Packet Generation of SIP Traffic using GANs

Technical and Practical Aspects: Meeting n°2

For full list of references visit: https://bit.ly/3jad5He

(Amar Meddahi 2021)

Outline

- Introduction
  - Summary of the last week
  - Status of the implementation
- Last Achievements
  - SIP-GAN
  - Generator
  - Decoder
  - Preliminaries Results
- Next Step: Evaluation
- Q&A

For full list of references visit: https://bit.ly/3jad5He

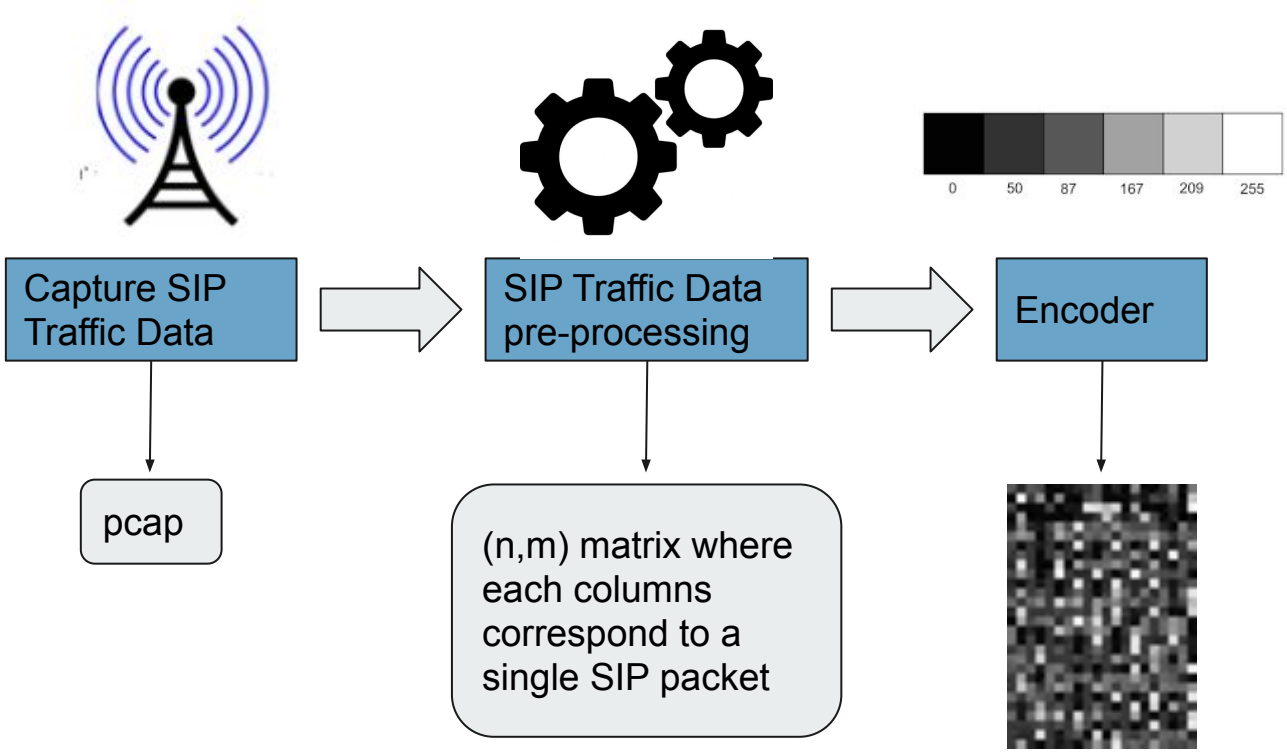
(Amar Meddahi 2021)

Introduction

For full list of references visit: https://bit.ly/3jad5He

(Amar Meddahi 2021)

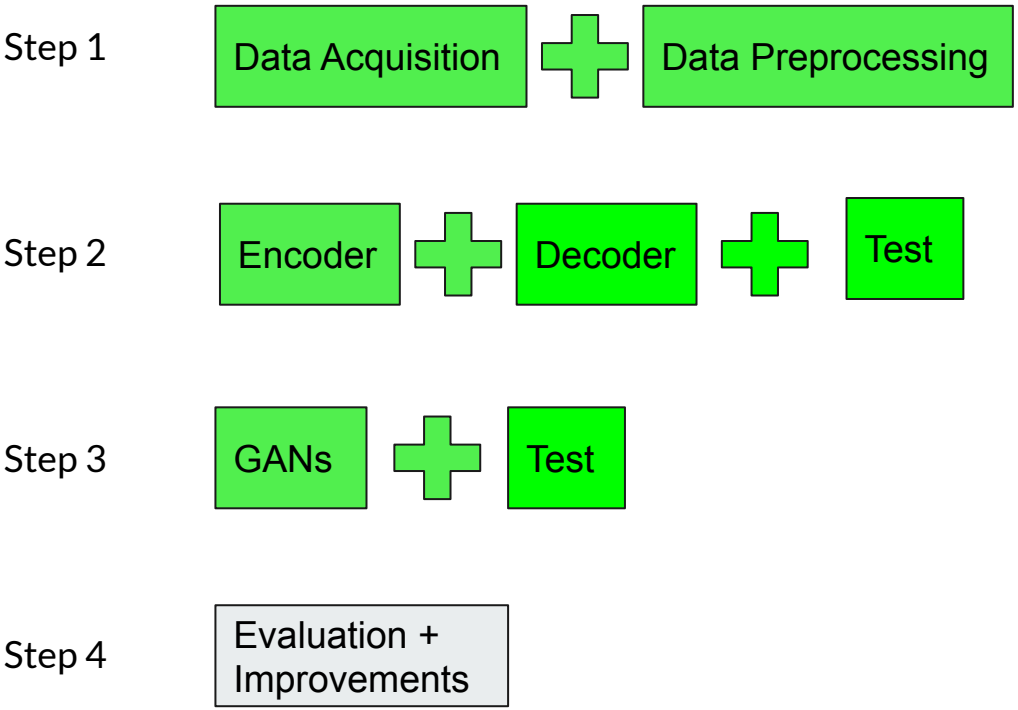
Summary of the last presentation



For full list of references visit: https://bit.ly/3jad5He

(Amar Meddahi 2021)

Status of the implementation



For full list of references visit: https://bit.ly/3jad5He

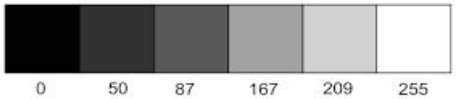
(Amar Meddahi 2021)

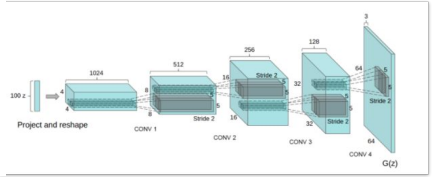
Last achievements

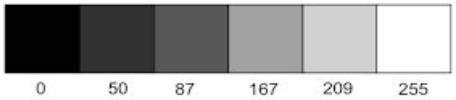
For full list of references visit: https://bit.ly/3jad5He

(Amar Meddahi 2021)

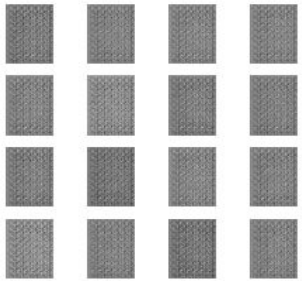
SIP-GAN: Overview







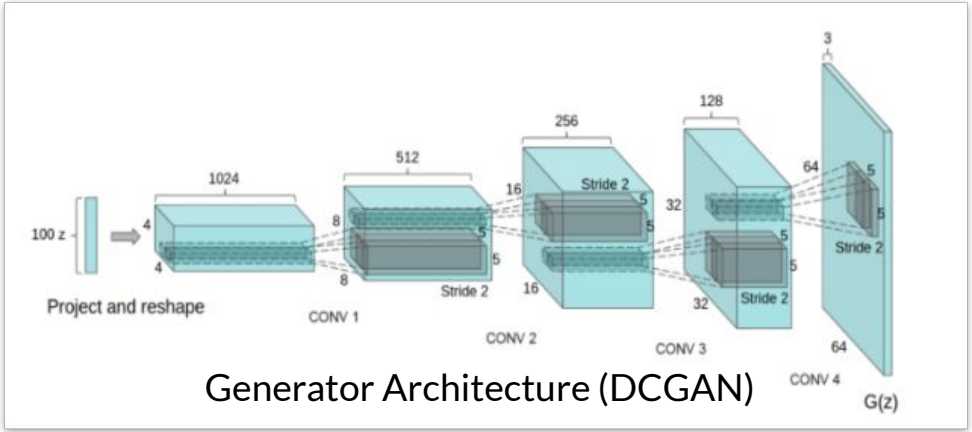
Encoder → Generator → Decoder



For full list of references visit: https://bit.ly/3jad5He

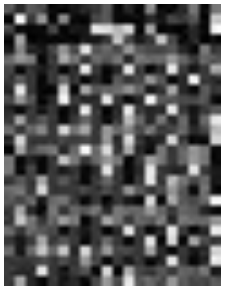
(Amar Meddahi 2021)

Generator

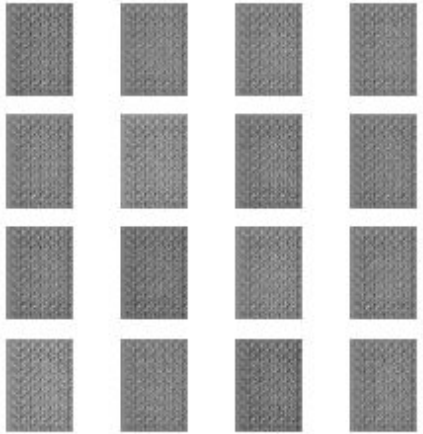


Generator Architecture (DCGAN)

FAKE PACKET



REAL PACKET



Results of the generator on 50 EPOCHS

For full list of references visit: https://bit.ly/3jad5He

(Amar Meddahi 2021)

Decoder

SIP-packet.png

d = 3

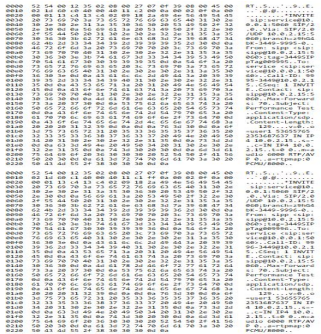
88 88 81 ...
88 88 74
65 95 98
...

SIP-packet

88 88 81
88 88 74
65 95 98

mean → 85

f^{-1} → 5 ... ...



dataset.txt (ETH + IP + UDP + SIP)

text2pcap → pcap

For full list of references visit: https://bit.ly/3jad5He

(Amar Meddahi 2021)

CPU/GPU/Dataset

Evaluation Conditions:

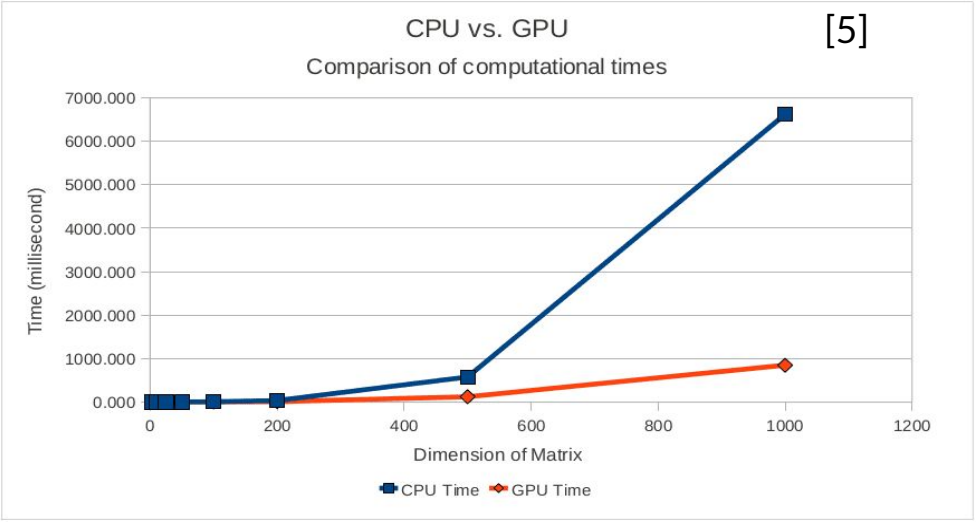
- TensorFlow **GPU + CUDA**
- Dataset = 10000 SIP Packets
- EPOCHS = 50
- Batch Size = 32

AMD Ryzen™ 9 5950X

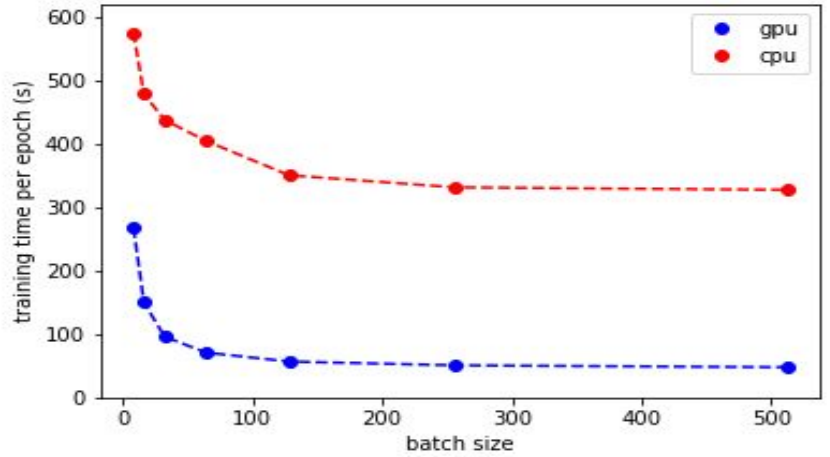
Carte graphique NVIDIA® GeForce RTX™ 3090

64 Go de mémoire DDR4 XMP bicanale à 3 466 MHz ;

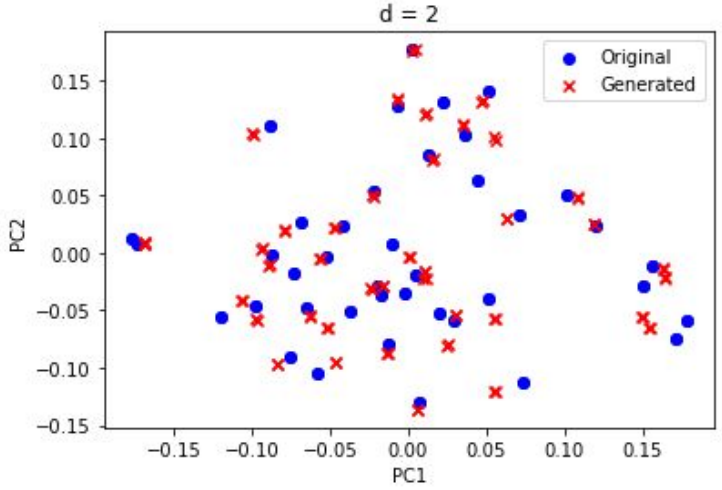
[5]

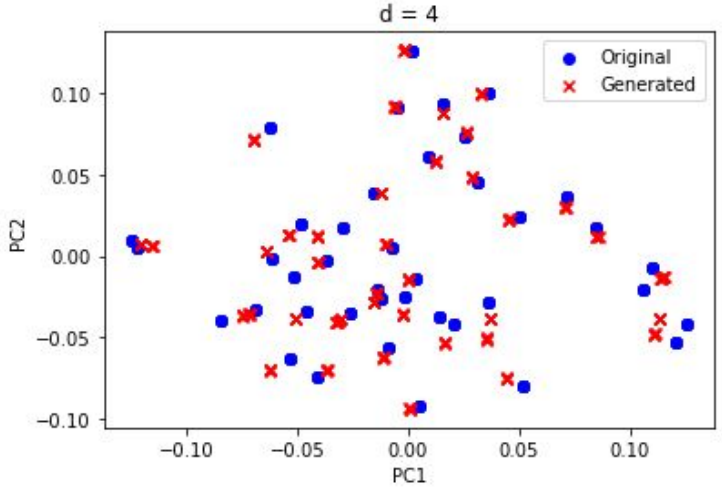


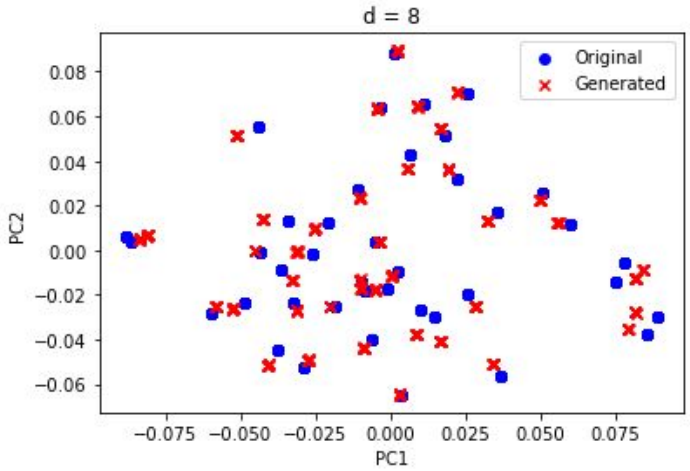
[6]



Preliminaries Results (PCA)







training time:

- d = 8: 1929 sec (32,15 min)

Preliminaries Results (Packet Analysis)

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.0.2.15	10.0.0.1	SIP/SDP	546	Request: INVITE sip:service@10.0.0.1:5060 |

Real SIP INVITE

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	NorskDat_07:0f:5c	RealtekU_13:26:06	0x0a00	560	Ethernet II
2	0.000001	PcsCompu_08:0f:5c	RealtekU_13:26:06	0x0a00	560	Ethernet II
3	0.000002	PcsCompu_08:0f:5c	RealtekU_13:26:06	0x0a00	560	Ethernet II
4	0.000003	PcsCompu_07:0f:5c	RealtekU_13:25:06	0x0a00	560	Ethernet II
5	0.000004	PcsCompu_07:0f:5c	RealtekU_13:25:05	0x0a00	560	Ethernet II
6	0.000005	PcsCompu_07:0f:5d	52:53:00:13:26:06	0x0a00	560	Ethernet II
7	0.000006	NorskDat_08:0f:5c	RealtekU_13:25:05	0x0a00	560	Ethernet II
8	0.000007	PcsCompu_08:0f:5c	RealtekU_13:36:06	0x0a00	560	Ethernet II
9	0.000008	PcsCompu_07:0f:5d	52:53:00:13:26:06	0x0a00	560	Ethernet II
10	0.000009	PcsCompu_07:0f:5c	RealtekU_13:26:06	0x0a00	560	Ethernet II

d = 2

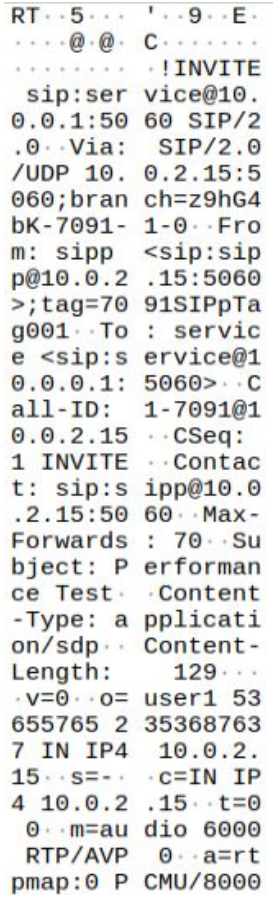
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	NorskDat_06:0f:39	RealtekU_12:35:03	0x0900	560	Ethernet II
2	0.000001	10.0.2.15	10.0.0.1	UDP	560	5060 → 5060 Len=258
3	0.000002	10.0.2.15	10.0.0.2	UDP	560	5060 → 5044 Len=258
4	0.000003	10.0.2.15	10.0.0.1	UDP	560	5060 → 5060 Len=258
5	0.000004	10.0.2.15	10.0.0.1	UDP	560	5060 → 5060 Len=258
6	0.000005	10.0.2.15	10.0.0.1	UDP	560	5060 → 5060 Len=258
7	0.000006	10.0.2.15	10.0.0.1	UDP	560	5060 → 5044 Len=258
8	0.000007	10.0.2.15	10.0.0.1	UDP	560	5060 → 5044 Len=258
9	0.000008	10.0.2.15	10.0.0.1	UDP	560	5060 → 5044 Len=258
10	0.000009	10.0.2.15	10.0.0.1	UDP	560	5060 → 5044 Len=258

d = 4

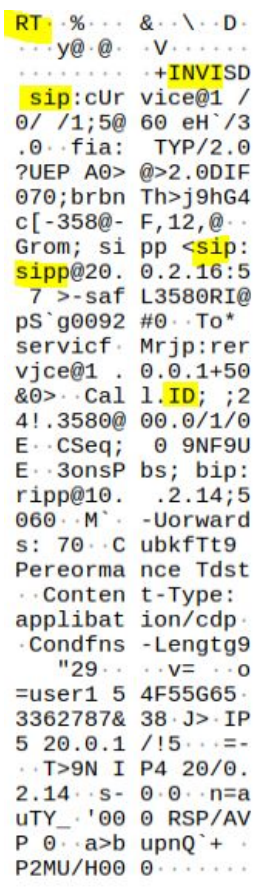
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.0.2.15	10.0.0.1	IPv4	560	Fragmented IP protocol
2	0.000001	10.0.2.15	10.0.0.1	IPv4	560	Fragmented IP protocol
3	0.000002	10.0.2.15	10.0.0.1	IPv4	560	Fragmented IP protocol
4	0.000003	10.0.2.15	10.0.0.1	IPv4	560	Fragmented IP protocol
5	0.000004	10.0.2.15	10.0.0.1	IPv4	560	Fragmented IP protocol
6	0.000005	10.0.2.15	10.0.0.1	IPv4	560	Fragmented IP protocol
7	0.000006	10.0.2.15	10.0.0.1	IPv4	560	Fragmented IP protocol
8	0.000007	10.0.2.15	10.0.0.1	IPv4	560	Fragmented IP protocol
9	0.000008	10.0.2.15	10.0.0.1	IPv4	560	Fragmented IP protocol
10	0.000009	10.0.2.15	10.0.0.1	IPv4	560	Fragmented IP protocol

d = 8

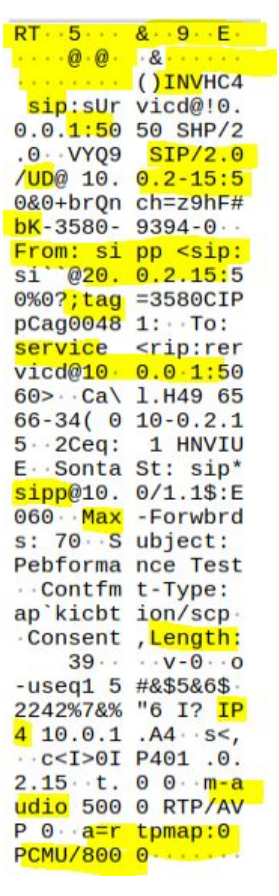
Preliminaries Results (Packet Analysis)



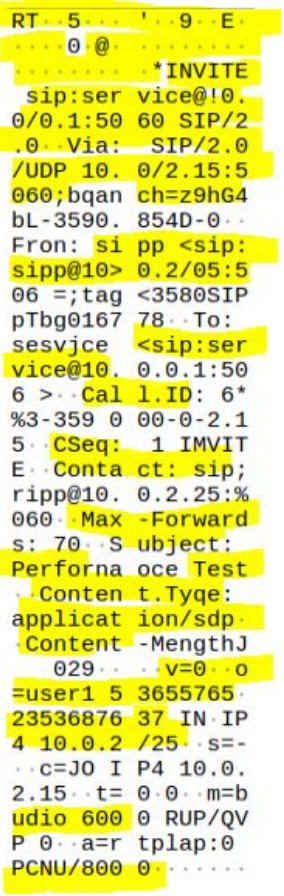
Real SIP INVITE



d = 2



d = 4



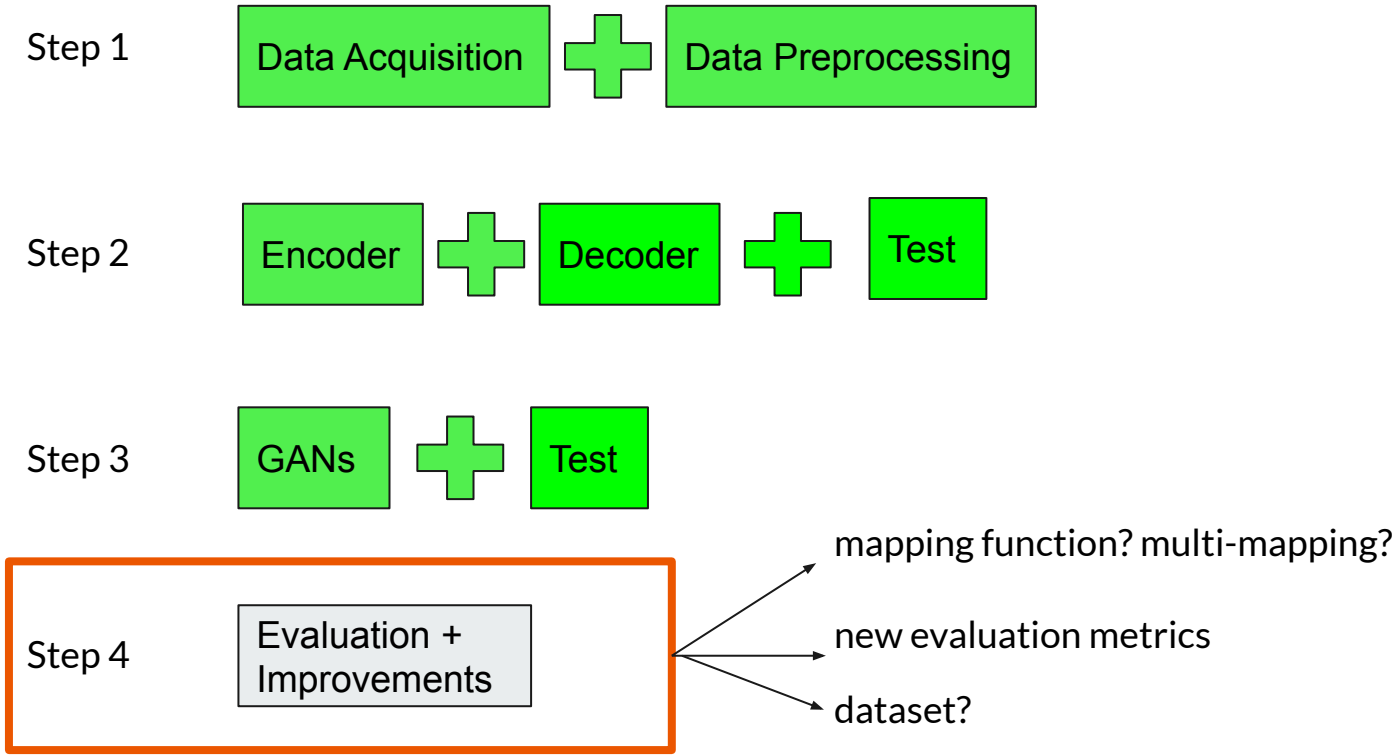
d = 8

Next Step

For full list of references visit: https://bit.ly/3jad5He

(Amar Meddahi 2021)

Next Step: Evaluation



For full list of references visit: https://bit.ly/3jad5He

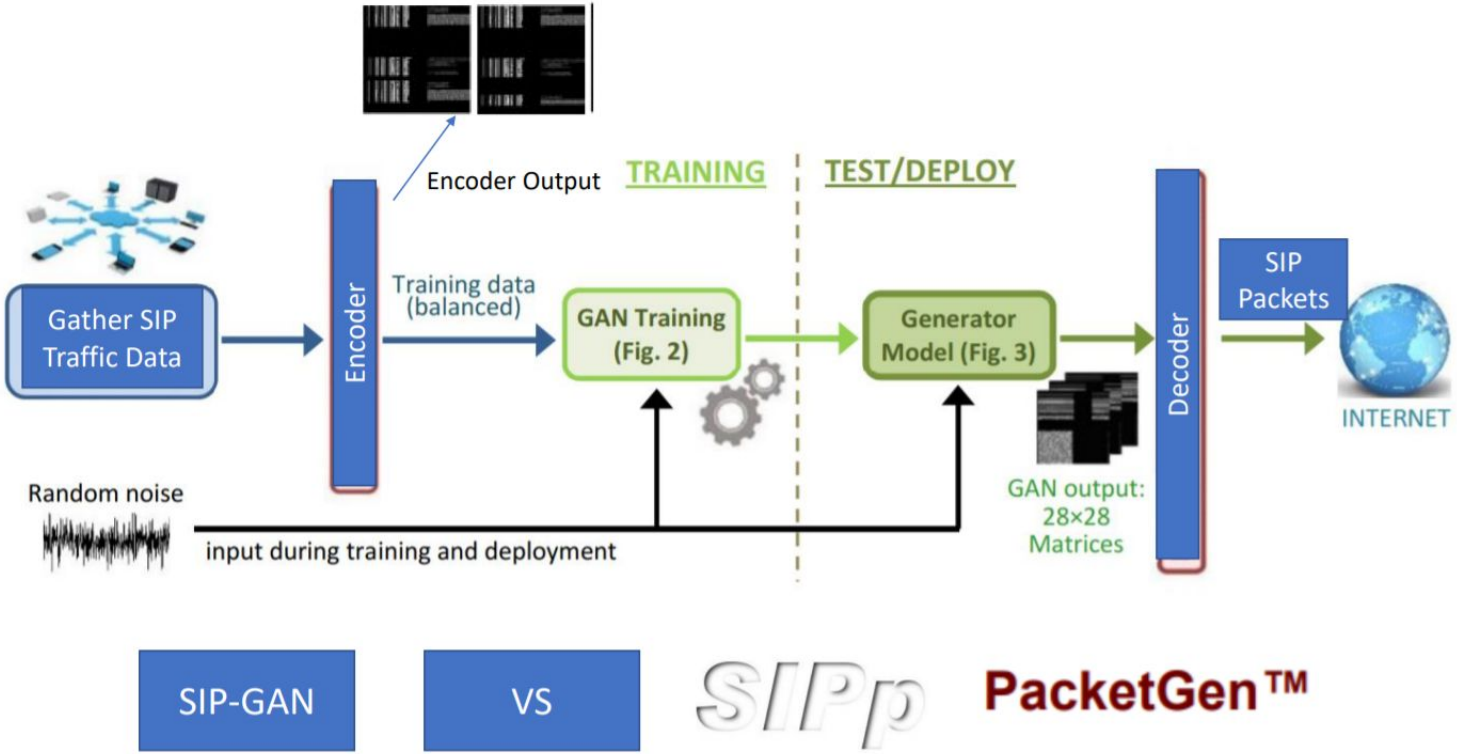
(Amar Meddahi 2021)

Q&A

For full list of references visit: https://bit.ly/3jad5He

(Amar Meddahi 2021)

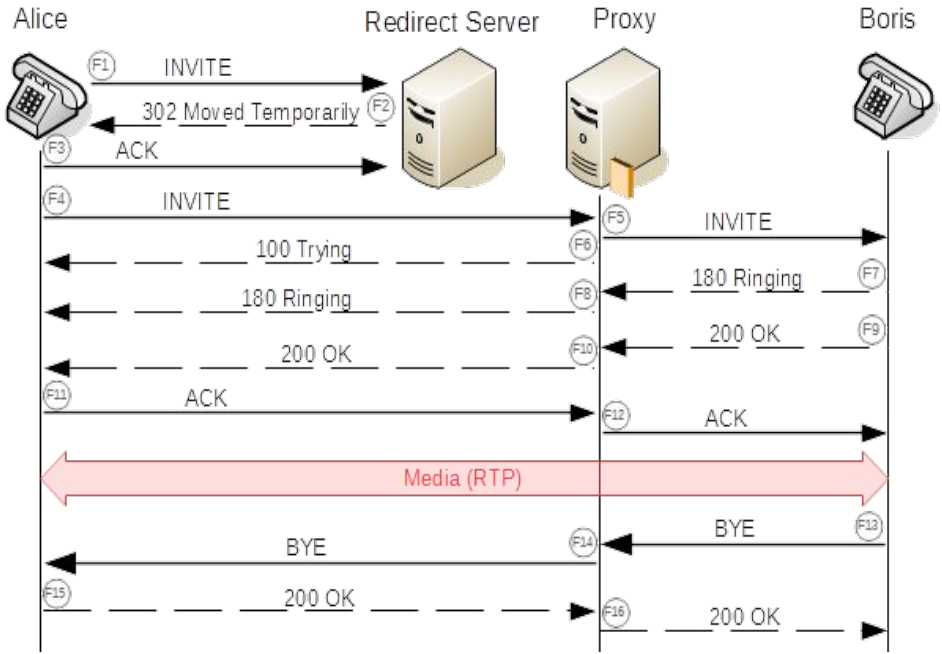
Appendix 1: SIP-GAN



For full list of references visit: https://bit.ly/3jad5He

(Amar Meddahi 2021)

Appendix 2: SIP Protocol



Establishment of a session

Version		Flow Label
Payload Length	Payload Type	Hop Limit
Source Address		
Destination Address		

32 Bit/s

SIP Header

For full list of references visit: https://bit.ly/3jad5He

(Amar Meddahi 2021)