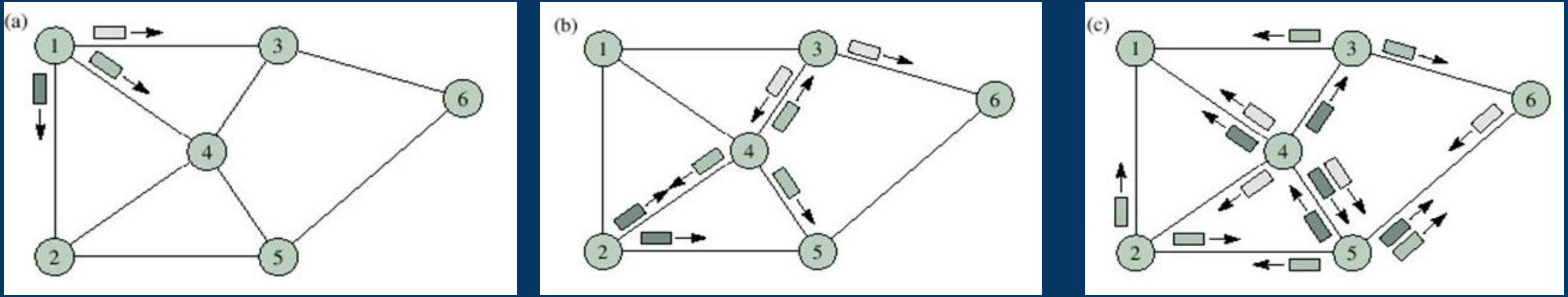
An efficient deep learning model for intrusion classification and prediction in 5G and IoT networks

Guide :
Dr. P. T. Kulkarni

By:
Mugdha Deokar
Mayur Wadekar
Yash Govilkar

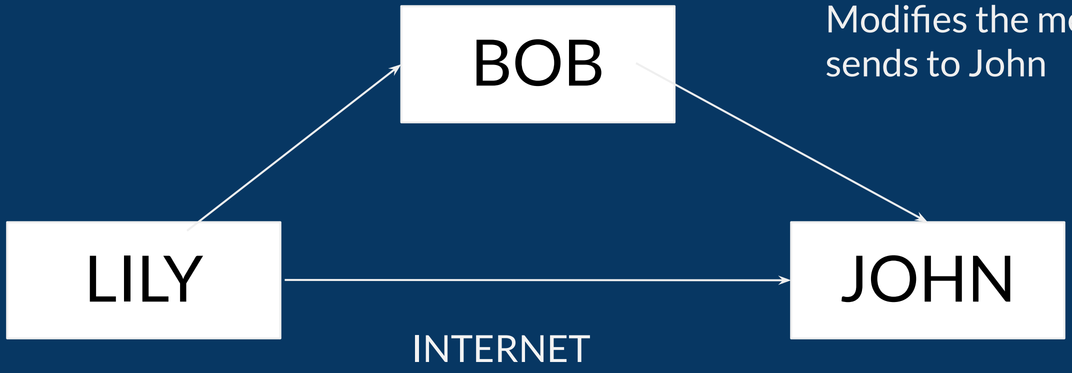
FLOODING

This category of attack is designed to cause an interruption or suspension of services of a specific host/server by flooding it with large quantities of useless traffic or external communication requests.



IMPERSONATION

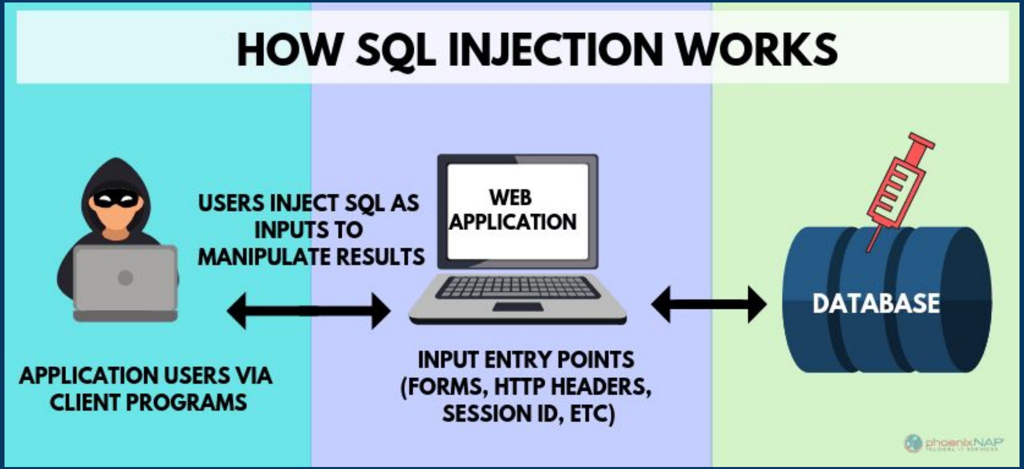
It is the act of pretending to be someone you are not and gaining unauthorized access.



Modifies the message and sends to John

Injection

Attacker uses existing vulnerabilities in the applications to inject a code/string for execution that exceeds the allowed and expected input to the system requested.


HOW SQL INJECTION WORKS
USERS INJECT SQL AS INPUTS TO MANIPULATE RESULTS
WEB APPLICATION
DATABASE
APPLICATION USERS VIA CLIENT PROGRAMS
INPUT ENTRY POINTS (FORMS, HTTP HEADERS, SESSION ID, ETC)
phoenixNAP

Workflow

- AWID Dataset (Real traces of normal and intrusive 802.11 WLAN)
  http://icsdweb.aegean.gr/awid/features.html
- Data Preprocessing
- Unsupervised pre-training with Autoencoder
- Supervised classification with Dense neural network
- Speeding up the training phase

Network Intrusion Detection Systems

- Classifier that differentiates unauthorized or anomalous traffic from authorized or normal traffic.

- NIDS are set up at a planned point within the network to examine the traffic from all devices on the network. Alert sent if attack is detected.

  Eg. Installing it on subnet where firewalls are located in order to see if someone is trying to crack the firewall.

Autoencoder

- A type of ANN used to learn efficient data representation in an unsupervised manner.

- It is a neural network consisting of three layers:
  Input layer, hidden (encoding) layer and decoding layer.

- The network is trained to reconstruct its input, which forces the hidden layer to try to learn better representation of input.

- It is a data compression algorithm.

Implementation

- Implementation using Python Keras library with Tensorflow backend.
- The autoencoder will facilitate an unsupervised pre-training on the data to provide compressed and less noisy representation of the input space.
- The final dense neural network will function as the supervised classifier of the attack types for the experimental intrusion detection scenario.

Neural Network Representation

- Layers are fully connected by neurons in a network layer.
- Each neuron in the layer receives an input from all the neurons present in the previous layer.

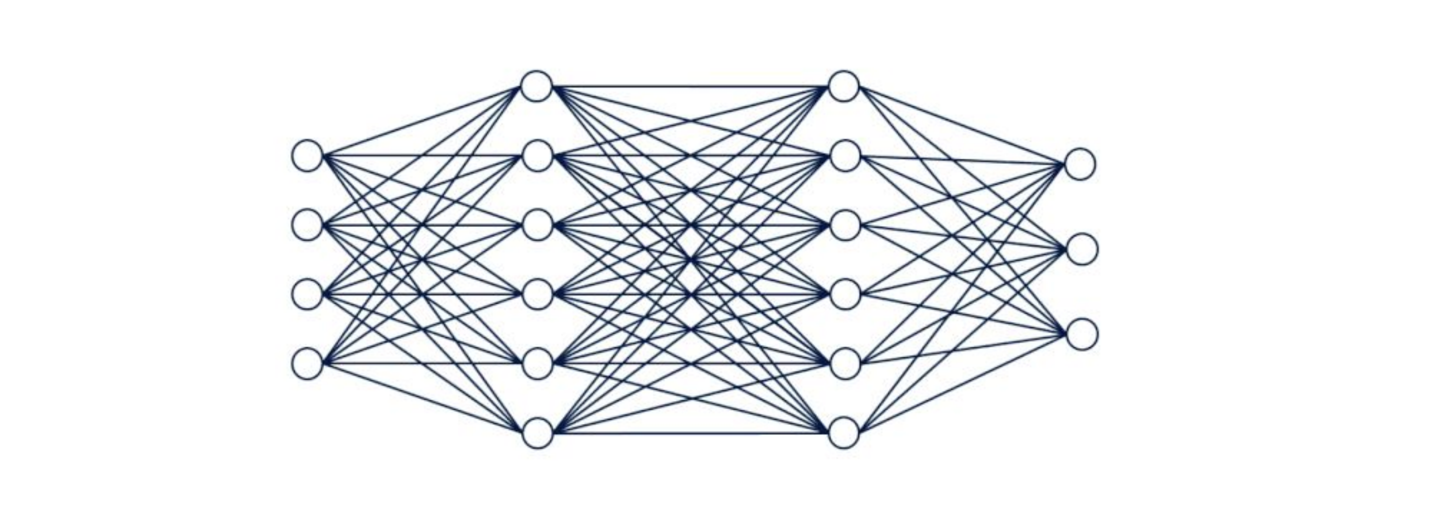
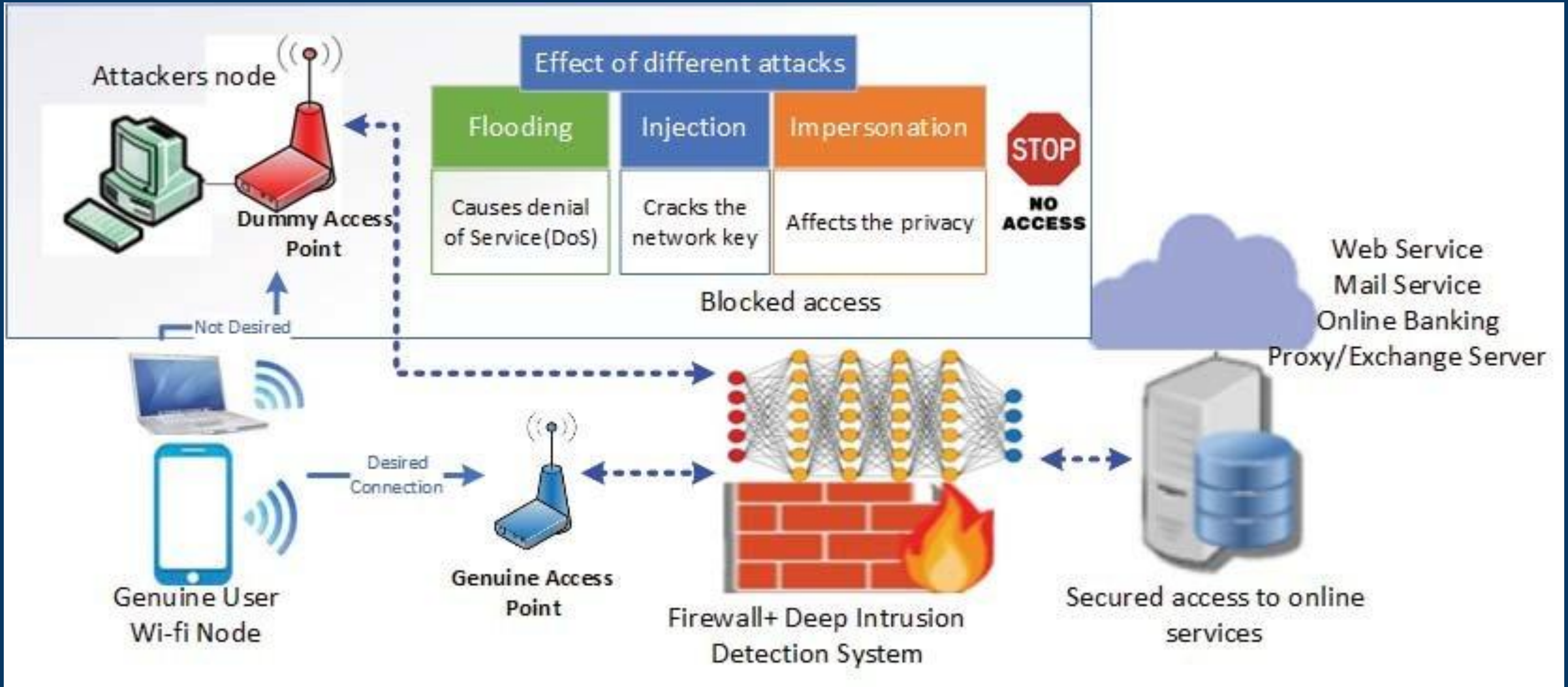


Illustration of the proposed Network Intrusion Detection System



Effect of different attacks

Flooding	Injection	Impersonation
Causes denial of Service(DoS)	Cracks the network key	Affects the privacy

Blocked access

Proposed Model

- The current model classifies three attacks. We propose to detect larger attack types and implement model that can be processed on mobile devices using the algorithm computationally less intensive by using tensorflow lite.

- Simulate a real time network using existing softwares available i.e. QualNet and train and test the model.

References

- S. Rezvy, Y. Luo, et al., “An efficient deep learning model for intrusion classification and prediction in 5G and IoT networks,” 2019 53rd Annual Conference on Information Sciences and Systems (CISS) https://ieeexplore.ieee.org/document/8693059

- Awid dataset - wireless security datasets project, 2014. [Online]. Available: http://icsdweb.aegean.gr/ awid/.