Proposal 2

Instigator: Yezekael Hayel, Avignon University, France

Title: Discrete-event simulation for compartmental stochastic processes on graph

Summary of the proposal

Discrete-event simulations [1] are common programs used to simulate large scale stochastic processes in order to evaluate their performances. The idea of such programs is based on events that occurs at random time, and then the dynamic evolution of complex systems can be studied. Many application domains are based on such approaches like performance evaluation of communication systems, virus propagation, road traffic management, etc.
We propose in this project to build from scratch a discrete-event simulator aiming to simulate compartmental stochastic processes. A well-known compartmental model that can be used as a benchmark is the *Susceptible-Infected* model [2], which is basically used to study epidemics. The simulator has to be reconfigurable such that variants of the SI model can be easily configured. We can cite for example SIR, SEIR and others specific compartmental stochastic models. All these models are based on Markov chain framework with particular transition rates. This is why simulation helps to understand both transient and stationary behavior of such complex system.

References

[1] Pierre-Jean Erard et Pontien Déguénon, *Simulation par événements discrets*, Lausanne/Paris, Presses polytechniques et universitaires romandes,
[2] Brauer F., « Compartmental models for epidemics», Centre for Disease Modelling, Preprint 2008-02, University of York. Consulté le 13 mars 2010.

Proposal 3

Instigators: Abderrahim Benslimane and Julio Perez, Avignon University, France

Title: Automatic identification of malicious activities by monitoring Darknet Network

Summary of the proposal

The Internet has become highly integrated into our current everyday lives. Society has gone digital through communication, socializing, learning and doing business online. Furthermore, in order to improve the quality and efficiency of work, governments are leveraging the Internet to operate their critical infrastructure. While cyberspace provides major benefits, our increasing reliance on it is producing new, significant vulnerabilities. As such, any security breach has the potential to result in debilitating effects on security, economy, public health, or safety. In addition, cyber attacks are dramatically increasing in size and number. Recent online threats demonstrated that organizations and governmental agencies could be subjected, nearly instantaneously and in full anonymity, to large-scale disrupting and orchestrated attacks with the potential to lead to severe security, privacy, and economic consequences (i.e. cyber-terrorism, DDoS (Distributed Denial of Service), DRDoS(Distributed Reflection Denial of Service), information theft, spam and fraud) [1]. Darknet network have been used for years as a source of information for cybersecurity. A darknet is a set of IP addresses advertised by routing protocols, however without hosting any device [2].

In this project we will propose an architecture that allow to collect traffic with the differently located darknet sensors considering parameters such as traffic pattern, protocols, targeted port (destination port) and use the collected data to train different Machine Learning classifiers. This may further help in to understand topological behaviors of darknet traffic and detect possible attacks in the network (i.e. DDoS, Probing activities). In addition, create new datasets could provide some additional important information or reconfirmation of previous findings.

Our goal in this project is to use the traffic collected on the Darknet to train a Machine Learning algorithm to detect possible attacks on the network.

Related Work

Usually darknets receive traffic only for one of three reasons: traffic sent accidentally/by mistake, backscatter, malicious activity of scanning and worms. Accidental Darknet requests can occur if an individual mistyped an IP address or the URL used had an incorrect Domain Name Service (DNS) entry leading to a darknet. To hide identity of sender, DoS attacks are launched using Spoofed IP address. All traffic reaching the darknet remains unanswered and, by definition, is considered unsolicited. A monitoring probe or darknet sensor listens to the darknet traffic, processing it in search for signals of new threats, misconfigurations and possibly sources/victims of attacks [3].

There is a lack for automatic ways to uncover correlations among different events, which could help reducing the manual work when interpreting darknet traffic [4]. A promising approach is to apply Machine Learning (ML) using supervised learning to train a threat detection system using malicious and normal traffic. Some authors have proposed the utilization of Machine learning algorithms to detect DoS and probing attacks [5-7].

Plan

- Study the state of the art in Darknet sensor and comparing the different existing architectures.
- Select adequates Machine Learning algorithms to classify (detect) the different attacks (e.g. DDoS, RDoS, Probing, etc).
- Get familiar with sniffing softwares (i.e. Wireshark) and with pentesting and probing tools (i.e. Kali Linux tools, Ethercap, DDoSIM (DDoS Simulator), nmap, etc).

The three tasks above should be done **before the first day of the internship**.

- Implementation of the darknet sensor and launch different attacks againt a victim computer and collect the traffic.
- Train the machine learning algorithms with the collected traffic and compare the performance using the confusion matrix.
- Final report.

REFERENCES

[1] C. Fachkha and M. Debbabi, “Darknet as a Source of Cyber Intelligence: Survey, Taxonomy, and Characterization,” *IEEE Commun. Surv. Tutorials*, vol. 18, no. 2, pp. 1197–1227, 2016, doi: 10.1109/COMST.2015.2497690.

[2] F. Soro, I. Drago, M. Trevisan, M. Mellia, J. Ceron, and J. J. Santanna, “Are darknets all the same? On darknet visibility for security monitoring,” *IEEE Work. Local Metrop. Area Networks*, vol. 2019-July, 2019, doi: 10.1109/LANMAN.2019.8847113.

[3] P. S. Joshi and H. A. Dinesha, “Survey on identification of malicious activities by monitoring darknet access,” *Proc. 3rd Int. Conf. Smart Syst. Inven. Technol. ICSSIT 2020*, no. Icssit, pp. 346–350, 2020, doi: 10.1109/ICSSIT48917.2020.9214121.

[4] F. Soro, M. Allegretta, M. Mellia, I. Drago, and L. M. Bertholdo, “Sensing the Noise: Uncovering Communities in Darknet Traffic,” *2020 Mediterr. Commun. Comput. Netw. Conf. MedComNet 2020*, 2020, doi: 10.1109/MedComNet49392.2020.9191555.

[5] P. S. Joshi and H. A. Dinesha, “Survey on identification of malicious activities by monitoring darknet access,” *Proc. 3rd Int. Conf. Smart Syst. Inven. Technol. ICSSIT 2020*, no. Icssit, pp. 346–350, 2020, doi: 10.1109/ICSSIT48917.2020.9214121.

[6] Z. Wang, W. Cheng, and C. Li, “DoS attack detection model of smart grid based on machine learning method,” *Proc. 2020 IEEE Int. Conf. Power, Intell. Comput. Syst. ICPICS 2020*, pp. 735–738, 2020, doi: 10.1109/ICPICS50287.2020.9202401.

[7] S. Kumar, H. Vranken, J. Van DIjk, and T. Hamalainen, “Deep in the Dark: A Novel Threat Detection System using Darknet Traffic,” *Proc. - 2019 IEEE Int. Conf. Big Data, Big Data 2019*, pp. 4273–4279, 2019, doi: 10.1109/BigData47090.2019.9006374.

Proposal 1

Instigators: Abderrahim Benslimane and Julio Perez, Avignon University, France

Title: Real time and accurate detection of pedestrians with Unnamed Areal Vehicles

Summary of the proposal

This project is related to objects detection from videos and images taken by mobile Unnamed Areal Vehicles (UAV). UAV is promising technology to be used to monitor crowded and hostile areas at distance without the near presence of humans.

The detection system will be used on images acquired through thermal cameras, to establish a complete Artificial Intelligence (AI) system for people tracking, social distancing classification, and body temperature monitoring.

AI methods are playing more and more a big role in the detection. Deep learning is an effective method to perform object detection [1] – [6]. These algorithms can be divided into two main categories. One type is two-stage methods which divide detection into two parts, region proposal and classification. These methods can achieve high detection accuracy but consume time. Another one refers to single-stage methods which treat detection as an end-to-end process to directly predict the location and categories of targets.
In this project, we intend to use Yolo as a detection system with some improvements.

With UAVs, the project is to implement a lightweight pedestrian detection network to accurately detect pedestrians by human head detection in real time and then calculate the social distancing between pedestrians on UAV images.

References

1. R. Girshick, “Rich feature hierarchies for accurate object detection and semantic segmentation”, IEEE Conference on Computer Vision and Pattern Recognition (CVPR), pp. 580–587, 2015.

2. J. Li, X. Liang, J. Li, Y. Wei, T. Xu, J. Feng, and S. Yan, “Multistage object detection with group recursive learning,” IEEE Transactions on Multimedia, vol. 20, no. 7, pp. 1645–1655, 2017.

3. P. Tang, X. Wang, S. Bai, W. Shen, X. Bai, W. Liu, and A. Yuille, “Pcl: Proposal cluster learning for weakly supervised object detection,” IEEE transactions on pattern analysis and machine intelligence, vol. 42, no. 1, pp. 176–191, 2018.

4. J. Redmon and A. Farhadi, “Yolov3: An incremental improvement,” arXiv preprint arXiv:1804.02767, 2018.

5. J. Redmon and A. Farhadi, “Yolo9000: better, faster, stronger,” in Proceedings of the IEEE conference on computer vision and pattern recognition, 2017, pp. 7263– 7271.

6. J. Redmon, S. Divvala, R. Girshick, and A. Farhadi, “You only look once: Unified, real-time object detection,” in Proceedings of the IEEE conference on computer vision and pattern recognition, 2016, pp. 779–788.

Proposal 5

Instigators: Abderrahim Benslimane and Julio Perez, Avignon University, France

Title: Implementation of a motion detector alarm system: feasibility of transmitting images on Lora

Description:

The need for effective and reliable intrusion detection with an alarm system has become a vital necessity due to the frequent instances of burglary. Attacks on homes, offices, factories, banks, etc. are on the rise. With advances in technology, motion can be detected by measuring the change in velocity or vector of an object in the field of view.

This can be achieved either by mechanical devices that physically interact with the field, or by an electronic device that quantifies and measures changes in the given environment. The goal of this project is to implement a motion detector alarm system. Indeed, this project will be built using two Arduino devices each connected to a motion sensor (PIR sensor). Their role will be to inform the application (which students must create on a server) when a movement is detected, this application can be used to access all the information collected by the final devices.

The application will then have to send an e-mail notifying the destination, the ID of the sensor that receives this information. The final devices must be programmed to receive two different downlink commands, by receiving the first command, they must create a sound using a buzzer and by receiving the second command, the final devices will flash their LED. Finally, an IP camera must start transmitting an image (or a luminous video with a given light encoding) to be transmitted over the network.

Required hardware and software:

Final device: two Arduino's each connected to a motion sensor, a buzzer (or speaker), an LED and a camera.

Gateway: Build a gateway using a Raspberry pi and LoRa concentrator board.

Server: TTN, LoraServer or any other LoRa server.

In order to achieve this goal, the following tasks will need to be completed:

- Perform a theoretical study: LoRa and LoRaWAN (technical overview), motion sensor (operation) etc.
- Make a connection diagram between the two Arduino, the motion sensors and the buzzer.
- Build a gateway using Raspberry pi and a LoRa hub board.
- Study the different server technologies for LORAWAN and create an application on the chosen server.