# LUCID: A Practical, Lightweight Deep Learning Solution for DDoS Attack Detection

IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT
2020

# Introduction

- **DDoS** attacks have become more difficult to detect due to the many **combinations** of attack approaches.
- Traditional **signature-based** intrusion detection systems cannot react to new attacks.
- Existing **statistical anomaly-based** detection systems are constrained by the requirement to define thresholds for detection.

➔ **CNN** has advanced the state-of-the-art in certain specific scenarios such as malware detection, network traffic analysis and intrusion detection.

- With the drive towards **edge computing**, it becomes to consider the ability to protect against attacks on resource-constrained devices.

# Contributions

1) CNN for online resource-constrained environments to learn the behaviour of DDoS and benign traffic flows with both low processing overhead and attack detection time. → **LUCID** (Lightweight, Usable CNN in DDoS Detection)
2) A **dataset-agnostic preprocessing mechanism** that produces traffic observations consistent with those collected in existing online systems
3) A **kernel activation analysis** to interpret and explain to which features LUCID attaches importance when making a DDoS classification.
4) An **empirical validation** of LUCID on a resource-constrained hardware platform to demonstrate the applicability of the approach in edge computing scenarios, where devices possess limited computing capabilities.

# Proposed Method

- Network Traffic Preprocessing

| | |
|---|---|
| Why | shared nature of the communication link→packets from different data flows are multiplexed resulting in packets from the same flow being separated for transmission |
| So what | the processing for live presentation of traffic to a NIDS is quite different to the processing of a static dataset |
| solve | converting the traffic flows in a dataset into array-like data structures and splits them into sub-flows based on time windows |

# Network Traffic Preprocessing

- Features extraction

| Pkt # | Time (sec)[1] | Packet Len | Highest Layer[2] | IP Flags | Protocols[3] | TCP Len | TCP Ack | TCP Flags | TCP Window Size | UDP Len | ICMP Type |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 151 | 99602525 | 0x4000 | 0011010001000b | 85 | 336 | 0x018 | 1444 | 0 | 0 |
| 1 | 0.092 | 135 | 99602525 | 0x4000 | 0011010001000b | 69 | 453 | 0x018 | 510 | 0 | 0 |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |
| $j$ | 0.513 | 66 | 78354535 | 0x4000 | 0010010001000b | 0 | 405 | 0x010 | 1444 | 0 | 0 |
| $j+1$ | 0 | 0 | 0 | 0 | 0000000000000b | 0 | 0 | 0 | 0 | 0 | 0 |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |
| $n$ | 0 | 0 | 0 | 0 | 0000000000000b | 0 | 0 | 0 | 0 | 0 | 0 |

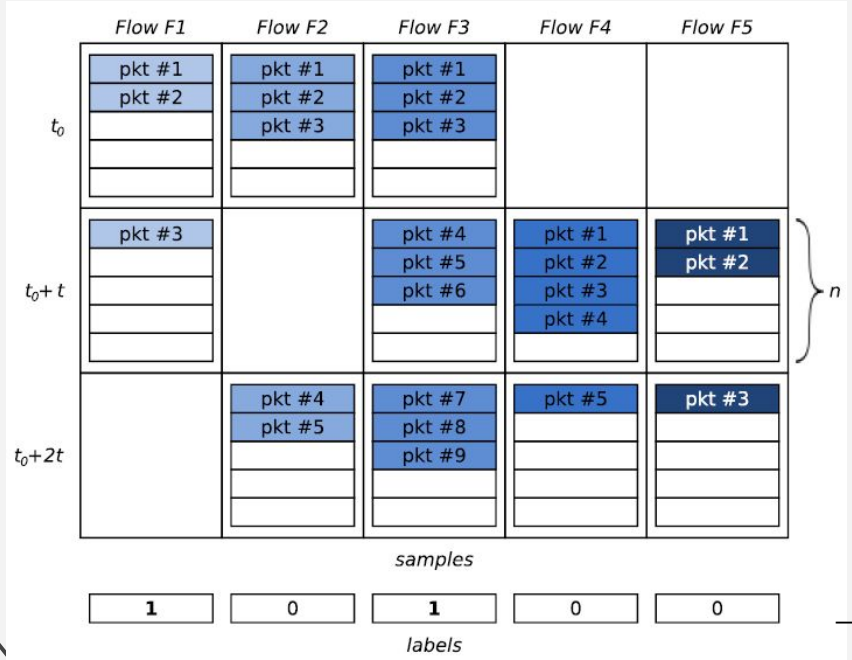
# Network Traffic Preprocessing

- Normalization and padding

| | Pkt # | Time (sec)[1] | Packet Len | Highest Layer[2] | IP Flags | Protocols[3] | TCP Len | TCP Ack | TCP Flags | TCP Window Size | UDP Len | ICMP Type |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| *Packets* | 0 | 0 | 151 | 99602525 | 0x4000 | 0011010001000b | 85 | 336 | 0x018 | 1444 | 0 | 0 |
| | 1 | 0.092 | 135 | 99602525 | 0x4000 | 0011010001000b | 69 | 453 | 0x018 | 510 | 0 | 0 |
| | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |
| | $j$ | 0.513 | 66 | 78354535 | 0x4000 | 0010010001000b | 0 | 405 | 0x010 | 1444 | 0 | 0 |
| *Padding* | $j+1$ | 0 | 0 | 0 | 0 | 0000000000000b | 0 | 0 | 0 | 0 | 0 | 0 |
| | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |
| | $n$ | 0 | 0 | 0 | 0 | 0000000000000b | 0 | 0 | 0 | 0 | 0 | 0 |

# Network Traffic Preprocessing

- Data processing algorithm



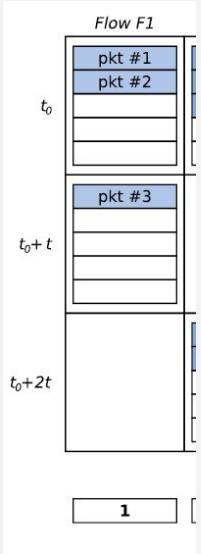

simulates the traffic capturing process of online IDSs
→ the traffic is collected for a certain amount of time t before being sent to the anomaly detection algorithms.

→labelling by the original data

**Algorithm 1** Network Traffic Preprocessing Algorithm

**Input:** Network traffic trace ($NTT$), flow-level labels ($\mathcal{L}$), time window ($t$), max packets/sample ($n$)
**Output:** List of labelled samples ($\mathcal{E}$)

**procedure** PREPROCESSING($NTT$, $\mathcal{L}$, $t$, $n$)
  $\mathcal{E} \leftarrow \emptyset$ ▷ Initialise the set of samples
  $\tau \leftarrow -1$ ▷ Initialise the time window start-time
  **for all** $pkt \in NTT$ **do** ▷ Loop over the packets
    $id \leftarrow pkt.tuple$ ▷ 5-tuple flow identifier
    **if** $\tau == -1$ **or** $pkt.time > \tau + t$ **then**
      $\tau \leftarrow pkt.time$ ▷ Time window start time
    **end if**
    **if** $\left|\mathcal{E}[\tau, id]\right| < n$ **then** ▷ Max $n$ pkts/sample
      $\mathcal{E}[\tau, id].pkts.append(pkt.features)$
    **end if**
  **end for**
  $\mathcal{E} \leftarrow normalization\_padding(\mathcal{E})$
  **for all** $e \in \mathcal{E}$ **do** ▷ Labelling
    $e.label \leftarrow \mathcal{L}[e.id]$ ▷ Apply the label to the sample
  **end for**
  **return** $\mathcal{E}$
**end procedure**

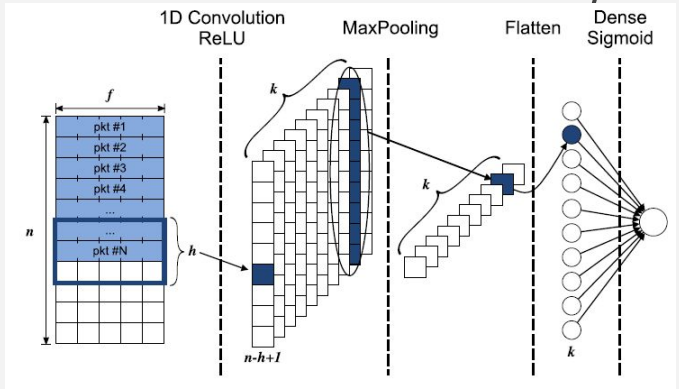



| | | | |
|---|---|---|---|
| $\alpha$ | Learning rate | $n$ | Number of packets per sample |
| $f$ | Number of features per packet | $s$ | Batch size |
| $h$ | Height of convolutional filters | $t$ | Time window duration |
| $id$ | 5-tuple flow identifier | $\tau$ | Time window start time |
| $k$ | Number of convolutional filters | $\mathcal{E}$ | Array of labelled samples |
| $m$ | Max pooling size | $\mathcal{L}$ | Set of labels |

# LUCID Model

- Objective: minimise the complexity and performance time of CNN model for feasible deployment on resource-constrained devices.
- Input: $\boldsymbol{F}$ = [ $\boldsymbol{n}$ x $\boldsymbol{f}$ ] (a traffic flow)
- CNN layer:
  - $\boldsymbol{k}$ filters of size $\boldsymbol{h}$ x $\boldsymbol{f}$ $\rightarrow$ extract and learn local features
  - Activation map a $a_k = ReLU(Conv(F)\, W_k, b_k)$
  - Activation matrix $\boldsymbol{A}$ of size $(n\text{-}h\text{+}1)$ x $k$
- Max pooling、flatten
- Output: sigmoid
  - $\boldsymbol{P}$ >0.5 $\rightarrow$ DDoS
- Loss function

$$c = -\frac{1}{s}\sum_{o=1}^{s}(y_o \log p_o + (1-y_o)\log(1-p_o))$$



# Datasets

- ISCX2012, CIC2017 and CSECIC2018

| Dataset | Traffic trace | #Flows | #Benign | #DDoS |
|---|---|---|---|---|
| ISCX2012 | Tue15 | 571698 | 534320 | 37378 |
| CIC2017 | Fri7PM | 225745 | 97718 | 128027 |
| CSECIC2018 | Wed21 | 1048575 | 360832 | 687743 |

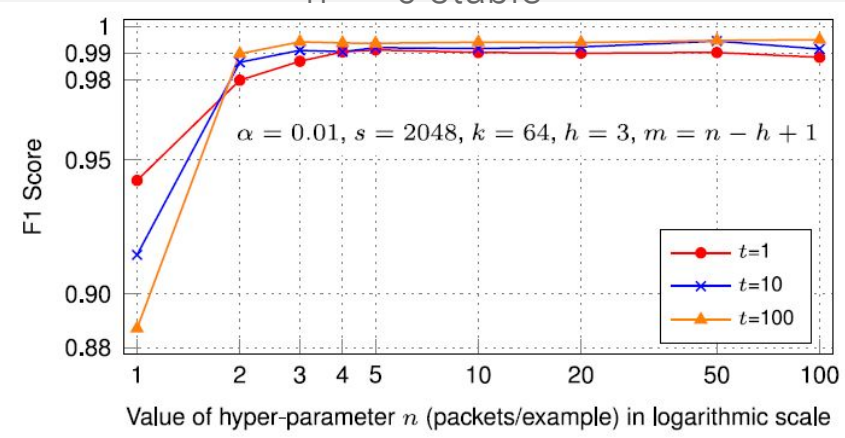
- Data processing algorithm → UNB201X
- 90% training (10% validation) + 10% testing

# Hyper-parameter Tuning

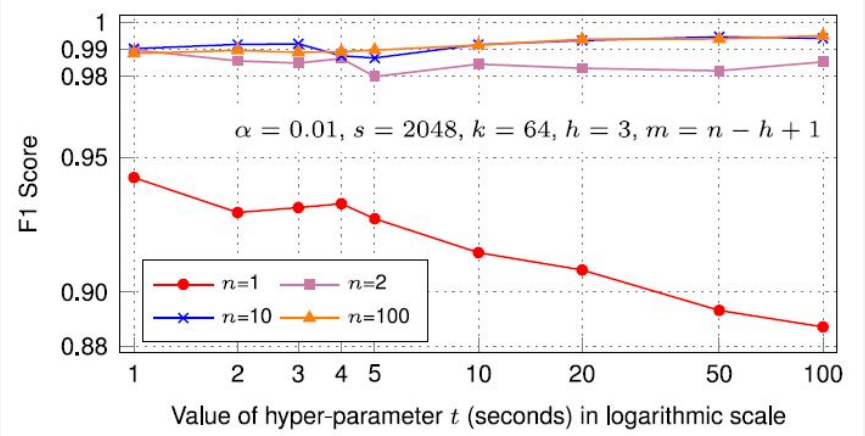
- Grid search (using F1 score as performance metric)
- Using the validation set

Maximum number of packets/samples

n >= 5 stable




insensitive to "time window" for n > 1



# Hyper-parameter Tuning (cont.)

- Height of convolutional filters
  - (testing) h = 1, 2, 3, 4, 5 $\longrightarrow$ h=3 (0.9950)
- Number of convolutional filters
  - k by powers of 2, from k = 1 to k = 64
  - steady increase in the F1 score $\longrightarrow$ k = 64
- Result:
  - grid search on 2835 combinations of hyperparameters
  - $\mathbf{n}$ = 100, $\mathbf{t}$ = 100, $\mathbf{k}$ = 64, $\mathbf{h}$ = 3, $\mathbf{m}$ = 98, $\mathbf{s}$ = 2048, $\alpha$ = 0.01
  - Adam optimizer

# Experimental Result

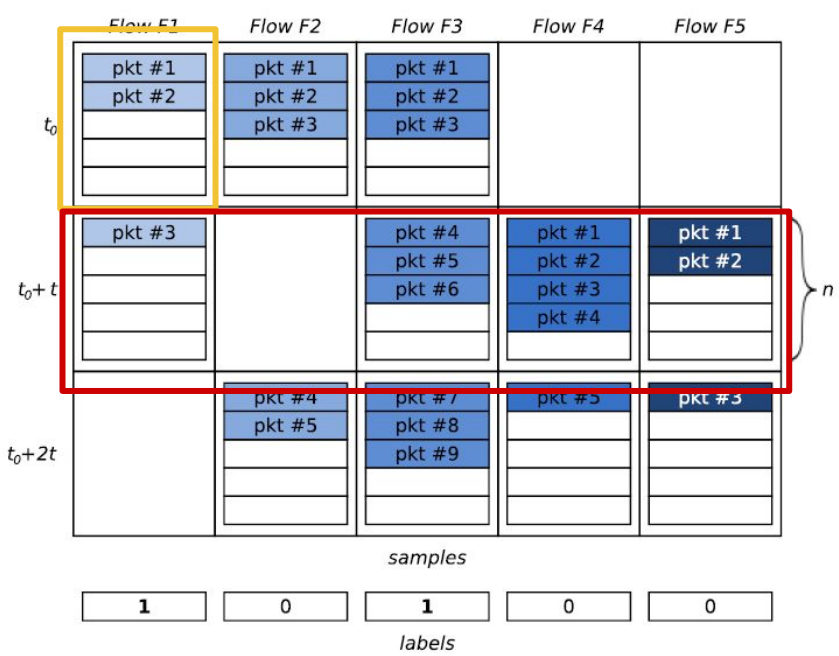
LUCID DETECTION PERFORMANCE ON THE TEST SETS

| Test set | ACC | FPR | PPV | TPR | F1 |
|---|---|---|---|---|---|
| ISCX2012 | 0.9888 | 0.0179 | 0.9827 | 0.9952 | 0.9889 |
| CIC2017 | 0.9967 | 0.0059 | 0.9939 | 0.9994 | 0.9966 |
| CSECIC2018 | 0.9987 | 0.0016 | 0.9984 | 0.9989 | 0.9987 |
| UNB201X | 0.9946 | 0.0087 | 0.9914 | 0.9979 | 0.9946 |

- LSTM ??
  - Be very difficult to train
  - Performance is inherently slower for long sequences
- data preprocessing method combined with the CNN removes the requirement to maintain temporal each whole flow.

# State-of-the-Art Comparison

- **DeepDefense** (dataset: ISCX2012)




**LUCID**

**DeepDefense**

# State-of-the-Art Comparison (cont.)

- DeepDefense - **3LSTM** (the highest score)
  - 6 LSTM layers of 64 neurons each, 2 fully connected layers of 128 neurons each, and 4 batch normalization layers

- The same architecture trains on UNB201X

| Model | Trainable Parameters | ISCX 2012 | CIC 2017 | CSECIC 2018 | UNB 201X |
|---|---|---|---|---|---|
| LUCID | 2241 | 0.9889 | 0.9966 | 0.9987 | 0.9946 |
| 3LSTM | 1004889 | 0.9880 | 0.9968 | 0.9987 | 0.9943 |

→ 3LSTM is more than 40 times slower.
LUCID is much lower computational compexity.

# State-of-the-Art Comparison (con't)

PERFORMANCE COMPARISON WITH STATE-OF-THE-ART APPROACHES USING THE ISCX2012 DATASET FOR DDOS DETECTION

| Model | ACC | FPR | PPV | TPR | F1 |
|---|---|---|---|---|---|
| LUCID | 0.9888 | 0.0179 | 0.9827 | 0.9952 | 0.9889 |
| DeepDefense 3LSTM [4] | 0.9841 | N/A | 0.9834 | 0.9847 | 0.9840 |
| TR-IDS [36] | 0.9809 | 0.0040 | N/A | 0.9593 | N/A |
| E3ML [47] | N/A | N/A | N/A | 0.9474 | N/A |

- TR-IDS is an IDS which adopts a text-CNN to extract features from the payload of the network traffic.
- E3ML uses 20 entropy-based traffic features and three ML classifiers

# State-of-the-Art Comparison (con't)

PERFORMANCE COMPARISON WITH STATE-OF-THE-ART APPROACHES USING THE CIC2017 DATASET FOR DDOS DETECTION

| Model | ACC | FPR | PPV | TPR | F1 |
|---|---|---|---|---|---|
| LUCID | 0.9967 | 0.0059 | 0.9939 | 0.9994 | 0.9966 |
| DeepGFL [35] | N/A | N/A | 0.7567 | 0.3024 | 0.4321 |
| MLP [38] | 0.8634 | N/A | 0.8847 | 0.8625 | 0.8735 |
| 1D-CNN [38] | 0.9514 | N/A | 0.9814 | 0.9017 | 0.9399 |
| LSTM [38] | 0.9624 | N/A | 0.9844 | 0.8989 | 0.8959 |
| 1D-CNN + LSTM [38] | 0.9716 | N/A | 0.9741 | 0.9910 | 0.9825 |

- DeepGFL is a framework designed to extract high order traffic features from low-order features forming a hierarchical graph representation.
- [38] propose four different DL models for DDoS attack detection in Internet of Things (IoT) networks.

# Analysis

- Kernel activations

RANKING OF THE TOTAL COLUMN-WISE FEATURE KERNEL ACTIVATIONS FOR THE UNB201X DATASET

| Feature | Total Kernel Activation | Feature | Total Kernel Activation |
|---|---|---|---|
| Highest Layer | 0.69540 | Time | 0.11108 |
| IP Flags | 0.30337 | TCP Win Size | 0.09596 |
| TCP Flags | 0.19693 | TCP Ack | 0.00061 |
| TCP Len | 0.16874 | UDP Len | 0.00000 |
| Protocols | 0.14897 | ICMP Type | 0.00000 |
| Pkt Len | 0.14392 | | |

- Highest Layer: highest layer links to the type of DDoS attack, e.g.network, transport, or application layer attack.
- IP Flags (16 bits): *flags Reserved Bit, Don't Fragment, More Fragments, and Fragment offset value*

"*Don't Fragment*" set to 1
DDoS 99%
Benign 92%

# USE-CASE: DDOS DETECTION AT THE EDGE

- In contrast to cloud high performance servers, edge nodes cannot exploit sophisticated solutions against DDoS attacks, due to their limited computing and memory resources.

**Testing**

- GPU/CPU
- 1 GB RAM
- Training time

TRAINING CONVERGENCE TIME

| Setup | Time/epoch (sec) | Convergence time (sec) |
|---|---|---|
| LUCID Server | 10.2 | 1880 |
| LUCID Dev. board (GPU) | 25.8 | 4500 |
| LUCID Dev. board (CPU) | 40.5 | 7450 |
| 3LSTM Dev. board (GPU) | 1070 | >90000 |

## INTRODUCTION

Here you could describe the topic of the section

01

## PRESENTATION

Here you could describe the topic of the section

02

## ANALYSIS

Here you could describe the topic of the section

03

## CONCLUSION

Here you could describe the topic of the section

04

“This is a quote. Words full of wisdom that someone important said and can make the reader get inspired.”

**—SOMEONE FAMOUS**

# WHOA!

Here you could give a brief description of the topic you want to talk about. For example, if you want to talk about Mercury, you could say that it's the closest planet to the Sun and the smallest one in our Solar System

# THE SLIDE TITLE GOES HERE!

Do you know what helps you make your point clear? Lists like this one:

- They’re simple
- You can organize your ideas clearly
- You’ll never forget to buy milk!

And the most important thing: the audience won’t miss the point of your presentation

# 01

# NAME OF THE SECTION

You could enter a subtitle here if you need it

# MAYBE YOU NEED TO DIVIDE THE TEXT

## MERCURY

Mercury is the closest planet to the Sun and the smallest one in our Solar System—it's only a bit larger than our Moon

## VENUS

Venus has a beautiful name and is the second planet from the Sun. It's terribly hot—even hotter than Mercury

# YOU COULD USE THREE COLUMNS, WHY NOT?

Mercury is the closest planet to the Sun and the smallest one in our Solar System

Venus has a beautiful name and is the second planet from the Sun

Despite being red, Mars is actually a cold place. It's full of iron oxide dust

# A PICTURE ALWAYS REINFORCES THE CONCEPT

If you want to replace this picture in Google Slides, select it, right-click and choose Replace image > Upload from computer. Open the file that you want and then adjust it if needed. In PowerPoint, select the picture, right-click and choose Change Picture. Open the file and adjust it

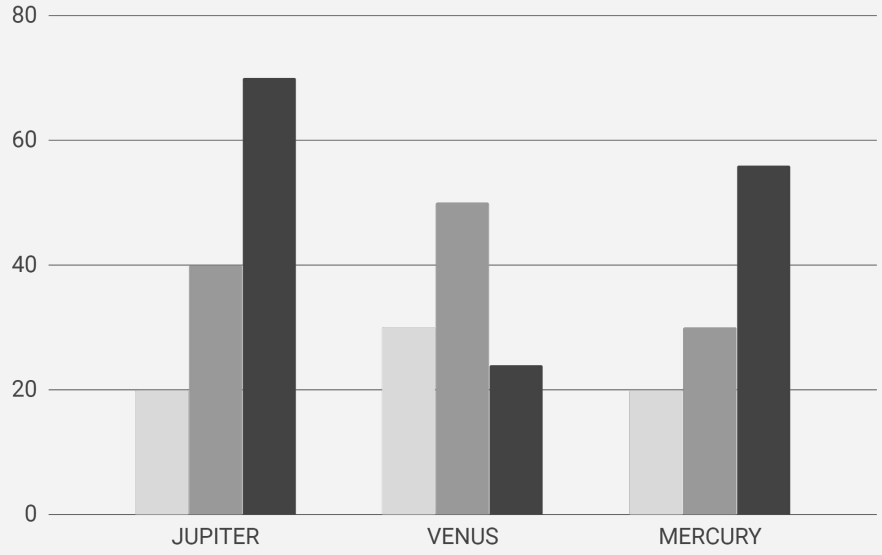
# 02

# NAME OF THE SECTION

You could enter a subtitle here if you need it

# A PICTURE IS WORTH A THOUSAND WORDS

# IF YOU WANT TO MODIFY THIS GRAPH, CLICK ON IT, FOLLOW THE LINK, CHANGE THE DATA AND REPLACE IT




**JUPITER** is a gas giant and the biggest planet in our Solar System

**VENUS** has a beautiful name and is the second planet from the Sun

**MERCURY** is the smallest planet in our Solar System

# A TIMELINE ALWAYS WORKS WELL

01

Mercury is the closest planet to the Sun and the smallest one in our Solar System

Venus has a beautiful name and is the second planet from the Sun. It's terribly hot

02

# A TIMELINE ALWAYS WORKS WELL

Saturn is the ringed planet. It's a gas giant composed mostly of hydrogen and helium

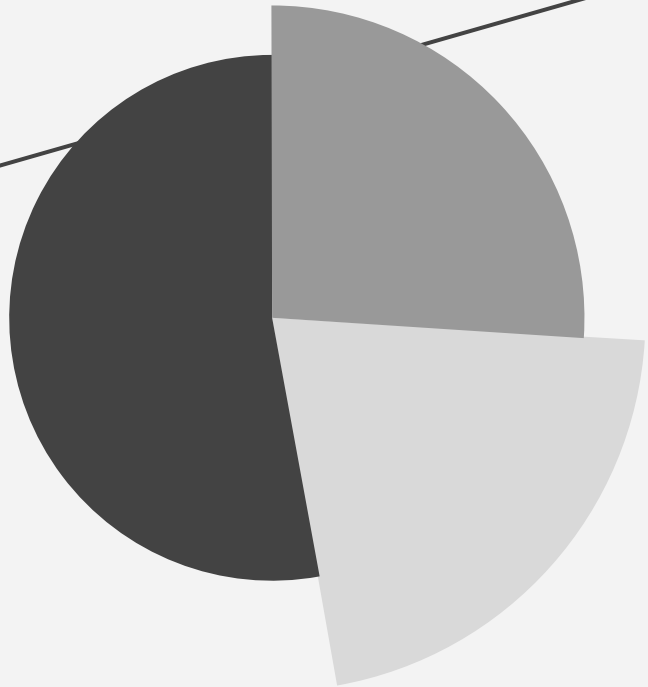
**03**

**04**

Neptune is the farthest planet from the Sun and the fourth-largest by diameter in our Solar System

# AWESOME WORDS

# THIS IS A GRAPH



Mercury is the closest planet to the Sun and the smallest one in our Solar System

Venus has a beautiful name and is the second planet from the Sun

Despite being red, Mars is actually a cold place. It’s full of iron oxide dust

# ... AND THE SAME GOES FOR TABLES

| | 2010 | 2015 | 2020 |
|---|---|---|---|
| MERCURY | 3,000,000 | 4,000,000 | 5,000,000 |
| VENUS | 1,500,000 | 2,000,000 | 2,500,000 |

# HOW ABOUT THESE PERCENTAGES?

**45%**

Neptune is the farthest planet from the Sun

**22%**

Mercury is the closest planet to the Sun

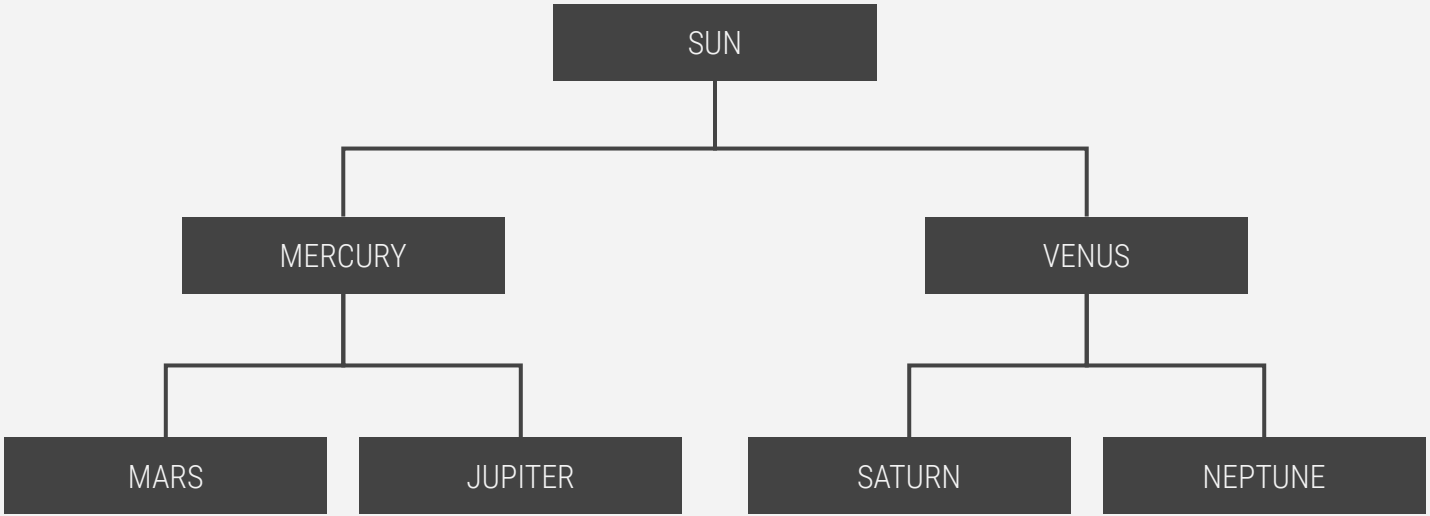
**33%**

Despite being red, Mars is actually a cold place

# 44,000,000

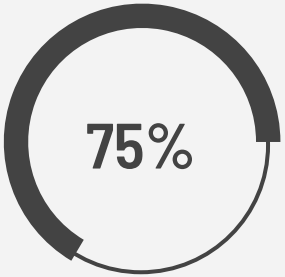
Mercury is the closest planet to the Sun and the smallest of them all

# DON’T FORGET WHAT’S IMPORTANT



# DO YOU PREFER THESE OTHER PERCENTAGES?

Venus has a beautiful name

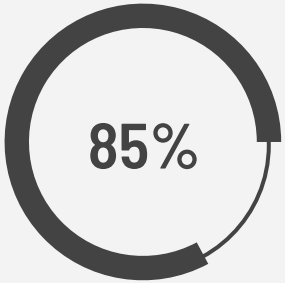



2010

Neptune is the farthest planet from the Sun


2015

Mercury is the closest planet to the Sun




2020

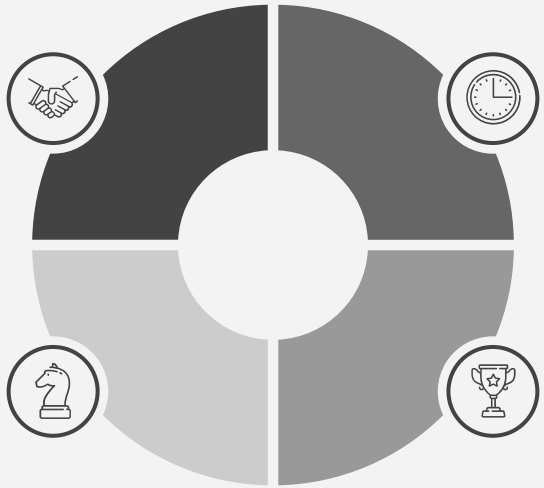
# REINFORCE THE CONCEPTS USING INFOGRAPHICS!

## MARS

Despite being red, Mars is actually a cold place

## JUPITER

It's a gas giant and the biggest planet in our Solar System



## VENUS

Venus has a beautiful name and is the second planet

## MERCURY

Mercury is the smallest planet in our Solar System

# SOMETIMES, REVIEWING CONCEPTS IS A GOOD IDEA

## 01

Despite being red, Mars is actually a cold place

## 02

Mercury is the smallest planet in our Solar System

## 03

Saturn is a gas giant, composed mostly of hydrogen and helium

## 04

Venus has a beautiful name, but it's very hot

## 05

Neptune is the farthest planet from the Sun

## 06

Jupiter is the biggest planet in our Solar System

# OUR SERVICES

## $0

You can explain your product or your service

Characteristic
Characteristic

**FREE**

## $35

You can explain your product or your service

Characteristic
Characteristic

**PREMIUM**

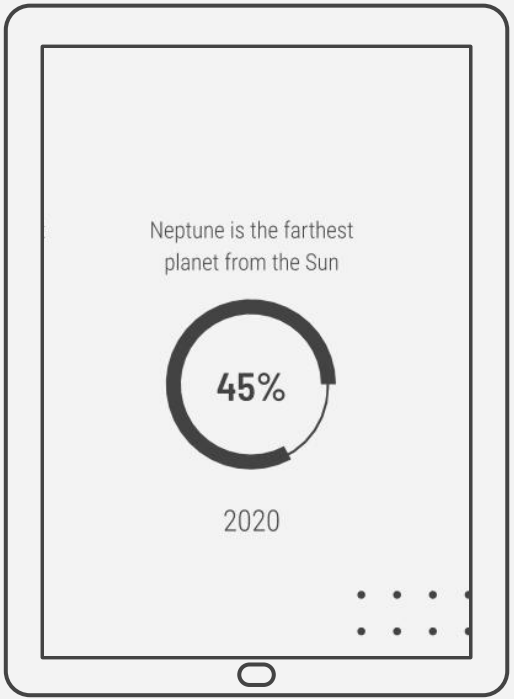
# 03

# NAME OF THE SECTION

You could enter a subtitle here if you need it

# TABLET APP

You can replace the image on the screen with your own work. Just delete this one, add yours and send it to the back

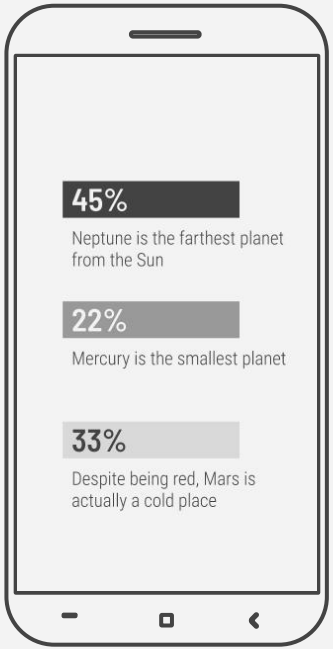



# DESKTOP SOFTWARE

You can replace the image on the screen with your own work. Just delete this one, add yours and send it to the back

# MOBILE WEB

You can replace the image on the screen with your own work. Just delete this one, add yours and send it to the back



# OUR TEAM

## SAMMY PATTERSON, 40

You can replace the image on the screen with your own

## JENNA DOE, 32

You can replace the image on the screen with your own

# THANKS!

Do you have any questions?

youremail@freepik.com
+91  620 421 838
yourcompany.com

# ALTERNATIVE RESOURCES

**PHOTOS**

- High angle view of player throwing basketball in the hoop
- Group of people holding their hands up
- Girl catching a ball helped by her team mates
- Young businessman holding coffee cup in hand looking at buildings in the city
- Group of young businesspeople analyzing graph over wooden desk

# RESOURCES

**PHOTOS**

- City skyline and bridge with us flag
- Crop female keeping baseball and glove
- Brooklyn bridge and skyscrapers on skyline
- Front view women working together
- Rear view of a young man practicing basketball

# Instructions for use

In order to use this template, you must credit **Slidesgo** by keeping the **Thanks** slide.

**You are allowed to:**

- Modify this template.
- Use it for both personal and commercial projects.

**You are not allowed to:**

- Sublicense, sell or rent any of Slidesgo Content (or a modified version of Slidesgo Content).
- Distribute Slidesgo Content unless it has been expressly authorized by Slidesgo.
- Include Slidesgo Content in an online or offline database or file.
- Offer Slidesgo templates (or modified versions of Slidesgo templates) for download.
- Acquire the copyright of Slidesgo Content.

For more information about editing slides, please read our FAQs or visit Slidesgo School:

https://slidesgo.com/faqs and https://slidesgo.com/slidesgo-school

# Fonts & colors used

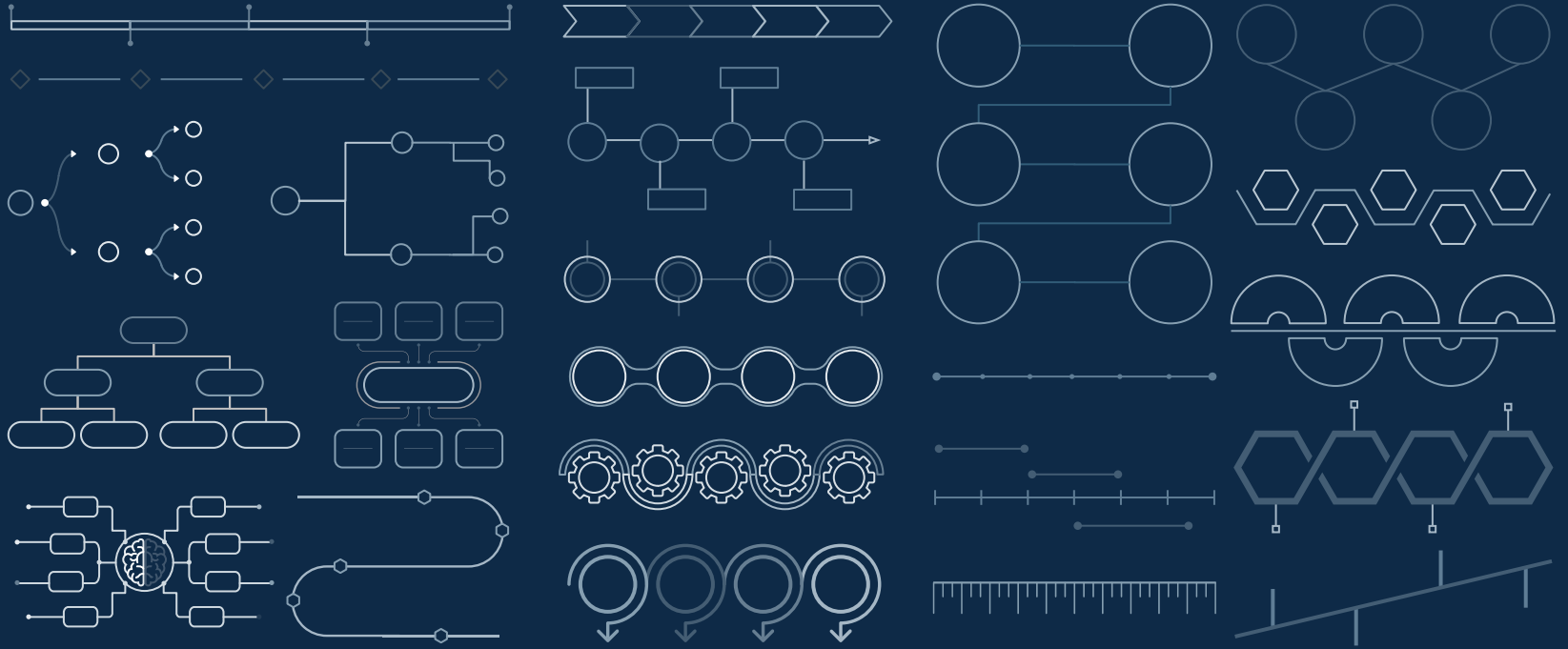
This presentation has been made using the following fonts:

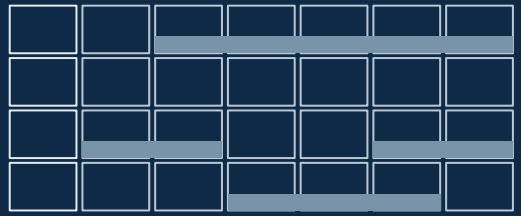
**Barlow Semi Condensed**
(https://fonts.google.com/specimen/Barlow+Semi+Condensed)

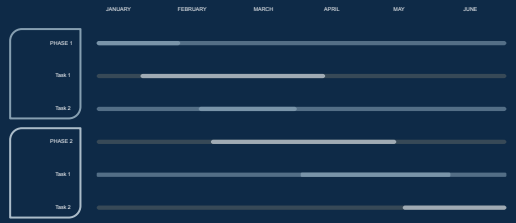
**Roboto Condensed**
(https://fonts.google.com/specimen/Roboto+Condensed)

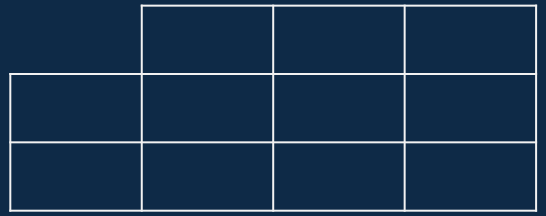
# Use our editable graphic resources...

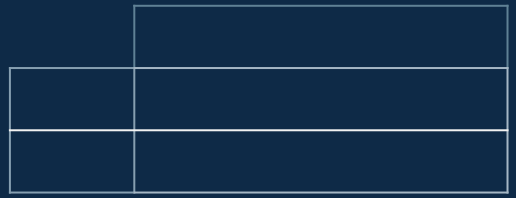
You can easily resize these resources, keeping the quality. To change the color, just ungroup the resource and click on the object you want to change. Then, click on the paint bucket and select the color you want. Don't forget to group the resource again when you're done.

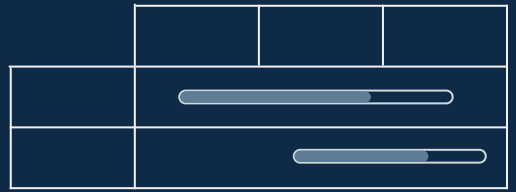


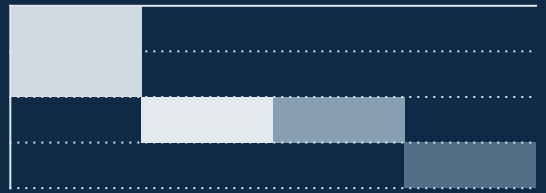


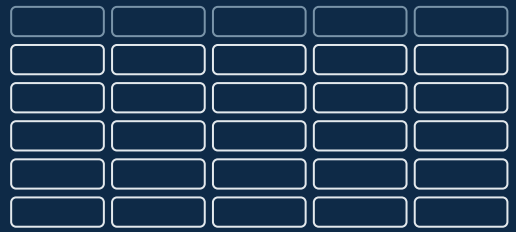

JANUARY
FEBRUARY
MARCH
APRIL
MAY
JUNE
PHASE 1
Task 1
Task 2
PHASE 2
Task 1
Task 2

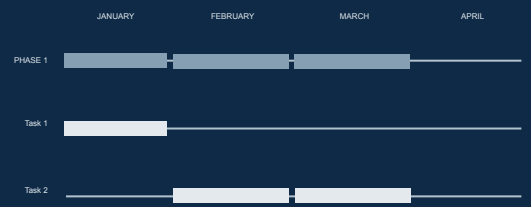


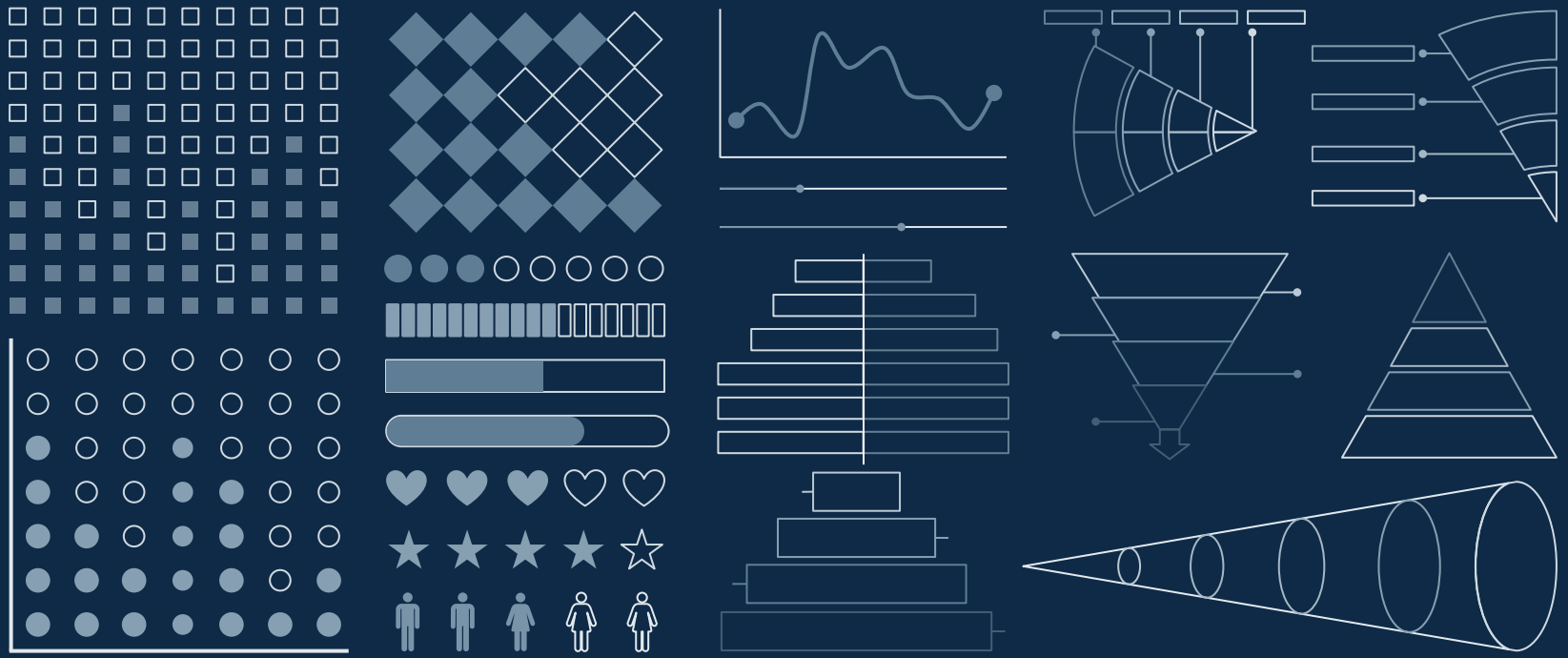









JANUARY
FEBRUARY
MARCH
APRIL
PHASE 1
Task 1
Task 2



# ...and our sets of editable icons

You can resize these icons, keeping the quality.
You can change the stroke and fill color; just select the icon and click on the paint bucket/pen.
In Google Slides, you can also use Flaticon's extension, allowing you to customize and add even more icons.

## Educational Icons

## Medical Icons

## Business Icons

## Teamwork Icons

## Help & Support Icons

## Avatar Icons

## Creative Process Icons

## Performing Arts Icons

# Nature Icons

# SEO & Marketing Icons


slidesgo