6GAN: IPv6 Multi-Pattern Target Generation via Generative Adversarial Nets with Reinforcement Learning

中国科学院信息工程研究所
INSTITUTE OF INFORMATION ENGINEERING,CAS

IEEE INFOCOM

Tianyu Cui, Gaopeng Gou, Gang Xiong, Chang Liu, Peipei Fu and Zhen Li

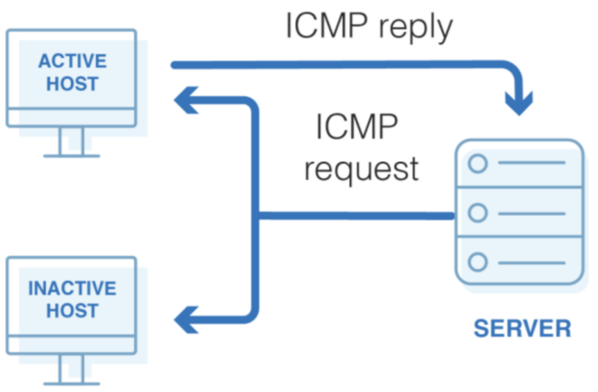
Institute of Information Engineering, Chinese Academy of Sciences
School of Cyber Security, University of Chinese Academy of Sciences

Background - IPv6 Scanning

IPv6 Scanning

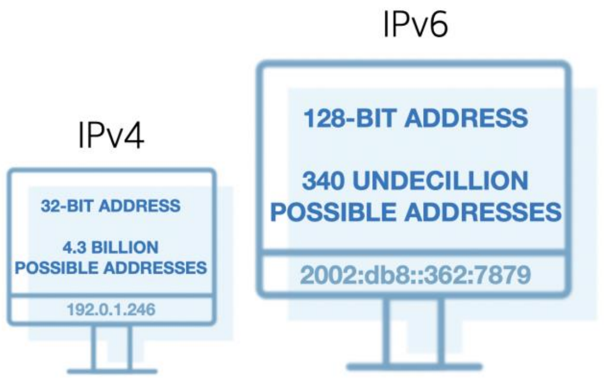
Global IPv6 Address Exploration

- Enhancing the ability of researchers to conduct wide-ranging assessments of the next-generation Internet.
- Passive measurement - limited by vantage points to monitor the traffic.
- **Active scanning** - a fast means required by the community.



Bottlenecks of IPv6 Scanning

- The system sends a ping to each device on the network and awaits a response.
- IPv6 - 128-bit address space - 340 undecillion addresses - Can not work !



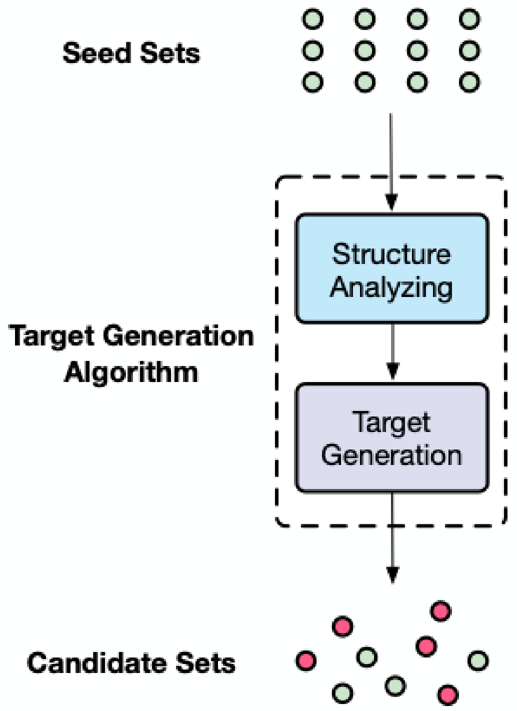
Background - IPv6 Target Generation

IPv6 Target Generation

Target Generation Algorithms[1,2,3]

- A recently proposed solution to overcome IPv6 scanning bottlenecks.
- **Seed sets** of active IPv6 seed addresses as the input.
- **Structure analyzing** - learning features of the seed set.
- **Target Generation** - predicting the active individuals or regions in the real network space to provide the **candidate set** waiting for scanning.
- Budget - the size of the candidate set.

The quality of the candidate set is directly determined by the algorithmic design.



[1] Foremski, P., Plonka, D., Berger, A.: Entropy/ip: Uncovering structure in ipv6 addresses. In: Proceedings of the 2016 Internet Measurement Conference. pp. 167–181. ACM (2016)
[2] Murdock, A., Li, F., Bramsen, P., Durumeric, Z., Paxson, V.: Target generation for internet-wide ipv6 scanning. In: Proceedings of the 2017 Internet Measurement Conference. pp. 242–253 (2017)
[3] Z. Liu, Y. Xiong, X. Liu, W. Xie, and P. Zhu, "6tree: Efficient dynamic discovery of active addresses in the ipv6 address space," Computer Networks, vol. 155, pp. 31–46, 2019.

Challenge - IPv6 Addressing Pattern

Target Generation Challenge

Challenge 1 - IPv6 addressing pattern

Network administrators are allowed to freely select IPv6 address configuration schemes, which enables multiple allocation patterns for **interface identifier (IID)** in the address. According to RFC 7707:

Embedded-IPv4	0:0:c0a8:20a	Embedding an IPv4 address 192.168.2.10
Embedded-port	0:0:0:80	Embedding a decimal port 80 for HTTP
IEEE-derived	250:56ff:fe89:49be	Inserting word "fffe" between OUI and the rest of the Ethernet address
Low-byte	0:0:0:a	Only setting the least significant bytes in one or two lowest-order
Pattern-bytes	face:b00c:0:a7	Specific addressing patterns different from the above
Randomized	7c61:2880:3148:36e1	Privacy addresses with a pseudorandom IID representation

- 2001:0db8:0106:0001:????:????:????:???? - How to determine ?
- Multiple IPv6 schemes cause difficulty in algorithmic inferences.

Challenge - IPv6 Aliasing

Target Generation Challenge

Challenge 2 - IPv6 Aliasing

Aliased addresses refer to all addresses under aliased prefixes, which unconditionally respond to scan queries but are not bound to unique devices. For instance:

2001:db8::/32 is a known aliased prefix.
Then 2001:db8::20:1a is an aliased address.

- Aliased addresses seriously affect the accuracy of host discovery approaches.
- Performing alias detection has been a consensus in IPv6 scanning.

Consideration

Multi-Pattern Target Generation

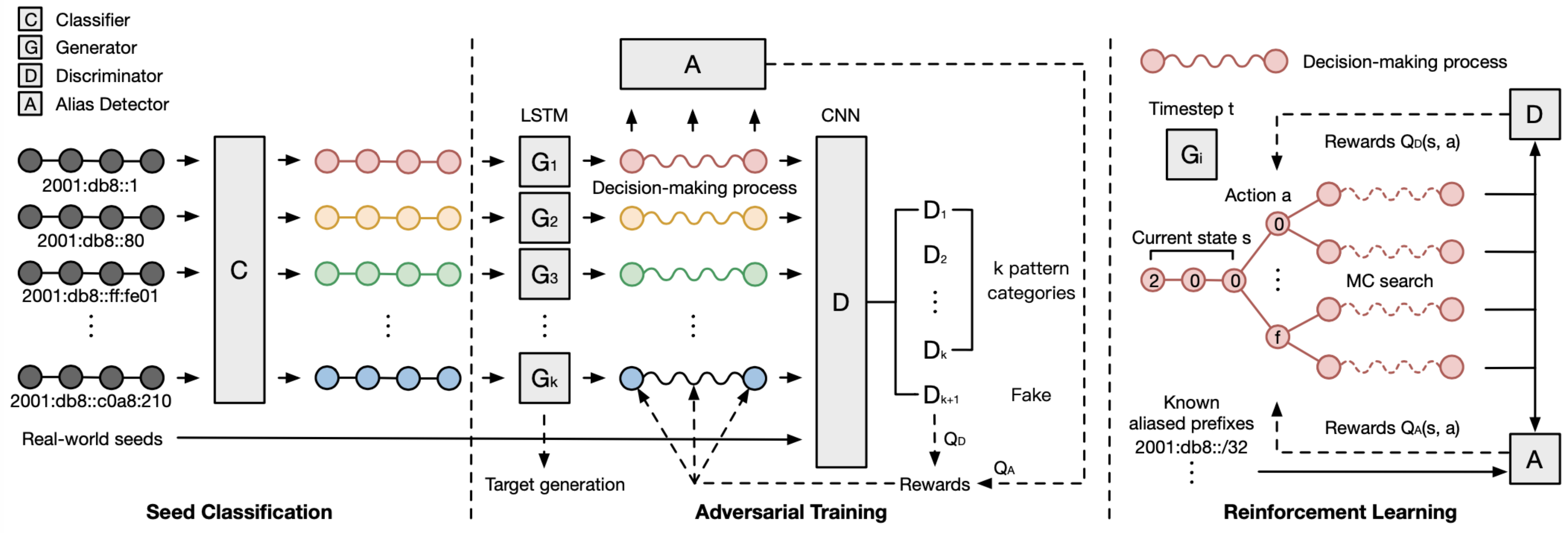
- Addressing patterns could be clustered into limited categories.
- Target generation can't bear the pressure of the whole IPv6 address space.
- A deep eye on each addressing pattern are urgently required.

Algorithm-level Alias Detection

- Candidate sets detection - consuming the budget to generate aliased addresses.
- Seed sets detection - reconstructing the aliased address during prediction.
- Discouraging learning aliased prefixes during algorithmic execution.

6GAN

Overall Architecture



- **Seed Classification** - pattern discovery through known seed classification methods.
- **Generator Learning -** generating addresses with k pattern types to deceive the discriminator.
- **Discriminator Learning** - distinguishing between fake addresses generated by generators and real addresses.
- **Alias Detection** - helping prevent the generation of aliased addresses at the algorithmic level.

6GAN

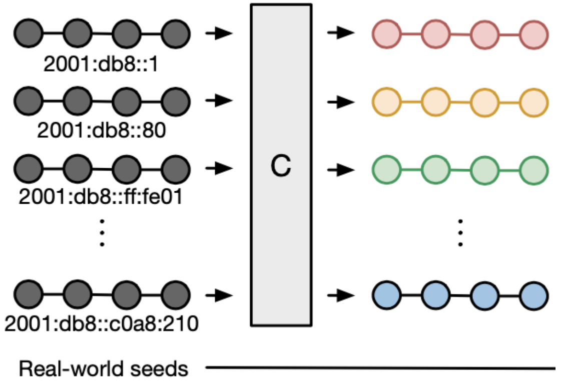
Seed Classification

we provide the following three seed classification methods to promote pattern discovery and determine the number of generators k:

- **RFC Based** - According to possible IPv6 addressing patterns proposed in RFC 7707, the addr6 tool in ipv6toolkit[4] can match the patterns mentioned in RFC 7707.

- **Entropy Clustering** - Gasser et al.[5] proposed entropy clustering, which uses information entropy of the nybble value under the same prefix in the seed set as a prefix fingerprint to perform unsupervised clustering to discover the prefix-level pattern set.

- **IPv62Vec** - Cui et al.[6] proposed IPv62Vec, which implements the mapping from address space to vector space by learning the addressing patterns with similar context of words in the address.



Seed Classification

[4] F. Gont, “Security/robustness assessment of ipv6 neighbor discovery implementations,” 2012.
[5] O. Gasser, Q. Scheitle, P. Foremski, Q. Lone, M. Korczyń ski et al., “Clusters in the expanse: Understanding and unbiasing ipv6 hitlists,” in Proceedings of the 2018 Internet Measurement Conference, IMC, 2018, pp. 364–378.
[6] T. Cui, G. Xiong, G. Gou, J. Shi, and W. Xia, “6veclm: Language modeling in vector space for ipv6 target generation,” arXiv preprint arXiv:2008.02213, 2020.

6GAN

Generator Learning

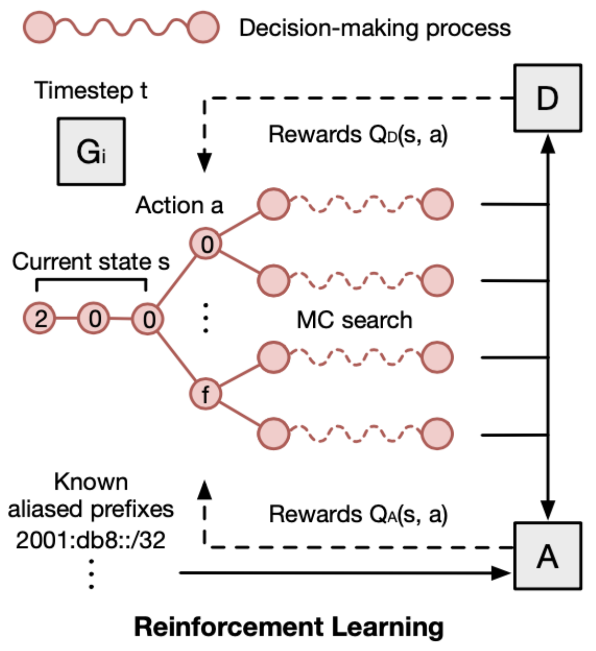
Target generation problem - address sequence decision-making problem

- A hexadecimal IPv6 address $X_{0:T} = (x_0, ..., x_t, ..., x_T), x_t \in V = \{0, 1, ..., f\}$
- State *s* at timestep *t* - currently produced address nybbles $X_{0:t-1} = (x_0, ..., x_{t-1})$
- Action *a* - the next nybble value x_t to be select
- $G_{\theta_i}(a = x_t | s = X_{0:t-1})$ - the probability of performing action *a* at the state *s*
- $Q_{AD_\phi}^{G_{\theta_i}}(s = X_{0:t-1}, a = x_t)$ - assessment of the sequence $X_{0:t}$ based on the discriminator *D* and the alias detector *A*

- The objective function $J(\theta_i)$ of the i-th generator :

$$J(\theta_i) = \sum_{t=1}^{T} G_{\theta_i}(x_t | X_{0:t-1}) Q_{AD_\phi}^{G_{\theta_i}}(X_{0:t-1}, x_t)$$

$$Q_{AD_\phi}^{G_{\theta_i}}(s, a) = Q_{D_\phi}^{G_{\theta_i}}(s, a) + \alpha Q_{A}^{G_{\theta_i}}(s, a)$$ where α is a hyperparameter.



6GAN

Generator Learning

At each timestep *t* - incomplete sequence $X_{0:t}$
To produce a complete sequence $X_{0:T}$ for judgment

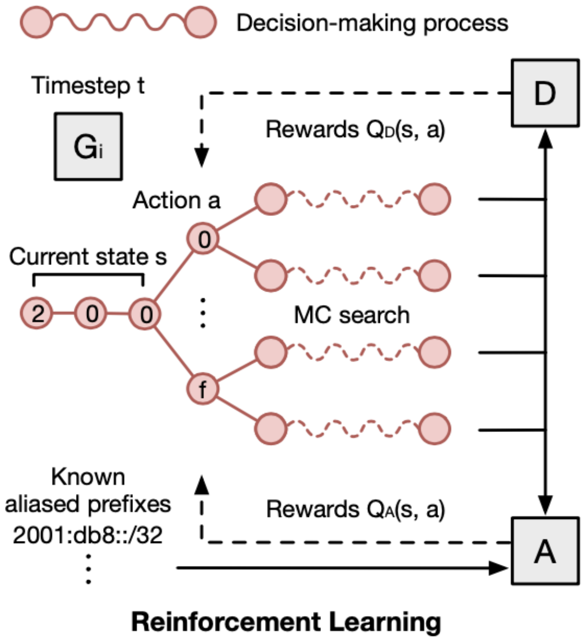
- N-time Monte Carlo search with a roll-out policy

$$\mathrm{MC}^{G_{\theta_i}}(X_{0:t}; N) = \{X_{0:T}^{1}, ..., X_{0:T}^{N}\}$$

All generators of 6GAN use Long Short-Term Memory (LSTM) cells to model $G_{\theta_i}(a|s)$:

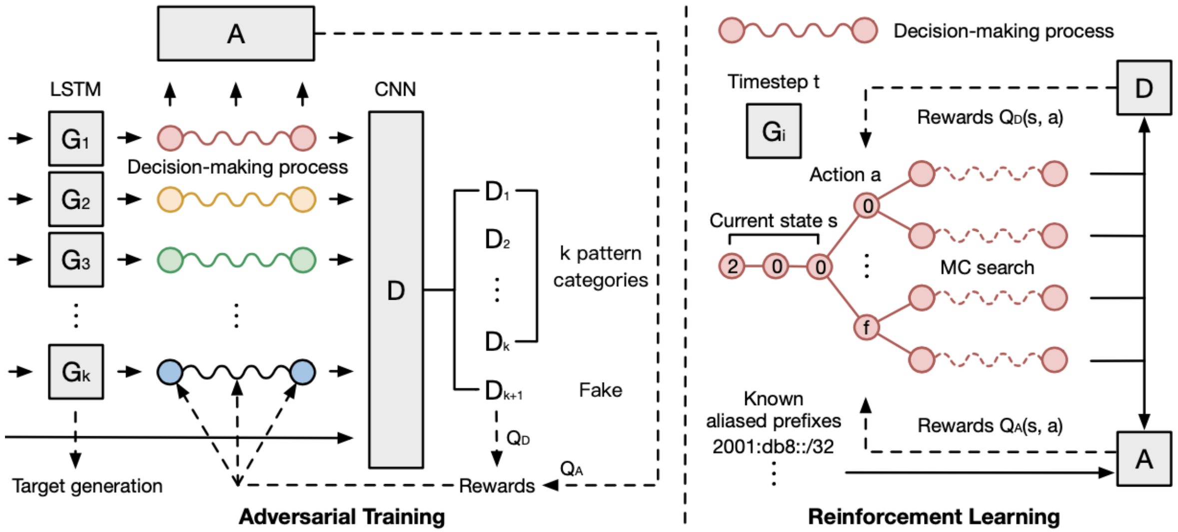
$$p(x_t|X_{0:t-1}) = \mathrm{softmax}(c + wh_t)$$
$$\text{where} \quad h_t = \mathrm{LSTM}(h_{t-1}, x_{t-1})$$

- The parameters are a bias matrix *c* and a weight matrix *w*.
- Softmax function achieves the selection probability of x_t.
- Each generator independently learns the addressing pattern to generate specific pattern addresses.



6GAN

Discriminator Learning



Multi-class classification objective

- Trained with the real-world seed addresses and the generated addresses.
- k + 1 categories - k pattern categories and a fake category.
- The objective function $J(\phi)$ of the discriminator is:

$$J(\phi) = -\sum_{i=1}^{k} \mathbb{E}_{X\sim p_i}[\log D_\phi^i(X)] - \mathbb{E}_{X\sim G_\theta}[\log D_\phi^{k+1}(X)]$$

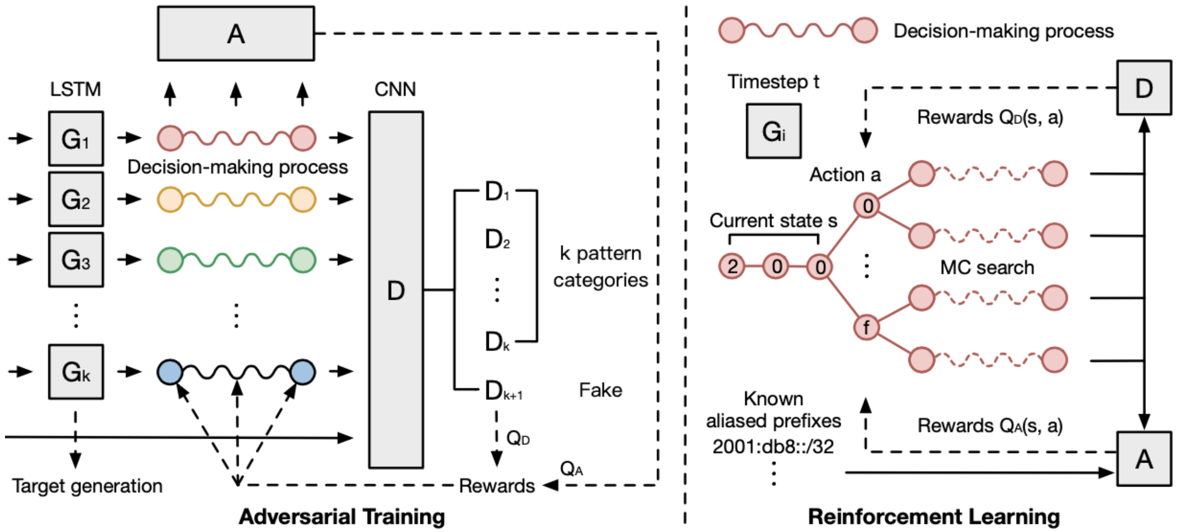
- *D(X)* scores - the probability of a sample being judged as the i-th pattern-type address.

6GAN

Discriminator Learning

- The discriminator provides the reward $Q_{D_\phi}^{G_{\theta_i}}(s, a)$

$$Q_{D_\phi}^{G_{\theta_i}}(s = X_{0:t-1}, a = x_t) = \begin{cases} \frac{1}{N}\sum_{n=1}^{N}(1 - D_\phi^i(X_{0:T}^n)), X_{0:T}^n \in \mathrm{MC}^{G_{\theta_i}}(X_{0:t}; N) & t < T \\ 1 - D_\phi^i(X_{0:t}) & t = T \end{cases}$$



- The discriminator of 6GAN is implemented using Convolutional Neural Networks (CNN) with multiple filters.

- Adversarial training - k generators and one discriminator will be trained alternately to achieve their respective goals.

6GAN

Alias Detection

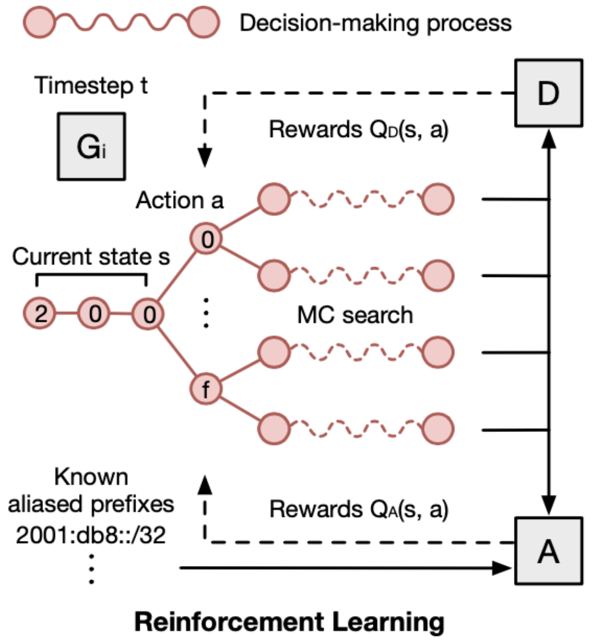
An aliased prefix $P_{0:L} = (p_0, ..., p_t, ..., p_L)$

- The alias detector provides the reward $Q_A^{G_{\theta_i}}(s, a)$
- The alias detector identifies an aliased address when $P_{0:L} = X_{0:L}$

$$A(X) = \begin{cases} \lambda & P_{0:L} = X_{0:L} \\ 0 & P_{0:L} \neq X_{0:L} \end{cases}$$

$$Q_A^{G_{\theta_i}}(s = X_{0:t-1}, a = x_t) = \begin{cases} \frac{t}{NL} \sum_{n=1}^{N} A(X_{0:T}^n), X_{0:T}^n \in \mathbf{MC}^{G_{\theta_i}}(X_{0:t}; N) & t \leq L \\ 0 & T \geq t > L \end{cases}$$

- Positive rewards are only provided on the prefix part.
- Coefficient $\frac{t}{L}$ - hierarchical rewards.
- More likely updating the high index and helping reduce the wide range changes of the prefix region.



Evaluation

Dataset and Evaluation Method

Dataset

- **IPv6 Hitlist** - Public dataset. [7]
- **CERN IPv6 2018** - Passively collected address sets under the China Education and Research Network from March to July 2018.

Dataset	Description	Period	#Seeds
IPv6 Hitlist	Active addresses	June 27, 2020	610.9k
	Source addresses		100.0k
	Aliased prefixes		516.1k
CERN IPv6 2018	Active addresses	March - July 2018	90.1k

Evaluation Method

- Zmapv6 tool. [8]
- ICMPv6, TCP/80, TCP/443, UDP/53, UDP/443 scanning.
- Continuous scanning for three days.

[7] Gasser, O., Scheitle, Q., Foremski, P., Lone, Q., Korczyn ́ski, M., Strowes, S.D., Hendriks, L., Carle, G.: Clusters in the expanse: Understanding and unbiasing ipv6 hitlists. In: Proceedings of the Internet Measurement Conference 2018. pp. 364–378. ACM (2018)
[8] IPv6 Hitlist. https://ipv6hitlist.github.io/

Evaluation

Evaluation Metric

A real-world address seed set with *k* types of pattern $S = \{S_1, ..., S_t, ..., S_k\}$.
A candidate set *C* using the *t*-th pattern generator.

- **Pattern quality** - the imitating ability of the generators to each addressing pattern.

$$Pattern(C) = \frac{1}{|C|} \sum_{i=1}^{|C|} \min\{\psi(C_i, S_{t_j})\}_{j=1}^{j=|S_t|}$$

- **Novelty quality** - the algorithmic ability to generate new address sequences.

$$Novelty(C) = \frac{e}{|C|} \sum_{i=1}^{|C|} (1 - \max\{\varphi(C_i, S_j)\}_{j=1}^{j=|S|})$$

- **Diversity quality** - whether candidate set is a diverse set, which contains a variety of se

$$Diversity(C) = \frac{e}{|C|} \sum_{i=1}^{|C|} (1 - \max\{\varphi(C_i, C_j)\}_{j=1}^{j=|C|, j \neq i})$$

- **Hit rate** - the proportion of active addresses in the candidate arning ability.

$$Hit(C) = \frac{|C \cap T - C \cap T_a|}{|C|}$$

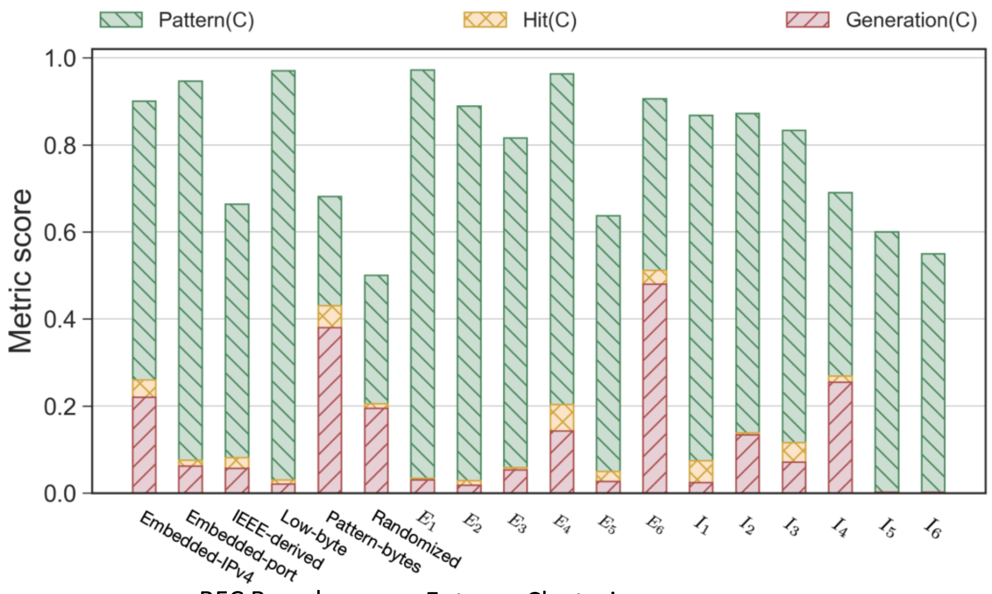
- **Generation rate** - the proportion of the active addre t in the seed ability.

$$Generation(C) = \frac{|C \cap T - C \cap T_a - C \cap S|}{|C|}$$

Where ψ is the Cosine similarity function, φ is the Jaccard similarity function, *e* = 100, *T* is the real active target set in the IPv6 space and T_a is the real aliased addresses set.

Evaluation

Pattern Target Generation



Seed Classification	Budget Allocation	#Targets	Generation(C)
None	1	0.5k	1.06%
RFC Based	11:3:3:1:19:10	12.7k	25.43%
Entropy Clustering	2:1:3:8:1:26	16.9k	33.82%
IPv62Vec	13:70:40:141:1:1	9.1k	18.19%

3 metric scores on each pattern

- 6GAN has a strong ability to imitate most patterns.
- Generation rate - the active user distribution in the addressing patterns.

6GAN's budget allocation

Given the generation rates of k patterns $(r_1, ..., r_i, ..., r_k)$ and the total budget $|C|$.

- the allocated budget of i-th pattern $|C_i|$:

$$|C_i| = \frac{r_i}{\sum_{j=1}^{k} r_j} \times |C|$$

The budget allocation of 6GAN could be represented as $(|C_1| : ... : |C_k|)$.

Evaluation

Pattern Discrimination

6GAN's discriminator can be optimized to achieve pattern discrimination.

- The overall accuracy of the discriminator reaches 0.966 scores for the 6 pattern types.

- 6GAN discriminator possess sufficient capacity to recognize addressing patterns in the IPv6 space.

Category	#Labels	# Preds	#Hits	#Errors	Accuracy
Embedded-IPv4	4.38k	4.54k	4.17k	0.37k	0.954
Embedded-port	0.57k	0.52k	0.50k	0.02k	0.898
IEEE-derived	3.19k	3.37k	3.18k	0.19k	0.998
Low-byte	12.82k	12.04k	11.93k	0.11k	0.931
Pattern-bytes	0.73k	1.49k	0.51k	0.98k	0.701
Randomized	28.31k	28.04k	28.02k	0.02k	0.990
Total	50.00k	50.00k	48.31k	1.69k	0.966

Evaluation

Performance of Alias Detection

Seed set

- 50k active addresses - 50k non-aliased addresses
- 50k source addresses - 7.9k aliased addresses and 42.1k non-aliased addresses

Seed set	Alias Detection	#Aliased Targets	Percentage
Active addresses	W/o	0.01k	0.02%
Active addresses	W/	0.00k	0.00%
Source addresses	W/o	6.91k	13.82%
Source addresses	W/	0.01k	0.02%

Ablation study results

- Training with non-aliased addresses - Recombining the aliased prefix during the sampling.
- Training with dataset containing aliased addresses - Greatly reducing the generation of aliased addresses.

- 6GAN's generator could intelligently avoid exploiting alias regions due to the reward guidance from the alias detector.
- High-quality candidate sets without wasting budgets.

Evaluation

Quality of Generated Addresses

Baselines

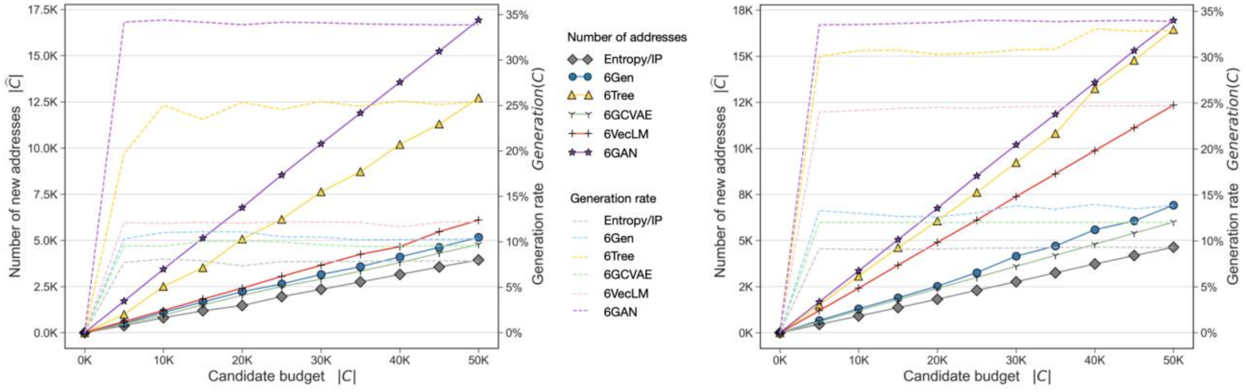
Approach	Target Generation	Alias Detection	Goal
Entropy/IP [13]	Analyzing addressing structures through information entropy	-	Visual address distribution
6Gen [14]	Searching the densest address clusters to provide active regions	Sampling scanning	Remarkable performance
6Tree [15]	Dynamic adjusting search directions with a space tree	Dynamic scanning	Faster time complexity
6GCVAE [16]	Reconstructing addresses through variational autoencoder	-	Deep learning attempts
6VecLM [17]	Predicting address sequences through language modeling	-	IPv6 semantics exploration
6GAN	**Multi-pattern target generation through adversarial training**	**Reinforcement learning**	**Higher-quality candidates**

- **Traditional Design Algorithms** - Entropy/IP, 6Gen, and 6Tree.
- **Deep Learning Approaches** - 6GCVAE, 6VecLM, and 6GAN.

Evaluation

Quality of Generated Addresses

Approach	Novelty(C)	Diversity(C)	Hit(C)	Generation(C)
Entropy/IP	12.37	6.80	12.03%	7.88%
6Gen	11.09	2.05	14.81%	10.33%
6Tree	11.16	2.06	24.40%	24.39%
6GCVAE	12.00	**7.66**	13.61%	9.50%
6VecLM	12.35	6.03	33.16%	12.20%
6GAN	**12.75**	4.73	**36.05%**	**33.21%**



(a) IPv6 Hitlist (b) CERN IPv6 2018

- 6GAN could generate creative addresses with high novelty quality.
- 6GAN obtains a not high diversity quality score.
- 6GAN outperforms all the baseline on the generation rate in our experiments.
- 6GAN could discover 1.03-1.33 times more active addresses than 6Tree.

Conclusion

- We propose **a novel architecture 6GAN** to generate diversified non-aliased active addresses of different addressing pattern types through using multiple generators guided by rewards from a discriminator and an alias detector.

- We employ **a multi-class objective of 6GAN's discriminator**, which can identify IPv6 addressing pattern categories.

- We implement **an alias detection approach embedded in the algorithm** by optimizing the generator, which saves algorithmic budget to generate high-quality candidates.

- We push the **quality of candidate sets** to a higher level. Experiments show that 6GAN outperforms state-of-the-art target generation algorithms on multiple metrics.

THANK YOU FOR LISTENING

Gaopeng Gou
gougaopeng@iie.ac.cn