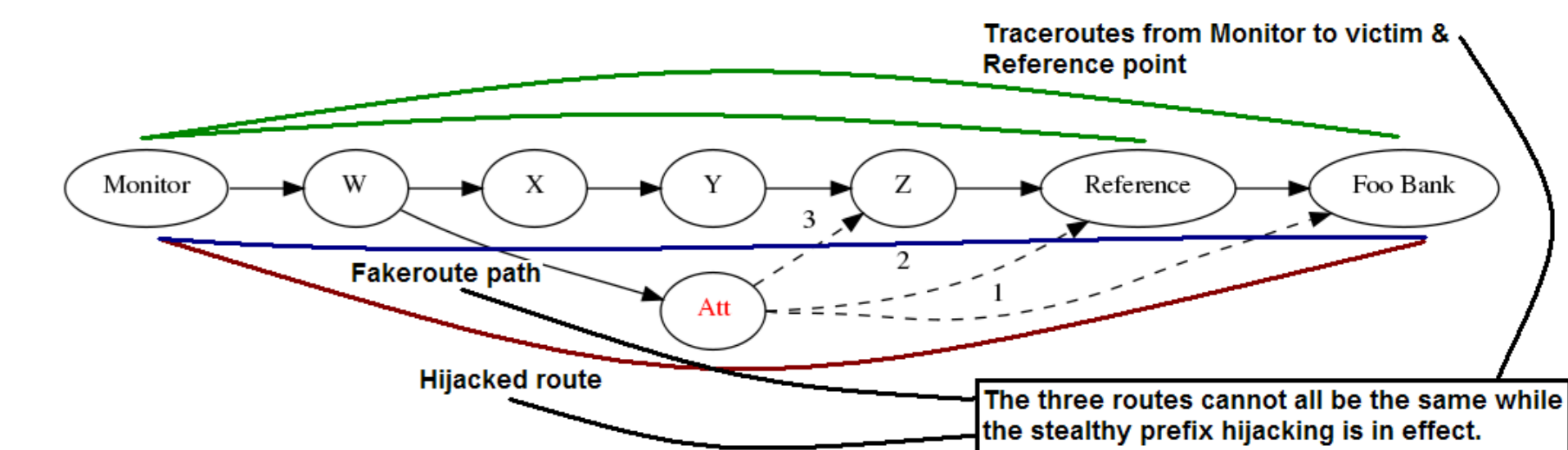
- IP addresses from traceroute requests are converted into AS numbers.
- This AS route is compared to the announced BGP route.
- Differences between the AS traceroute and the announced BGP route will trigger an alarm.

Current Detection Methods Ineffective

- Hop Count Change & Traceroute Disagreement detection methods easily defeated by use of fakeroute.
- AS Traceroute would not normally detect prefix hijacks as traceroutes would automatically match BGP routes.

Proposed Detection Method

- Combination of two existing methods:
 - Traceroute Disagreement
 - AS Traceroute
- Attacker can defeat traceroute disagreement, but trigger an alarm from AS Traceroute.
- Attacker can maintain the correct AS traceroute, but trigger an alarm from traceroute disagreement.
- Attack will be unable to defeat the combined detection method.



The three routes cannot all be the same while the stealthy prefix hijacking is in effect.

Conclusions

- With this project we:
- exposed a new class of prefix hijacking attacks that aims to impact a smaller number of ASes in order to evade detection.
 - exposed "fakeroute," a tool that falsifies traceroute replies to help evade detection.
 - proposed a method of detecting stealthy prefix hijackings.

Ongoing work

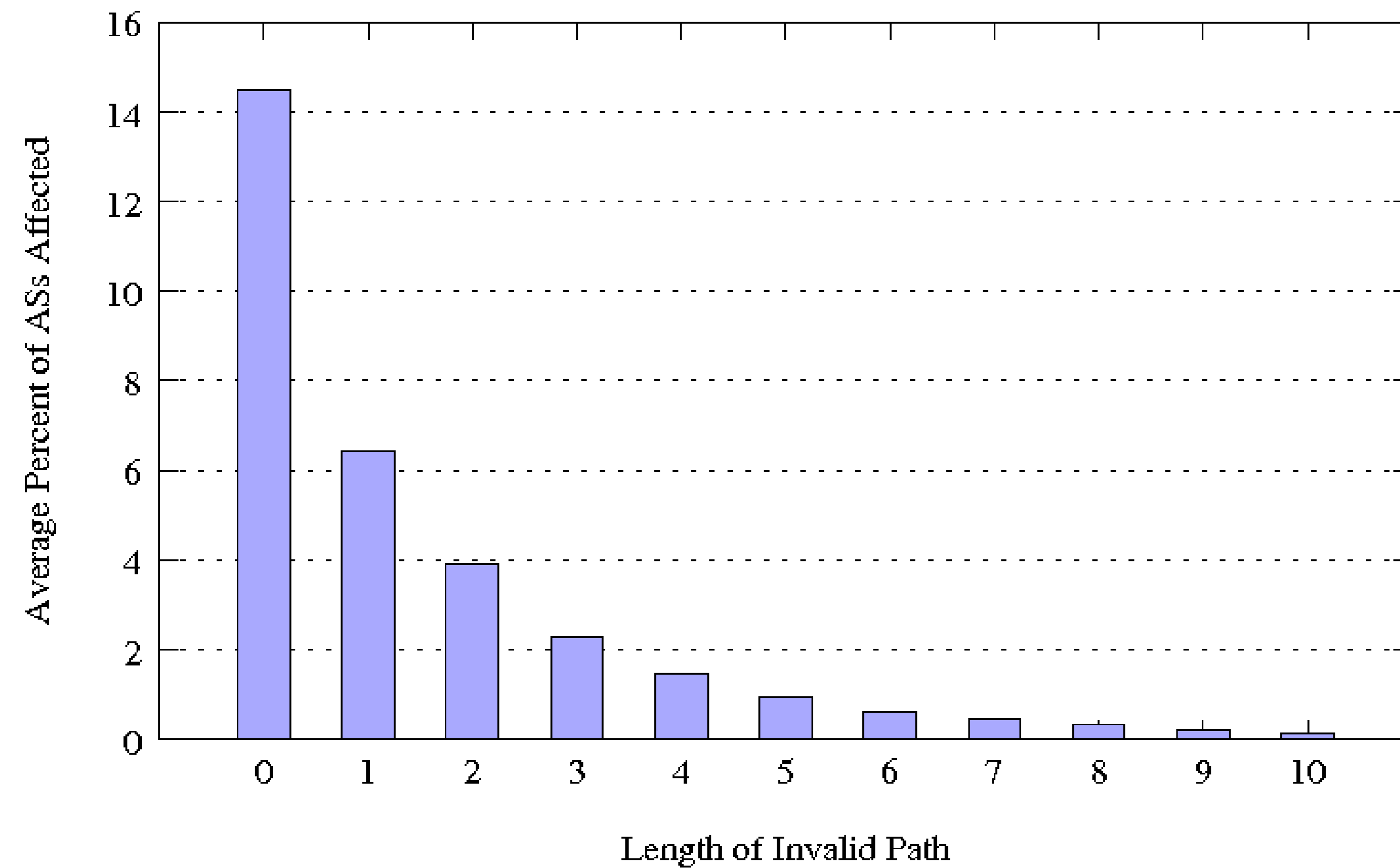
- Investigation of different classes of attacks to allow for more tuning of attack effects:
 - Multi-homed attacks
 - Attacks to target a source AS
- Determine amounts of traffic effected.

Stealthy IP Prefix Hijacking: Don't Bite Off More Than You Can Chew

What is a Stealthy Prefix Hijack? In prefix hijacking, an AS advertises invalid BGP routes for prefixes that are owned by another AS, so that the traffic intended for the real owner is hijacked and received by the attacker. Previous research confirmed that an attacker could potentially affect a large number of ASes on the Internet. But, what if the attacker's goal is not to maximize the number of affected ASes, but rather impact a smaller number of ASes, so that (1) the attacker can handle the amount of hijacked traffic (for phishing, recording, rerouting) and (2) the victim would not observe a sharp drop-off in its incoming traffic that would raise an alarm?

In order to perform a successful stealthy prefix hijacking, the BGP advertisements should have a small impact on the Internet. To do so, the attacker advertises an invalid route for the victim's prefix that has a longer path than what may be preferred by the majority of ASes. In particular, the exact length should be *long enough so that its effects will not be noticed by the victim's administrators, yet short enough to attract a fraction of the traffic intended for the victim.*

How Many ASes Can be Affected? To assess the impact of stealthy prefix hijacking attack, we utilized BGP advertisements provided by Route-Views. These views were combined to create a tree of AS paths for every prefix seen by the observer routers. We analyzed the effects of varying the lengths of the invalid advertisements on the number of ASes that would be tricked into believing those invalid advertisements. The figure below shows our results. As an attacker announces longer routes, fewer ASes are effected on average.



Methods of Detecting Prefix Hijackings

Changes in Hop Count:

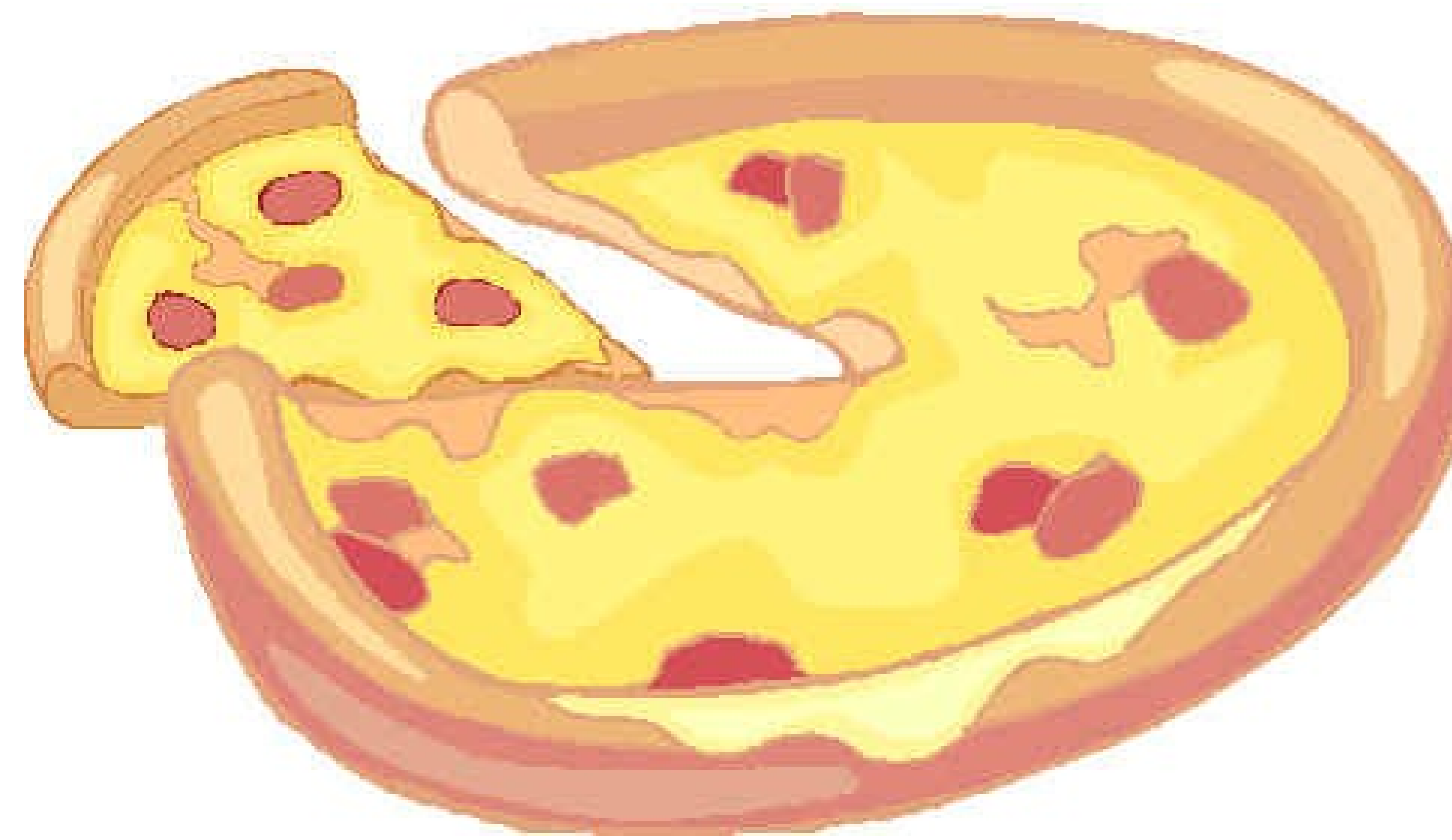
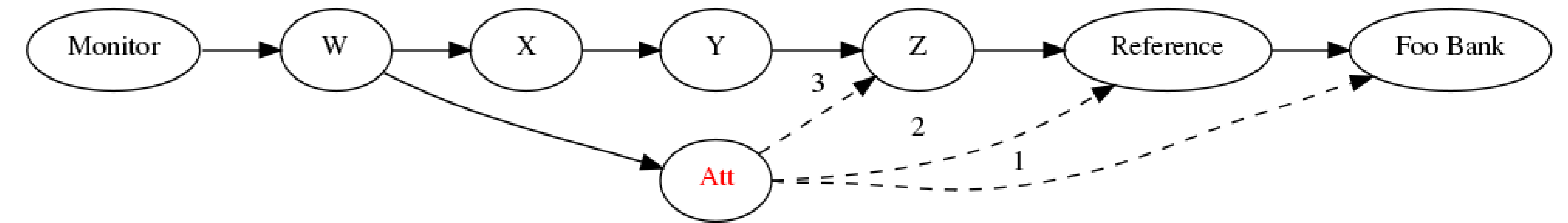
Whenever there is a significant change in the number of hops, an alarm is raised. Scenarios 1 and 2 in the top right figure will raise alarms. However, by using fakeroute, the number of hops will not differ during an attack as shown by "Falsifying Hop Count" in the table.

Traceroute Path Disagreement:

Another method relies on comparing a possible route from a monitor to the victim with another route to a reference point. The reference point is chosen to be as close as possible to the victim, yet outside the victim's prefix. During an attack, the traceroute from the monitor to the victim would take a different route than to the reference point. Once again, through the use of fakeroute, the entire path can be falsified. This is detailed in the table with "Falsifying Entire Path."

AS Traceroute:

AS Traceroute takes a traditional traceroute listing of routers and maps the routers' IP addresses into the corresponding AS numbers. To detect prefix hijacking, the AS traceroute path is compared to the BGP routing data for any discrepancies. In any of our hijacking scenarios the AS Traceroute path will match the BGP route. So this detection method alone does not raise any alarms.



Stealthy Prefix Hijack Algorithm:

1. For a chosen victim, discover the AS tree where the victim is the root of the tree.
2. Determine which ASes in the tree you can peer with.
3. For each possible peer estimate the potential effects of the hijack with differing lengths of invalid paths.
4. Establish a peering relationship with the desired AS.
5. Temporarily announce an invalid BGP route, hijacking the victim's prefix, and analyze the amount of incoming traffic.
6. If the amount of traffic received is not desired (too much or too little), repeat step 5 with an invalid BGP route with a different length.
7. Once the amount of traffic being received is desired, continue to announce the last route.

Fakeroute and Defeating Detection Methods:

Many detection methods rely on traceroute to detect hijacking attacks. To defeat those methods, we have created a tool, "fakeroute", that intercepts traceroute requests and falsifies its replies. Before the attacker hijacks a prefix, it does a traceroute and to the intended victim to learn about the ASes, routers and timing information along the legitimate path. Fakeroute uses this information to respond with the IP addresses (via spoofing the source Ips) and round-trip times (via adding the appropriate delay) of the legitimate routers, after the hijacking occurs. Responses from fakeroute could not be differentiated from legitimate responses.

Proposed Method of Detecting Stealthy Prefix Hijackings:

We believe that stealthy prefix hijackings can be detected by combining two detection methods: traceroute path disagreement and AS Traceroute. In order to avoid having discrepancies between the hijacked path and the BGP route, the attacker must provide a traceroute path in which the IPs of the routers translate into AS numbers that match the BGP route.

The path "Falsifying Hop Count" in the table illustrates as AS traceroute version matching the BGP announcement. However, if this route is compared to the route to the reference point there will be discrepancies suggesting a possible hijacking.

If the attacker uses fakeroute to respond with a path that would match the route to the reference point, the AS traceroute path would then disagree with the BGP announcement.

Therefore, by combining these two methods, path disagreement to a reference point and mapping the AS traceroute to the BGP route, stealthy prefix hijacking attacks are detected.

Traceroute & BGP Paths Attack Scenario 2

BGP Paths to the Victim (Foo Bank)

Before Attack Monitor – W – X – Y – X – Z – Reference – Foo Bank
After Attack Monitor – W – Attacker – Reference – Foo Bank

Traceroute Paths to the Victim (Foo Bank)

Before Attack Monitor – W – X – Y – X – Z – Reference – Foo Bank
After Attack Monitor – W – Attacker – Reference – Foo Bank
Falsifying Hop Count Monitor – W – Attacker – Attacker – Attacker – Reference – Foo Bank
Falsifying Entire Path Monitor – W – X – Y – X – Z – Reference – Foo Bank

Traceroute Paths to the Reference Point

Before Attack Monitor – W – X – Y – X – Z – Reference
After Attack Monitor – W – X – Y – X – Z – Reference