Disclaimer

Some elements in this presentation are the result of hard work and valuable suggestions of my co-authors in the research and myself, but in no way it represents them or their work directly.

This research is not related to my current employer and all thoughts are mine.

Although most of the content used in this presentation is hand-drawn doodles and belong to the speaker, but some of them might represent a registered company or product, the speaker does not take any ownership of such graphic, and they belong to their respective registered owners.

All the information shared in this presentation is for educational purpose.

NICS

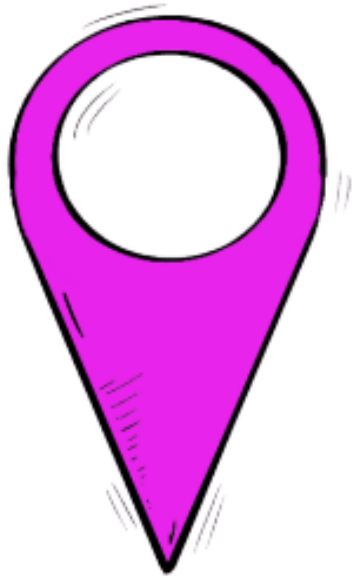
Modified Firefly Optimisation *inspired Intrusion Detection Systems*

~ Saket Upadhyay, et. al.

Our Goal

To understand the basics needed for the topic and get insight into bleeding edge research done by our team to improve existing solutions.

Who this is for?

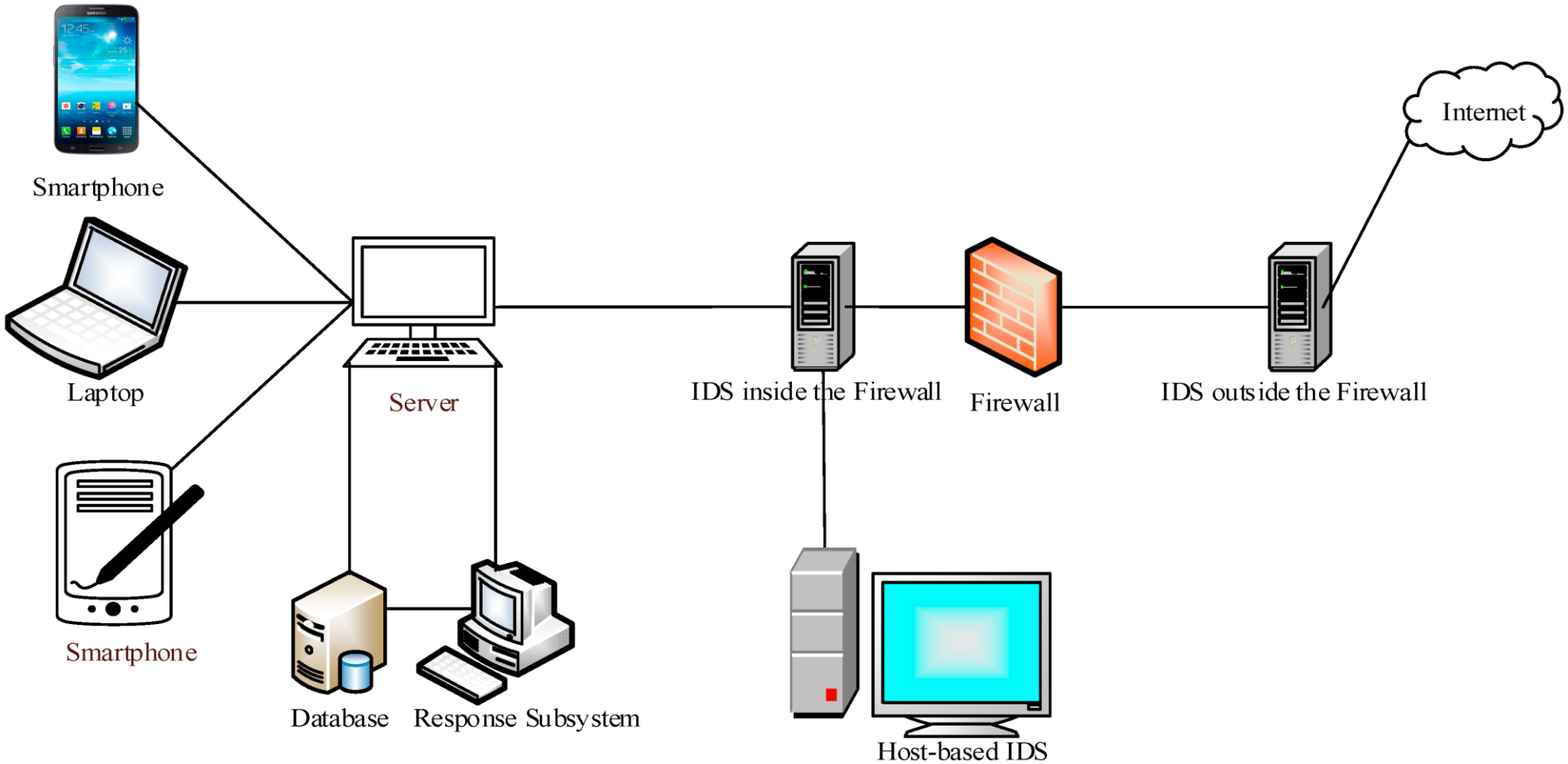


- High School and Senior School (Class 10th to 12th) students who want to know more about academic research in cybersecurity.
- Undergrads and Postgrads who are interested in cybersecurity research and projects.
- Potential co-researchers who would like to work together in this domain.

What is a IDS?

Where it is in the network and types

Intrusion Detection System



SRC: From Intrusion Detection to an Intrusion Response System: Fundamentals, Requirements and Future Directions https://www.mdpi.com/188434

##mdpialgorithms via @MDPIOpenAccess

IDS Types

Types -

- **Network-based intrusion detection system (NIPS):** monitors the entire network for suspicious traffic by analyzing protocol activity.
- **Network behavior analysis (NBA):** examines network traffic to identify threats that generate unusual traffic flows, such as distributed denial of service (DDoS) attacks, certain forms of malware and policy violations.
- **Host-based intrusion detection system (HIDS):** an installed software package which monitors a single host for suspicious activity by analyzing events occurring within that host.

Fire Fly Optimisation

What and How?

First Proposal

» In **mathematical optimization**, the firefly algorithm is a **metaheuristic** proposed by **Xin-She Yang** in 2008 and inspired by the flashing **behavior of fireflies**.

Algorithm

Begin

1) Objective function: $f(\mathbf{x}), \quad \mathbf{x} = (x_1, x_2, \ldots, x_d)$;
2) Generate an initial population of fireflies $\mathbf{x}_i \quad (i = 1, 2, \ldots, n)$;.
3) Formulate light intensity I so that it is associated with $f(\mathbf{x})$
   (for example, for maximization problems, $I \propto f(\mathbf{x})$ or simply $I = f(\mathbf{x})$;)
4) Define absorption coefficient γ

```
    While (t < MaxGeneration)
        for i = 1 : n (all n fireflies)
            for j = 1 : i (n fireflies)
                if (I_j > I_i),
                    Vary attractiveness with distance r via exp(−γ r);
                    move firefly i towards j;
                    Evaluate new solutions and update light intensity;
                end if
            end for j
        end for i
        Rank fireflies and find the current best;
    end while

    Post-processing the results and visualization;

end
```

Inspiration

Inspired by the unisex attraction and flashing behavior of fireflies. The location of firefly ***i*** at each time iteration is calculated as

$$X_i^{t+1} = X_i^t + \beta^{-\gamma r_{ij}^2}(X_j^t - X_i^t) + \alpha_t \epsilon_t,$$

where **β** is the attractiveness, **γ** is the absorption coefficient, r is the distance between nodes **xi** and **xj** , **αt** is the step size, And ϵ_t is the vector drawn from a Gaussian distribution

Brightness function (Modified)

$$\beta_{new} = (\beta_{init} - \beta_{min})e^{-\gamma r^2} + \beta_{min}.$$

Initially, each node is given a minimum brightness β_{min}, and its brightness is updated given an initial brightness β_{init}

To ensure that the brightness of the nodes does not fall below the predefined minimum value β_{min}. The brightness is significantly affected by the absorption coefficient γ and the Euclidean distance between two fireflies. (Euler's number 'e')

Euclidean Distance of Nodes

$$d(p,q) = \sqrt{(q_1 - p_1)^2 + (q_2 - p_2)^2}$$

OR

$$r = d(p,q) = \sqrt{\sum_{i=1}^{n} (q_i - p_i)^2}$$

where **p** and **q** are two points in the Euclidean **n-space**, and **qi** and **pi** are Euclidean vectors, starting from t

Modified Fire Fly

And IDS integration.

Modified Firefly Optimization Algorithm-based IDS

SHISHIR KUMAR SHANDILYA[1] (Senior Member, IEEE), BONG JUN CHOI[2] (Senior Member, IEEE), AJIT KUMAR[3], SAKET UPADHYAY[4]

[1]Vellore Institute of Technology, VIT Bhopal University, India (e-mail: shishir.sam@gmail.com)
[2]Soongsil University, Seoul, South Korea (e-mail:davidchoi@soongsil.ac.kr)
[3]Soongsil University, Seoul, South Korea (e-mail:ajitkumar.pu@gmail.com)
[4]Vellore Institute of Technology, VIT Bhopal University, India (e-mail: saketupadhya@gmail.com)

Corresponding author: Bong Jun Choi E-mail: davidchoi@soongsil.ac.kr

This research was supported by the MSIT, Korea, under National Research Foundation (NRF) Korea (2019R1C1C1007277), and the ITRC support program (IITP-2020-2020-0-01602) supervised by the IITP.

Our Research

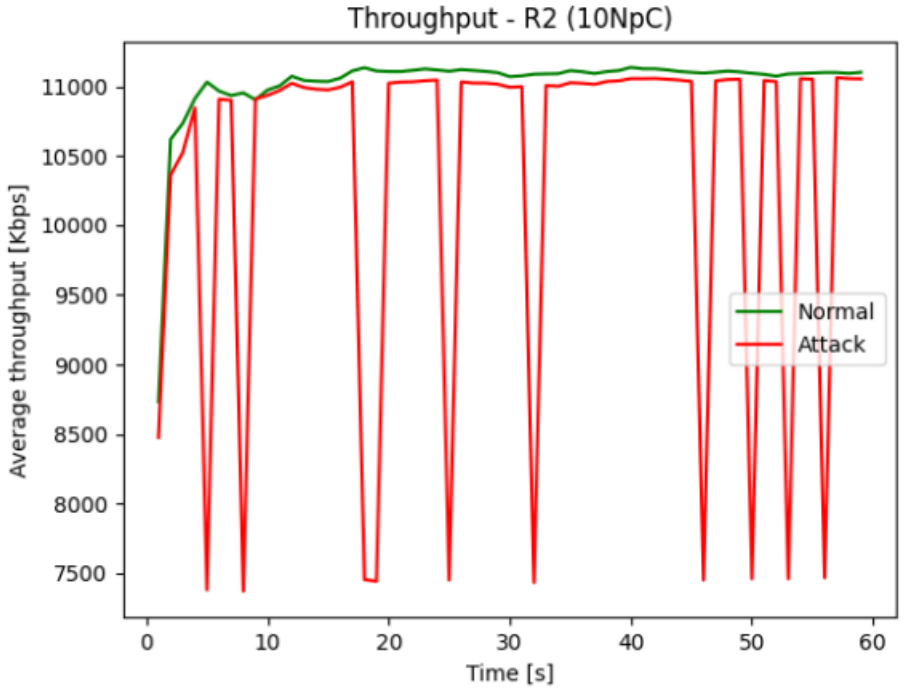
Our new brightness function and node grid implementation

Based on the parameters of network nodes, we define the health function of **node i** at **time t** as

$$hf(i,t) = \frac{(\frac{\sum_{x=0}^{N} NTP_x}{N} - ATP(i,t)) + ETED(i,t)}{PDR(i,t)}$$

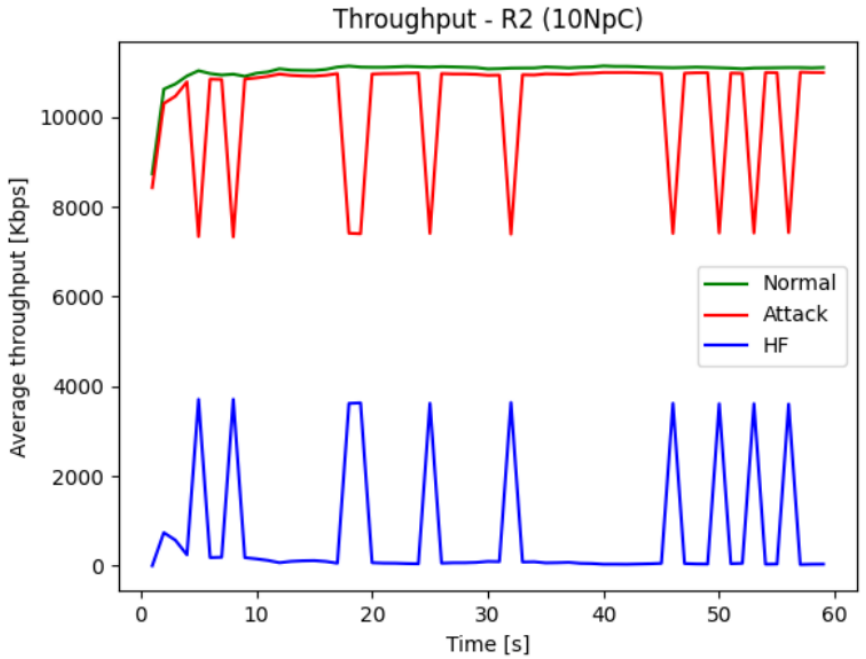
$$\beta \propto hf(i,t).$$

How it works?



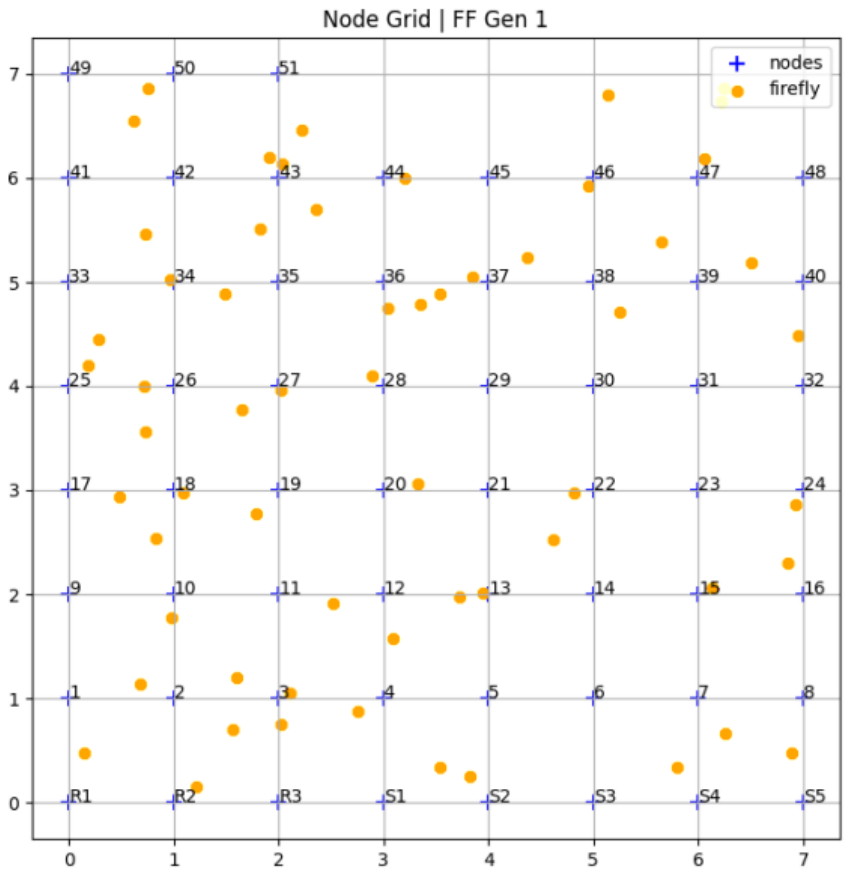
(a) Router 2

$$hf(i,t) =$$

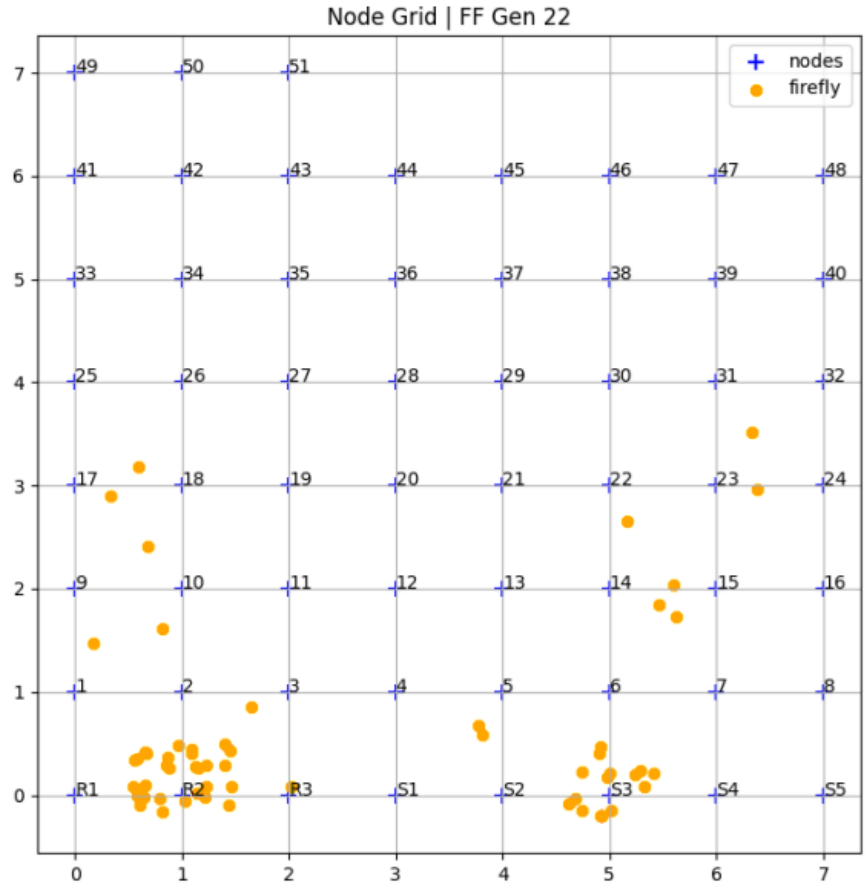


(a) Router 2

How it works?



$$hf(i,t) =$$



Q&A ?

Thank You

- Saket Upadhyay (@ **x64mayhem**)
- saketupadhya@gmail.com
- https://saket-upadhyay.github.io/about