On the State of the Inter-domain and Intra-domain Routing Security

Mingwei Zhang

April 19, 2016
Internet Architecture

- The Internet consists of many *domains*, i.e., autonomous systems (ASes)
- Routing protocols are used to exchange reachability information about IP addresses and prefixes
The Internet consists of many *domains*, i.e., autonomous systems (ASes).

Routing protocols are used to exchange reachability information about IP addresses and prefixes.

**Inter-domain routing**: *IP prefixes*; among multiple ASes
The Internet consists of many domains, i.e., autonomous systems (ASes)

Routing protocols are used to exchange reachability information about IP addresses and prefixes

**Inter-domain routing**: IP prefixes; among multiple ASes

**Intra-domain routing**: IP addresses; within one AS
Internet Architecture

Intra-domain traffic

Inter-domain traffic
Inter-domain Routing

- **Inter**-domain routing: exchanges reachability information about IP prefixes among ASes
- **Border Gateway Protocol (BGP)** is the *de facto* inter-domain routing protocol.
Inter-domain routing: exchanges reachability information about IP prefixes among ASes

Border Gateway Protocol (BGP) is the de facto inter-domain routing protocol.

ASes have two main BGP operations:

- Originate prefixes: “if you want to reach prefix A, please forward the traffic to me”
- Propagate routes toward prefixes: “you can reach prefix A through me”
Inter-domain routing: exchanges reachability information about IP prefixes among ASes

Border Gateway Protocol (BGP) is the de facto inter-domain routing protocol.

ASes have two main BGP operations:
- Originate prefixes: “if you want to reach prefix A, please forward the traffic to me”
- Propagate routes toward prefixes: “you can reach prefix A through me”

Vulnerable to attacks:
- Prefix hijacking
- AS path spoofing
Intra-domain routing: decide forwarding paths for traffic within one AS.

**Software-defined networking (SDN)** is the new paradigm for intra-domain routing that provides the following benefits:

- Programmable switches
- Centralized control at the controller node
- Unified communication interface: **OpenFlow**
Intra-domain routing: decide forwarding paths for traffic within one AS.

Software-defined networking (SDN) is the new paradigm for intra-domain routing that provides the following benefits:
- Programmable switches
- Centralized control at the controller node
- Unified communication interface: OpenFlow

SDN suffers from security problems:
- Flooding attacks on the controllers
- Control message forgeries
- Application conflicts
Routing Security Solutions

- We investigate the security solutions for both BGP and SDN
- BGP security:
  - Attack prevention
  - Attack detection
- SDN security:
  - Attack prevention
  - Attack detection
  - Security using SDN
Taxonomy of Security Mechanisms

- Attack prevention solutions:
  - Proactively stop routing attacks
  - Find loopholes and prevent attacks
  - Upgrade the protocol design or operations
Taxonomy of Security Mechanisms

- **Attack prevention solutions:**
  - Proactively stop routing attacks
  - Find loopholes and prevent attacks
  - Upgrade the protocol design or operations

- **Attack detection solutions:**
  - Reactively detect routing attacks
  - Mostly through anomaly detection approaches
  - Usually do not require changes of the protocol or infrastructure
  - Especially needed when prevention mechanisms cannot be deployed
Taxonomy of Security Mechanisms

- **Internet Routing Security**
  - Inter-domain Routing: BGP
    - Attack Prevention
    - Attack Detection
  - Intra-domain Routing: SDN
    - Attack Prevention
    - Attack Detection
Section

1. Internet Routing Security
   - Background
   - Internet Routing Security

2. Inter-domain Routing Security
   - Attacks on BGP
   - BGP Attack Prevention
   - BGP Attack Detection

3. Intra-domain Routing Security
   - Security Solutions of SDN
   - Security Solutions Using SDN

4. Conclusion
Attacks on BGP

- BGP mainly exchanges the information about:
  - IP prefix ownership: unit of reachability
  - AS path: routes toward any IP prefixes

- BGP lacks sufficient verification for the update messages
BGP mainly exchanges the information about:

- **IP prefix ownership**: unit of reachability
- **AS path**: routes toward any IP prefixes

BGP lacks sufficient verification for the update messages

**Attacks on BGP**:  
- *Prefix hijacking*: falsely announce ownership  
- *AS-path spoofing*: forge or modify routes
BGP Attack – Prefix Hijacking

"I own prefix B"
BGP Attack – AS Path Spoofing

AS5, AS4 < AS2, AS3, AS4

"My next hop is AS4"
Outline

Inter-domain Routing Security
- Attacks on BGP
- BGP Attack Prevention
- BGP Attack Detection
BGP Attack Prevention

BGP Attack Prevention

Control-plane Solutions

Cryptography-based

(8)

Data-plane Solutions

Non-cryptography-based

(2)

(3)
### BGP Attack Prevention

<table>
<thead>
<tr>
<th>Method</th>
<th>Control-plane</th>
<th>Crypto-based</th>
<th>Overhead</th>
<th>Data Source</th>
<th>Path</th>
<th>Origin</th>
<th>Deployment</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGPSec [8], [9], [10]</td>
<td>✓</td>
<td>✓</td>
<td>high</td>
<td>PKI</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>psBGP [12]</td>
<td>✓</td>
<td>✓</td>
<td>high</td>
<td>peer</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>SPV [13]</td>
<td>✓</td>
<td>✓</td>
<td>low</td>
<td>registry</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Listen &amp; Whisper [14]</td>
<td>✓</td>
<td>✓</td>
<td>medium</td>
<td>peer</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>RAVS [15]</td>
<td>✓</td>
<td>✓</td>
<td>low</td>
<td>peer</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>IRR</td>
<td>✓</td>
<td>✓</td>
<td>low</td>
<td>registry</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>IRV [16]</td>
<td>✓</td>
<td>✓</td>
<td>medium</td>
<td>peer</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>GTSM [17]</td>
<td></td>
<td></td>
<td>low</td>
<td>N/A</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TCP MD5 Sig. [18]</td>
<td></td>
<td></td>
<td>low</td>
<td>N/A</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IPSEC [19]</td>
<td></td>
<td></td>
<td>medium</td>
<td>N/A</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Non-cryptography-based Attack Prevention from the Control Plane

- **Internet Routing Registry (IRR)**
  - Centralized routing information registry
  - BGP updates can be verified using IRR databases
  - Incomplete and inaccurate information
    - ASes lack motivation to submit their routing information
    - They also do not update IRR data frequently
Non-cryptography-based Attack Prevention from the Control Plane

- **Internet Routing Registry (IRR)**
  - Centralized routing information registry
  - BGP updates can be verified using IRR databases
  - Incomplete and inaccurate information
    - ASes lack motivation to submit their routing information
    - They also do not update IRR data frequently

- **Internet Route Validation (IRV)**
  - Query IRV servers of the ASes on an AS path
  - ASes will respond whether they have seen/propagated the routes
  - Problems:
    - Unclear how to find the IRV servers
    - Not effective during partial deployment
    - Attackers can also forge IRV messages
Cryptography-based Attack Prevention from the Control Plane

- Depend heavily on cryptographic operations to secure the content of the BGP updates
- Focus on securing the prefix origin and AS paths information
- Two main solutions are being deployed: RPKI and BGPsec
- Other previous solutions: soBGP, psBGP, SPV
Cryptography-based Prevention – RPKI

- RPKI helps prevent prefix hijacking
  - RPKI provides cryptographically verifiable certificates that show the origin ASes of every registered prefix
  - Contains credentials for every registered AS, such as public key
Cryptography-based Prevention – RPKI

- RPKI helps prevent prefix hijacking
  - RPKI provides cryptographically verifiable certificates that show the origin ASes of every registered prefix
  - Contains credentials for every registered AS, such as public key

**Diagram:**
- RPKI
- AS2
- Who can originate prefix B?
- AS 4
Cryptography-based Prevention – BGPsec

- **BGPsec** also protects AS paths
  - Utilizes the RPKI to validate prefix ownership announcement
  - Requires every AS to sign all updates when propagating them
Cryptography-based Prevention – BGPsec

- **BGPsec** also protects AS paths
  - Utilizes the RPKI to validate prefix ownership announcement
  - Requires every AS to sign all updates when propagating them
**BGPsec** also protects AS paths

- Utilizes the RPKI to validate prefix ownership announcement
- Requires every AS to sign all updates when propagating them
Attack Prevention from the Data Plane

- Data-plane solutions secure the communication between BGP routers
Attack Prevention from the Data Plane

- Data-plane solutions secure the communication between BGP routers
- **TCP MD5 Signature**: only verifies integrity
Attack Prevention from the Data Plane

- Data-plane solutions secure the communication between BGP routers
- **TCP MD5 Signature**: only verifies integrity
- **IPSEC**: encrypts entire communication
Attack Prevention from the Data Plane

- Data-plane solutions secure the communication between BGP routers
- **TCP MD5 Signature**: only verifies integrity
- **IPSEC**: encrypts entire communication
- **Generalized TTL Security Mechanism (GTSM)**: restricts hop distance
Outline

2 Inter-domain Routing Security
- Attacks on BGP
- BGP Attack Prevention
- BGP Attack Detection
BGP Attack Detection

- BGP attack prevention solutions are slowly being deployed, while the attacks happen with increasing frequency
- Need quick BGP attack detection and reaction
- Categorize by data sources:
  - Control-plane solutions
  - Data-plane solutions
- Categorize by methodologies:
  - Active monitoring solutions
  - Passive monitoring solutions
### BGP Attack Detection Taxonomy

<table>
<thead>
<tr>
<th>method</th>
<th>control-plane</th>
<th>data-plane</th>
<th>anomaly verification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>active</td>
<td>passive</td>
<td>active</td>
</tr>
<tr>
<td>NeighborWatch [26]</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>TERRAIN [37]</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>subMOAS [22]</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Kruegel et al. 2003 [38]</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Buddyguard [39]</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>I-Seismograph [40]</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Geo-location [41]</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Argus [42], [43]</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Wavelet [44], [45]</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>BGP-lens [46]</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>BGPeEye [47]</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Concurrency-based [48]</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Machine-learning-based [49]</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PHAS [50]</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PGBGP [51]</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>rcc [52]</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Topology-based [53]</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TAMM [54]</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Listen and Whisper [14]</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Host-signature based [55]</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Hop-distance based [56]</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>iSPY [57]</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Crowd-based [58]</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LDC [59]</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PurgePromote [60]</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**TABLE II: Taxonomy of the attack detection methods**
Passive Monitoring from the Control Plane

- Passively listen to the control-plane messages
- Prefix hijacking detection:
  - Prefix-origin relationship: PHAS, PGBGP
  - Prefix-prefix relationship: Buddyguard
Prefix Hijackings Detection: Prefix-Origin Relationship

- During training phase: build prefix-origin mapping
- During monitoring phase:
  - **PHAS**: alert inconsistent BGP updates
  - **PGBGP**: quarantines inconsistent BGP updates

**Training**

Prefix 1  \[\leftrightarrow\] AS A

**Monitoring**

Prefix 1  \[\leftrightarrow\] AS B
Prefix Hijackings Detection: Prefix-Origin Relationship

- During training phase: build prefix-origin mapping
- During monitoring phase:
  - **PHAS**: alert inconsistent BGP updates
  - **PGBGP**: quarantines inconsistent BGP updates
- Problems:
  - Cleanness of the training data cannot be guaranteed

![Diagram showing training and monitoring phases with no alert](image.png)
Prefix Hijackings Detection: Prefix-Origin Relationship

- During training phase: build prefix-origin mapping
- During monitoring phase:
  - **PHAS**: alert inconsistent BGP updates
  - **PGBGP**: quarantines inconsistent BGP updates
- Problems:
  - Cleanness of the training data cannot be guaranteed
  - Unable to capture the “quiet” prefixes

### Diagram

**Training**

Prefix 1

**Monitoring**

Prefix 1 → AS B

No alert!
Prefix Hijackings Detection: Prefix-Origin Relationship

- During training phase: build prefix-origin mapping
- During monitoring phase:
  - PHAS: alert inconsistent BGP updates
  - PGBGP: quarantines inconsistent BGP updates
- Problems:
  - Cleanness of the training data cannot be guaranteed
  - Unable to capture the “quiet” prefixes
  - Unable to update model for the legitimate changes

![Diagram showing prefix hijacking](image)

**Training**

Prefix 1 ↔ AS A

**Monitoring**

Prefix 1 ↔ AS B

*False alert!*
- **Buddyguard** discovers the “fate-sharing” prefixes as buddies for the monitored prefix.
- Suspicious behavior: path change of target prefix but not its buddies.
- It is **resilient** against attackers’ countermeasures:
  - Hard to obtain the list of buddies.
  - Hard to hijack all buddies.
Active Monitoring from the Control Plane

<table>
<thead>
<tr>
<th>Control-plane</th>
<th>Passive</th>
<th>Active</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data-plane</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Active monitoring solutions: queries to third-party registries for routing information
- Combine data from various sources to construct knowledge base
- Information: routing information: e.g., from IRR
- Geographical information
Active Monitoring from the Control Plane

- Active monitoring solutions:
  - queries to third-party registries for routing information
  - combine data from various sources to construct knowledge base
Active Monitoring from the Control Plane

<table>
<thead>
<tr>
<th></th>
<th>Passive</th>
<th>Active</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control-plane</td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>Data-plane</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Active monitoring solutions:**
  - queries to third-party registries for routing information
  - combine data from various sources to construct knowledge base

- **Information:**
  - routing information: e.g., from IRR
  - geographical information
1. Probe Routing Information for Anomaly Detection

- Siganos et al. proposed **Neighborhood Watch** that utilizes information from IRR to detect anomalies
- Actively probes IRR for information related to suspicious BGP updates
- Detect inconsistencies between IRR and BGP updates
- Problems:
  - IRR has out-of-date information
- Sriram et al. proposed to validate routing information from IRR before usage to improve accuracy
2. Combine Routing Information with Other Sources

- Kruegel et al. designed a system that incorporates topological and geographical information
  - constructs clusters of ASes based on their geographical distances between each other
  - categorizes the ASes into edge and inner ASes
  - only edge AS can connect to ASes from other cluster
Other approaches utilize data-plane information
Other approaches utilize data-plane information.
They focus on detecting the impacts from prefix hijackings:

- Traffic changes
- Reachability changes
- End-host information changes
1. Detecting Traffic Changes

- Liu et al. proposed to detect changes of the traffic load distribution (LDC)
  - LDC shows how the traffic to a prefix is distributed among all the ASes
  - Suspicious changes can be detected comparing with the normal clusters
1. Detecting Traffic Changes

- **Liu et al.** proposed to detect changes of the **traffic load distribution (LDC)**
  - LDC shows how the traffic to a prefix is distributed among all the ASes
  - Suspicious changes can be detected comparing with the normal clusters

- **Hiran et al.** proposed to measure **round-trip time (RTT)** to detect prefix hijackings
  - The system passively collects RTT to the monitored prefix from many vantage points
  - It detects suspicious increases of RTT as an indication of prefix hijacking
2. Detecting Reachability Changes

- **iSPY, Argus, and Listen** detect prefix hijackings by monitoring the reachability of the target prefixes.
2. Detecting Reachability Changes

- iSpy, Argus, and Listen detect prefix hijackings by monitoring the reachability of the target prefixes.
2. Detecting Reachability Changes

- **iSPY**, **Argus**, and **Listen** detect prefix hijackings by monitoring the reachability of the target prefixes.
2. Detecting Reachability Changes

- **iSPY**, **Argus**, and **Listen** detect prefix hijackings by monitoring the reachability of the target prefixes.
3. Detecting Changes of End-hosts Information

- Hu et al. designed a fingerprinting system that creates profiles for the machines in a network.
- When a prefix hijacking happens, the profiles of the machines in that prefix will not match anymore.
- Similarly, Schlamp et al. propose to build profiles for only the HTTPS servers in the network.

![Suspicious change!](image-url)
Section

1. Internet Routing Security
   - Background
   - Internet Routing Security

2. Inter-domain Routing Security
   - Attacks on BGP
   - BGP Attack Prevention
   - BGP Attack Detection

3. Intra-domain Routing Security
   - Security Solutions of SDN
   - Security Solutions Using SDN

4. Conclusion
Intra-domain Routing

- Traditional intra-domain routing
  - Protocols include RIP, OSPF, IS-IS, EIGRP, etc.
  - Use vendor specific management software
  - Equipment lacks extensibility
  - Lack of unified management mechanism
Intra-domain Routing

- **Traditional intra-domain routing**
  - Protocols include RIP, OSPF, IS-IS, EIGRP, etc.
  - Use vendor specific management software
  - Equipment lacks extensibility
  - Lack of unified management mechanism

- **Software-Defined Networking (SDN)**
  - Centralized control over all switches
  - Unified communication protocol: **OpenFlow**
  - Switches are programmable to conduct different tasks on demand
Software-Defined Networking

SDN Applications

SDN Controller

SDN Switches

End-hosts
Software-Defined Networking

- SDN Applications
- SDN Controller
- SDN Switches
- End-hosts
3 Intra-domain Routing Security

- Security Solutions of SDN
- Security Solutions Using SDN
Securing SDN against Malicious Controllers

- **Fleet** defends against malicious controllers.
- Any new rules require acknowledgment from other controllers (Shamir’s scheme).
**Fleet** defends against malicious controllers

Any new rules require acknowledgment from other controllers (Shamir’s scheme)
Securing SDN against Malicious Controllers

- **Fleet** defends against malicious controllers
- Any new rules requires acknowledgment from other controllers (Shamir’s scheme)
- Problems:
  - many controller software only support one controller per network
  - all controllers share the same set of configuration and policies, making it less cost-effective
Securing SDN against Malicious Applications

- Malicious (or conflicting) SDN applications are the main concern in this field.
- Solutions take different approaches to secure SDN against malicious applications:
  - **Modeling checking**: NICE, ConfigChecker, Flowchecker
  - **Rule conflict detection**: FortNOX, FlowGuard, VeriFlow, NetPlumber
  - **Network isolation**: FlowVisor
1. Model Checking Solutions

- **NICE**, **FlowChecker** and **ConfigChecker** use *model checking* technique to explore all possible states of an OpenFlow application.

- Combined with *symbolic execution*, they are able to locate erroneous states without executing programs on the switch.
2. Rule Conflict Detection

- **FortNOX** detect conflicts from rules generated by different applications
- **FlowGuard, NetPlumber, and Veriflow** detect rules that violate security policies

![Diagram showing rule conflicts and policy violations]
3. Network Isolation

- **FlowVisor** divides one physical network into multiple *slices* of virtual networks
- Each *slice* has its own controller and topology
- FlowVisor can be used to isolate erroneous applications, and often be used to enable multiple controllers on one physical network
3. Network Isolation

- **FlowVisor** divides one physical network into multiple *slices* of virtual networks
- Each *slice* has its own controller and topology
- FlowVisor can be used to isolate erroneous applications, and often be used to enable multiple controllers on one physical network
- **Problems:**
  - FlowVisor relies on other software to resolve issues from malicious applications
Chi et al. focused on detecting compromised switches.

The system carefully crafts rules and packets to detect these misbehaviors.
Securing SDN against Malicious End-hosts

- The end-hosts in an SDN network can also present various threats
The end-hosts in an SDN network can also present various threats:

- Control message flooding attack

**Securing SDN against Malicious End-hosts**

- Flood of OpenFlow messages
- Unique flows that can generate OpenFlow messages
Defending OpenFlow Message Flooding Attack

- **AVANT-GUARD** defends specifically the flooding caused by TCP SYN flood

Only complete TCP flows can pass
Defending OpenFlow Message Flooding Attack

- **AVANT-GUARD** defends specifically the flooding caused by TCP SYN flood

Only complete TCP flows can pass
Defending OpenFlow Message Flooding Attack

- **AVANT-GUARD** defends specifically the flooding caused by TCP SYN flood

Only complete TCP flows can pass
Defending OpenFlow Message Flooding Attack

- **AVANT-GUARD** defends specifically the flooding caused by TCP SYN flood

Only complete TCP flows can pass
Defending OpenFlow Message Flooding Attack

- **AVANT-GUARD** defends specifically the flooding caused by TCP SYN flood
- **FloodGuard** defends against the flooding traffic by slowing down the traffic to the controller
Outline

3 Intra-domain Routing Security
- Security Solutions of SDN
- Security Solutions Using SDN
SDN Can Help Secure Networks

- SDN’s centralized management benefits these tasks
  - Monitor traffic over the entire network
  - Perform actions on matched flows, such as dropping or rate-limiting
SDN Can Help Secure Networks

- SDN’s centralized management benefits these tasks
  - Monitor traffic over the entire network
  - Perform actions on matched flows, such as dropping or rate-limiting
- Researchers have investigated the potential applications of SDN in the following areas:
  - Traffic anomaly detection
  - Distributed denial-of-service attack defense
Traffic Anomaly Detection

- Mehdi et al. ported existing anomaly detection systems into SDN environment and evaluated their performance.
- They showed that SDN can work well with traditional algorithms in terms of traffic anomaly detection.
Mehdi et al. ported existing anomaly detection systems into SDN environment and evaluated their performance. They showed that SDN can work well with traditional algorithms in terms of traffic anomaly detection. Shin et al. proposed FRESCO, a programming framework for network security. The authors demonstrated a anomaly detection function with less than one hundred lines of code needed in FRESCO framework.
DDoS Defense

- Distributed denial-of-service (DDoS) attack has been plaguing the Internet for years
- SDN’s flexible control of the network equipment enables a set of new approaches toward defending DDoS attack
  - Traffic filtering solution: **Remote Blackhole**
  - Network maneuvering solutions: **Virtual IP, Random Host Mutation**
Section

1. Internet Routing Security
   - Background
   - Internet Routing Security

2. Inter-domain Routing Security
   - Attacks on BGP
   - BGP Attack Prevention
   - BGP Attack Detection

3. Intra-domain Routing Security
   - Security Solutions of SDN
   - Security Solutions Using SDN

4. Conclusion
Internet routing suffers and will still suffer from various attacks
Internet Routing is Not Secure

- Internet routing suffers and will still suffer from various attacks
- Inter-domain routing
  - Prefix hijacking and AS path spoofing attacks happen more and more frequently
  - Prevention solutions are not deployed widely
  - Detection solutions cannot mitigate the attack
Internet Routing is Not Secure

- Internet routing suffers and will still suffer from various attacks
- Inter-domain routing
  - Prefix hijacking and AS path spoofing attacks happen more and more frequently
  - Prevention solutions are not deployed widely
  - Detection solutions cannot mitigate the attack
- Intra-domain routing
  - SDN attracts great attention from industry and academia
  - However, security still weighs less than usability
What is still missing?

- BGP security
  - Prevention solutions that are effective in partial deployment
  - Motivation study for the deployment of prevention solutions
  - Effective detection + mitigation system
  - Mechanisms that can discourage misbehaviors
What is still missing?

- BGP security
  - Prevention solutions that are effective in partial deployment
  - Motivation study for the deployment of prevention solutions
  - Effective **detection + mitigation** system
  - Mechanisms that can discourage misbehaviors

- SDN security
  - Studies on the controller security
  - Evaluation framework to study various solutions
  - Applications of SDN on other network security topics
Future Research Directions

- Securing the end-to-end communication requires both inter-domain and intra-domain routing security
Future Research Directions

- Securing the end-to-end communication requires both inter-domain and intra-domain routing security
- BGP attack detection system with effective mitigation
Future Research Directions

- Securing the end-to-end communication requires both inter-domain and intra-domain routing security
- BGP attack detection system with effective mitigation
- SDN security and its application on defending against other security problems
Thank you!

Q & A