A Deep Learning Approach for IP Hijack Detection Based on ASN Embedding

TEL AVIV UNIVERSITY אוניברסיטת תל אביב

School of Electrical Engineering

TAL SHAPIRA & YUVAL SHAVITT

Intro - Autonomous Systems

- **Autonomous System (AS):** a collection of physical networks glued together using IP, have a unified administrative routing policy, and has been assigned a number (ASN - 32 bits).
  - ISP Internal networks: Verizon – 701, 702, 703 …, Leve3: 3356, 3549 …
  - Campus networks: University of Delaware – 2, MIT - 3
  - Corporate networks: Intel - 4983
  - Content provider: Google - 15169, 16591 …, Facebook - 32934, 63293 …
- **Border Gateway Protocol (BGP)** coordinates the Inter-AS routing in the Internet
  - BGP routing's update messages list the entire AS path to reach an IP address prefix (AP)
  - Policy-Based routing protocol

Intro – IP Hijack

- Prefix hijacking in a nutshell - another AS originates the prefix
- More than 40% of the network operators reported that their organization had been a victim of a hijack in the past
- What's to stop someone else?
  - BGP does not verify that the AS is authorized
  - Registries of prefix ownership are inaccurate
- How to?
  - Sub-prefix hijack (e.g. 1.1.1.1/24 instead of 1.1.1.1/22)
  - Path shortening (BGP may choose path based on cost and length)
  - Add a legitimate AS at the end of the path (and therefore it's hard to tell that the AS path is bogus)

Example – April 2010, China Telecom

This prefix and 50K others were announced by China Telecom

Traffic for some prefixes was possibly intercepted

Previous Approaches

- Prevention solutions (or reactive solutions):
  - Based on cryptographic authentications – RPKI[1] and BGPsec[2]
  - Operators are reluctant to deploy them due to technical and financial costs
- Detection solutions - based on the type of information:
  - Control-plane approaches[3] (passive solutions) – based on a distributed set of BGP monitors and route collectors
  - Data-plane approaches[4] - only relies on real-time data plane information that is obtained from multiple sensors that deploy active probing (pings/traceroutes)
  - Hybrid approaches[5]
- Most of the previous detection solutions rely on:
  - Features engineering + ML algorithm[6]
  - Heuristic assumptions (e.g. VF)

1. **[*Geoff Huston and Randy Bush 2011*]** *"Securing BGP and SIDR" (RPKI)*
2. **[Matt Lepinski and K Sriram 2017]** *"BGPSEC protocol specification"*
3. **[Sermpezis et al. 2018]** *"ARTEMIS: Neutralizing BGP Hijacking within a Minute"*
4. **[Zhang et al. 2008]** *"Ispy: detecting IP prefix hijacking on my own"*
5. **[Schlamp et al. 2016]** *"HEAP: reliable assessment of BGP hijacking attacks"*
6. **[Fontugne et al. 2019]** *"BGP hijacking classification"*

'Valley Free' Routing

- Routing rules:
  - Provider accepts everything
  - Peer only if it is for its customers
- Path Properties:
  - Up then down
  - No up-down-up
  - At most 1 P2P step (and only at the top)

[**Gao 2001**] *"On inferring autonomous system relationships in the Internet"*

Motivation

- Using an **assumption-free** method for **IP hijack Detection**
- Our method is based **only on** BGP announcements (or AS-level routes)
- We introduce the first end-to-end **deep learning** approach
- Our goal is to use **a generic approach** based on ASN embedding
  - We aim to learn the dense representations of ASNs from BGP routes
  - Apply machine/deep learning techniques based on the representations

Method

- An end-to-end deep learning approach:
  - First stage – **BGP2Vec** – ASN Embedding
  - Second stage –
    - IP hijack detection using **LSTM networks**

72.246.151.0/24	196.7.106.245	0	0	0 2905 6939 8551 8551 8551 8551 8551 8551 i
72.246.151.0/24	80.91.255.137	0	0	0 1299 6453 8551 i
72.246.151.0/24	85.114.0.217	0	0	0 8492 8551 i
72.246.151.0/24	91.228.151.1	0	0	0 31019 8551 ?
72.246.151.0/24	202.93.8.242	0	0	0 24441 1299 1299 1299 6453 8551 i
72.246.151.0/24	87.121.64.4	0	0	0 57463 8551 i
72.246.151.0/24	94.156.252.18	0	0	0 34224 8551 i
72.246.151.0/24	105.16.0.247	0	0	0 37100 8551 i
72.246.151.0/24	212.66.96.126	0	0	0 20912 6939 8551 8551 8551 8551 8551 8551 i
72.246.151.0/24	206.24.210.80	0	0	0 3561 209 6453 8551 i
72.246.151.0/24	198.58.198.255	0	0	0 1403 6939 8551 8551 8551 8551 8551 8551 i
72.246.151.0/24	198.58.198.254	0	0	0 1403 6939 8551 8551 8551 8551 8551 8551 i
72.246.151.0/24	154.11.12.212	0	0	0 852 6939 8551 8551 8551 8551 8551 8551 i
72.246.151.0/24	12.0.1.63	0	0	0 7018 6453 8551 i
72.246.151.0/24	147.28.7.1	0	0	0 3130 1239 6453 8551 i
72.246.151.0/24	137.39.3.55	0	0	0 701 3257 8551 i
72.246.151.0/24	216.221.157.162	0	0	0 40191 6939 8551 8551 8551 8551 8551 8551 i
72.246.151.0/24	202.73.40.45	0	0	0 18106 8551 i
72.246.151.0/24	198.129.33.85	1	0	0 293 6453 8551 i
72.246.151.0/24	140.192.8.16	0	0	0 54728 6939 8551 8551 8551 8551 8551 8551 i
72.246.151.0/24	4.69.184.193	0	0	0 3356 3257 8551 i
72.246.151.0/24	208.51.134.255	0	0	0 3549 3356 6453 8551 i
72.246.151.0/24	89.149.178.10	10	0	0 3257 8551 i
72.246.151.0/24	129.250.1.71	11	0	0 2914 6453 8551 i
72.246.151.0/24	144.228.241.130	80	0	0 1239 6453 8551 i

Figure 2: Our LSTM architecture.

A Deep Learning Approach for IP Hijack Detection Based on ASN Embedding

Datasets

- Route Views[1] BGP announcements (RV), collected in March 2018
  - 3,600,000 BGP paths
  - 62,525 Ases
  - 113,400 undirected AS links
- Labeled BGP routes:
  - Consists of approximately 2,648,900 standard routes ('GREEN') and 47,800 hijacked routes ('RED')
  - The labeling was generated by combinations of VF algorithms[2] and manual work

72.246.151.0/24	196.7.106.245	0	0	0 2905 6939 8551 8551 8551 8551 8551 8551 i
72.246.151.0/24	80.91.255.137	0	0	0 1299 6453 8551 i
72.246.151.0/24	85.114.0.217	0	0	0 8492 8551 i
72.246.151.0/24	91.228.151.1	0	0	0 31019 8551 ?
72.246.151.0/24	202.93.8.242	0	0	0 24441 1299 1299 1299 6453 8551 i
72.246.151.0/24	87.121.64.4	0	0	0 57463 8551 i
72.246.151.0/24	94.156.252.18	0	0	0 34224 8551 i
72.246.151.0/24	105.16.0.247	0	0	0 37100 8551 i
72.246.151.0/24	212.66.96.126	0	0	0 20912 6939 8551 8551 8551 8551 8551 8551 i
72.246.151.0/24	206.24.210.80	0	0	0 3561 209 6453 8551 i
72.246.151.0/24	198.58.198.255	0	0	0 1403 6939 8551 8551 8551 8551 8551 8551 i
72.246.151.0/24	198.58.198.254	0	0	0 1403 6939 8551 8551 8551 8551 8551 8551 i
72.246.151.0/24	154.11.12.212	0	0	0 852 6939 8551 8551 8551 8551 8551 8551 i
72.246.151.0/24	12.0.1.63	0	0	0 7018 6453 8551 i
72.246.151.0/24	147.28.7.1	0	0	0 3130 1239 6453 8551 i
72.246.151.0/24	137.39.3.55	0	0	0 701 3257 8551 i
72.246.151.0/24	216.221.157.162	0	0	0 40191 6939 8551 8551 8551 8551 8551 8551 i
72.246.151.0/24	202.73.40.45	0	0	0 18106 8551 i
72.246.151.0/24	198.129.33.85	1	0	0 293 6453 8551 i
72.246.151.0/24	140.192.8.16	0	0	0 54728 6939 8551 8551 8551 8551 8551 8551 i
72.246.151.0/24	4.69.184.193	0	0	0 3356 3257 8551 i
72.246.151.0/24	208.51.134.255	0	0	0 3549 3356 6453 8551 i
72.246.151.0/24	89.149.178.10	10	0	0 3257 8551 i
72.246.151.0/24	129.250.1.71	11	0	0 2914 6453 8551 i
72.246.151.0/24	144.228.241.130	80	0	0 1239 6453 8551 i

1. University of Oregon, Route Views Project, http://www.routeviews.org, March 2018
2. *[**Shavitt et al. 2009**]* "Near-Deterministic Inference of AS Relationships" *(ND-ToR)*

BGP2VEC[1] – ASN Embeding

AS8492 | AS9002 | AS3356 | AS11537 | AS22388 | AS7660 | AS23855 AS132500

Input	Output
(AS11537,	AS9002)
(AS11537,	AS3356)
(AS11537,	AS22388)
(AS11537,	AS7660)

- Based on Word Embedding (Word2Vec[2]), broadly used in NLP
- Embedding = represent discrete variables as continuous vectors
- An ASN is characterized by its context, i.e., neighboring ASNs
- V = 62,525, N= 32

An example with V= 4:

1. [**Shapira and Shavitt 2020**] *"Unveiling the Type of Relationship Between Autonomous Systems Using Deep Learning" (BGP2Vec)*
2. [**Mikolov et al. 2013**] *"Distributed representations of words and phrases and their compositionality" (Word2Vec)*

Exploration of ASN Embedings

Neighbour	ASN	Owner	Cosine Similarity	Degree	Distance from Tier-1	AS Class	Country	ToR	Grade
-	**3356**	Level3	1	5035	**0**	NSP	USA	-	-
1st	3549	Level3	0.897	2334	**0**	NSP	USA	S2S	5
2nd	1299	Telia	0.850	1747	**0**	NSP	Sweden	P2P	4
3rd	701	Verizon	0.849	1216	**0**	NSP	USA	P2P	3
4th	286	KPN	0.844	267	**0**	NSP	Netherlands	P2P	2
5th	6071	Unisys	0.843	4	1	-	USA	P2C	0

(a) AS3356: Level3, Tier 1 and siblings similarity example; Total similarity grade: 14.

Neighbour	ASN	Owner	Cosine Similarity	Degree	Distance from Tier-1	AS Class	Country	ToR	Grade
-	378	MACHBA	1	4	2	**Research**	Israel	-	-
1st	3268	CyNet	0.929	3	2	**Research**	Cyprus	None	5
2nd	1930	FCT	0.927	10	2	**Research**	Portugal	None	4
3rd	40981	University of Montenegro	0.925	2	2	**Research**	Montenegro	None	3
4th	57961	RASH	0.911	3	2	**Research**	Albania	None	2
5th	199354	ASREN	0.901	4	2	**Research**	Jordan	None	1

(c) AS378: MACHBA - Israel Inter-University Computation Center, Educational/Research similarity example; Total similarity grade: 15.

Neighbour	ASN	Owner	Cosine Similarity	Degree	Distance from Tier-1	AS Class	Country	ToR	Grade
-	15169	**Google**	1	54	1	**Content**	**USA**	-	-
1st	36385	**Google**	0.759	4	1	**Content**	USA	**S2S**	5
2nd	63293	**Facebook**	0.755	17	1	**Content**	USA	None	4
3rd	16591	**Google**	0.743	11	1	Cable/DSL/ISP	Canada	**S2S**	3
4th	133982	EXCITEL	0.739	6	2	Cable/DSL/ISP	India	None	0
5th	38726	VTC DIGICOM	0.736	16	1	NSP	Vietnam	None	0

(e) AS15169: Google, Content Provider similarity example; Total similarity grade: 12.

Training Neural Neyworks (IP Hijack)

- An LSTM Neural Network which is comprised of five layers
- *Categorical cross entropy* loss function
- Using the *Adam* gradient-based optimizer with default hyper-parameters
- We build and run our network using K + TensorFlow
- We train our network based on our labeled dataset
- We use 20% of the samples as a test set
- We run our network for 10 epochs
- Inference time: 0.1 milliseconds on a single Intel CPU

Figure 2: Our LSTM architecture.

Experiments and Results – IP Hijack

- IP hijack detection based on ASN embeding
  - 99.99% Accuracy, 0.00% FA
- 50% of our misclassified predictions were wrong, i.e., we found errors in the labeled dataset

Results on BGP data for Ground Truth Events

- The dataset[1] contains 70 events from February 2008 to July 2018
  - with an average number of 669 AS paths per event
- We classified correctly **all the events within 2 years** of our training data, or 2/3 of all the valid events

Table 3: Results over the *BGP data for ground truth events* dataset.

Category	Prepending	Typo	MOAS	Forged Path	All
Total Events	21	15	17	17	70
Valid Events	21	14	9	4	48
Detected Events	**18**	**8**	**3**	**3**	**32**
Success	**85.7%**	**57.1%**	**33.3%**	**75.0%**	**66.7%**
MAPS	0.986	0.985	0.982	0.988	0.985
Red Prevalence	50.1%	46.3%	27.5%	46.3%	47.1%

1. **[Cho et al. 2019]** *"BGP hijacking classification", TMA*

Summary

- A novel approach for ASN embedding using deep learning (BGP2VEC)
  - Unsupervised method
  - Based only on BGP announcements without any side-information
  - A building block for many problems
- Achieves excellent results for IP Hijack Detection
  - Without any assumptions (no 'VF')
  - 99.99% Accuracy with 0.00% FA on our own proprietry dataset
  - Although our method was trained with a dataset from March 2018 , we classified correctly 2/3 of past events, and al <u>all</u> recent hijack events
  - As far as we know, we are the first to employs deep learning for this problem.

Thank you for your attention. Questions?

TEL AVIV UNIVERSITY אוניברסיטת תל אביב

https://talshapira.github.io/ https://www.eng.tau.ac.il/~shavitt/