Intrusion Detection Systems

Objectives

- Intrusion Detection Systems (IDSs)
- Intrusion detection systems terminology
- Intrusion Detection System (IDS) vs Intrusion Prevention System (IPS)
- Classification of intrusion detection systems
  - By scope
  - By mode of operation
- Goals for intrusion detection systems
- Intrusion detection systems responses
- IDS performance

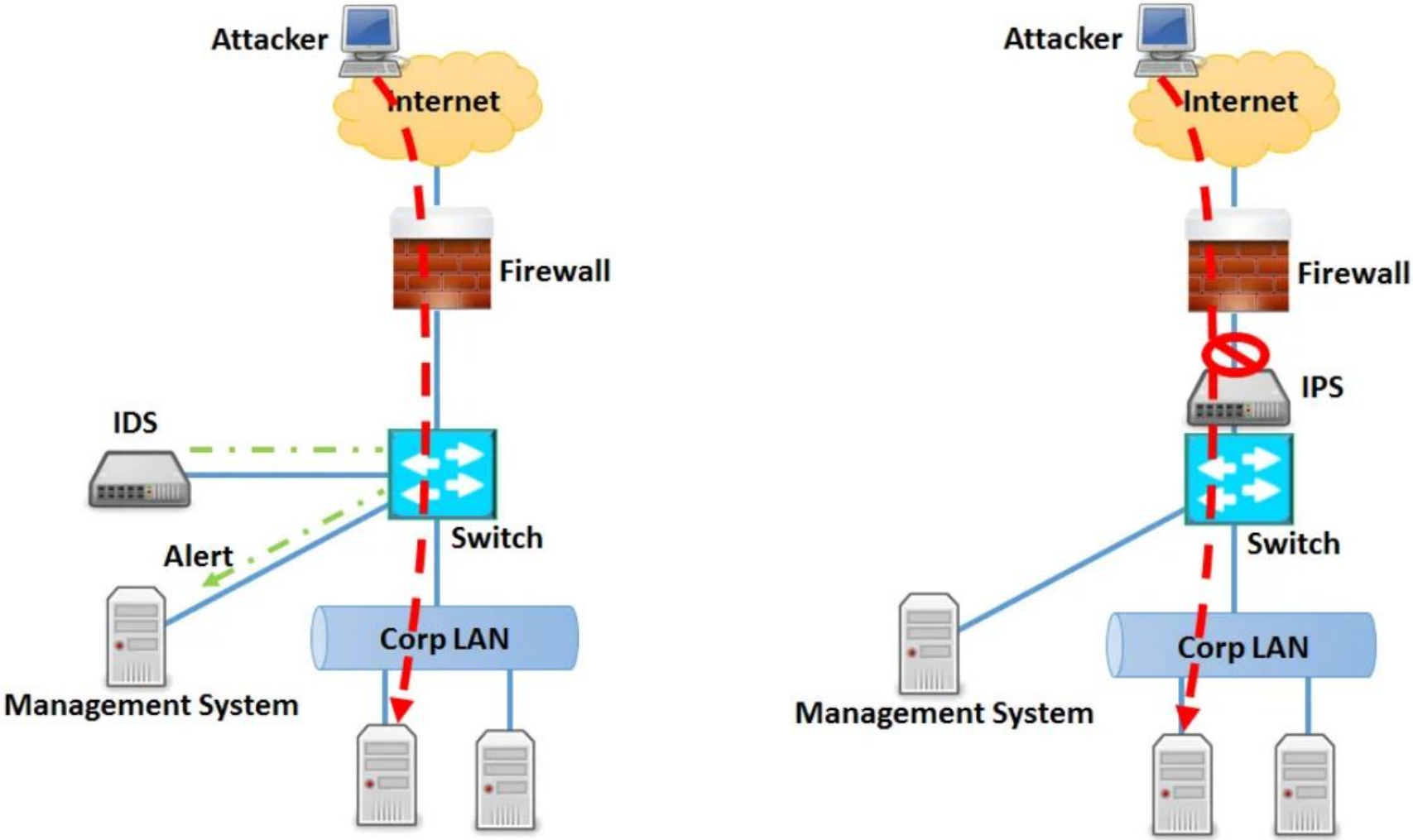
Intrusion Detection Systems

- An Intrusion Detection System (IDS) is a device that monitors system activities with a view towards detecting malicious or suspicious events
  - Intrusion detection systems attempt to detect:
    - Outsiders breaking into a system
    - Insiders attempting to perform inappropriate actions

Intrusion Detection Systems Terminology

- Common terms associated with the use of intrusion detection systems:
  - Anomaly
  - Misuse
  - Intrusion
  - Audit
  - Profiling

Intrusion Detection System (IDS) vs Intrusion Prevention System (IPS)



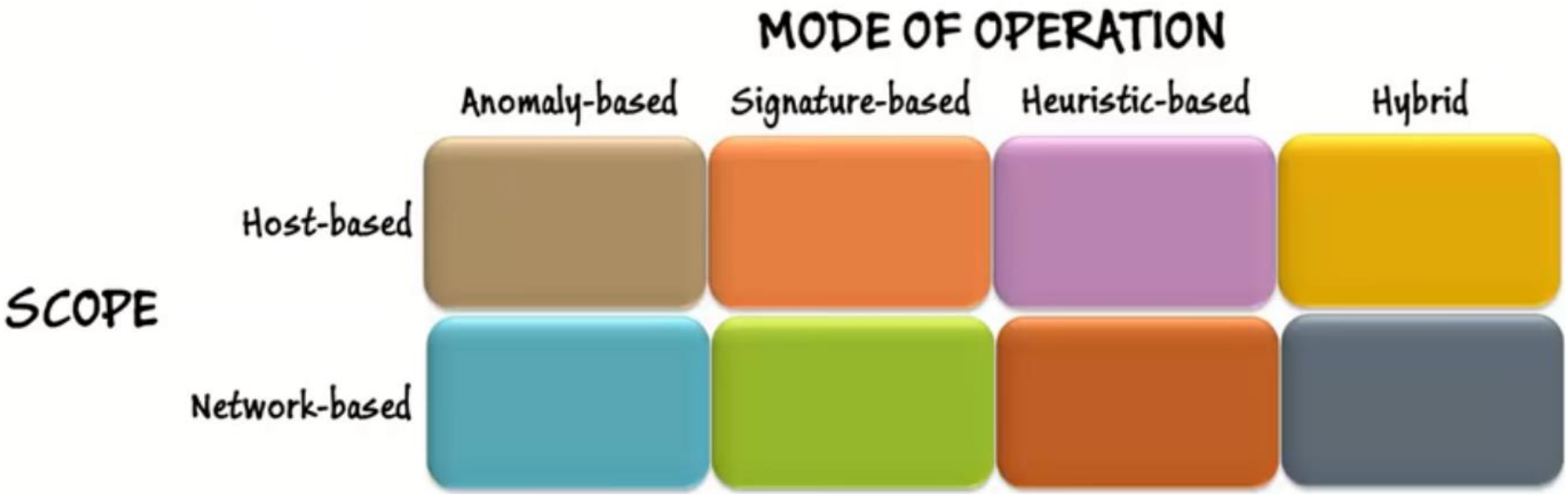
Source: https://ipwithease.com/difference-between-ips-and-ids-in-network-security/

Intrusion Detection Systems Classification

- Intrusion detection systems can be classified by scope:
  - Host-based
    - IDS runs on a host
    - IDS monitors activities on this host only
  - Network-based
    - The IDS is a stand-alone device
    - The IDS monitors the entire network or sub-network

- Intrusion detection systems can also be classified by their mode of operation:
  - Anomaly-based
    - IDS allows only permitted behavior
    - Uses models of acceptable user activities
  - Signature-based
    - The IDS looks for known attacks
    - To detect an attack, current activities are matched to known attacks signatures
  - Heuristic-based
    - The IDS automatically constructs a model of “normal” system behaviour
    - Current activities are compared what is considered normal in order to identify unacceptable system activities
  - Hybrid
    - IDS is a combination of anomaly, signature and/or Heuristic-based approaches

Intrusion Detection Systems Classification



Goals for Intrusion Detection Systems

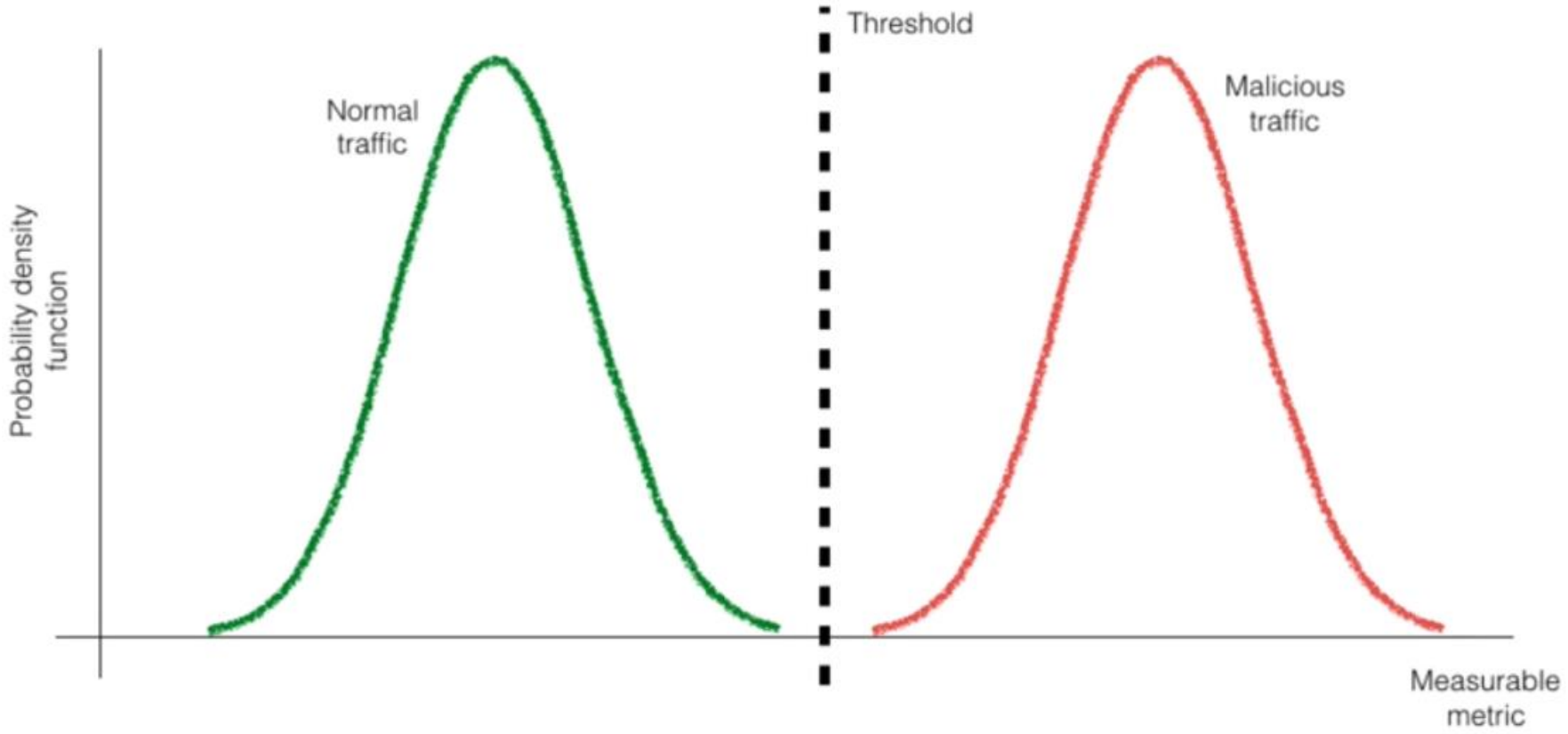
- Detect all attacks correctly
  - Avoid false positives
  - Avoid false negatives
- Monitor systems effectively with minimum overhead and performance degradation

Intrusion Detection Systems Responses

- Monitor the attack and collect data
- Protect systems and reduce exposure
- Alert a human

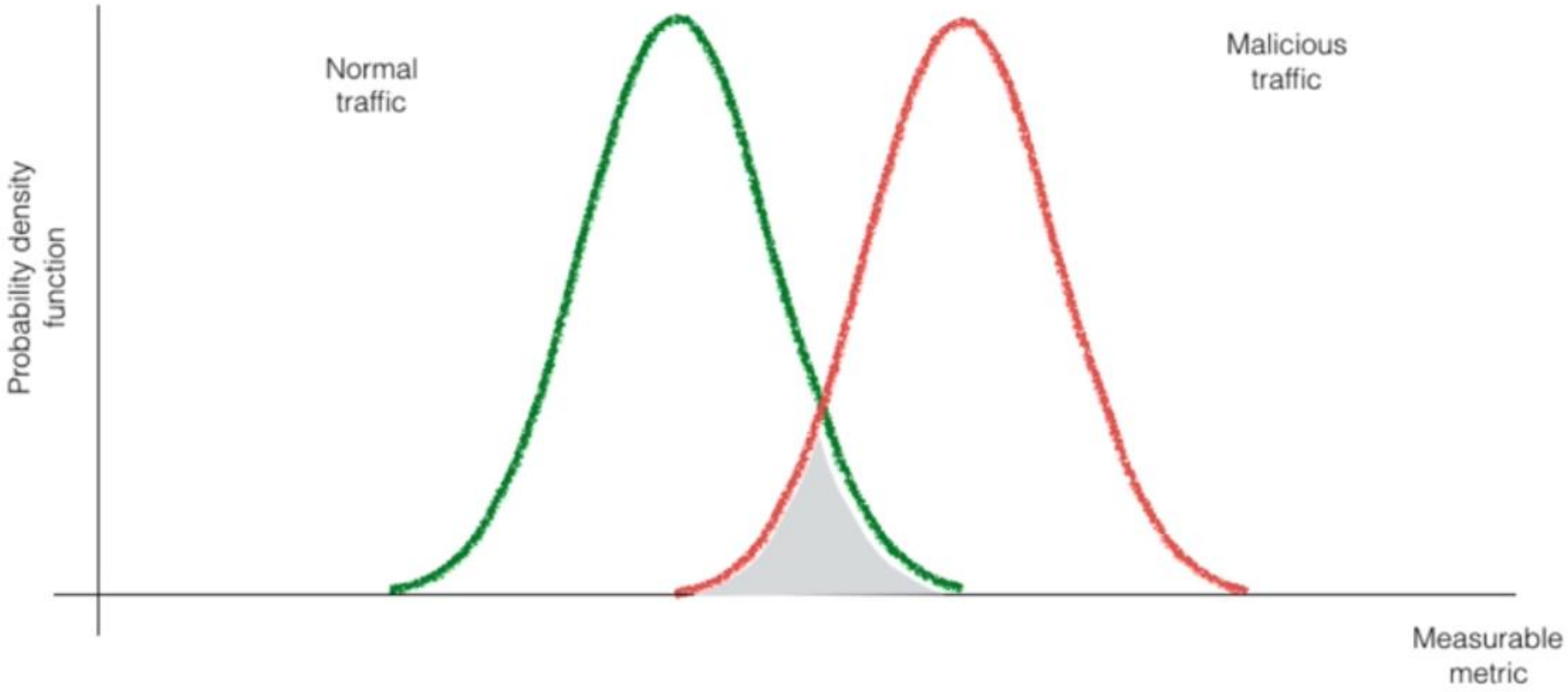
IDS Performance

- Traffic distinction

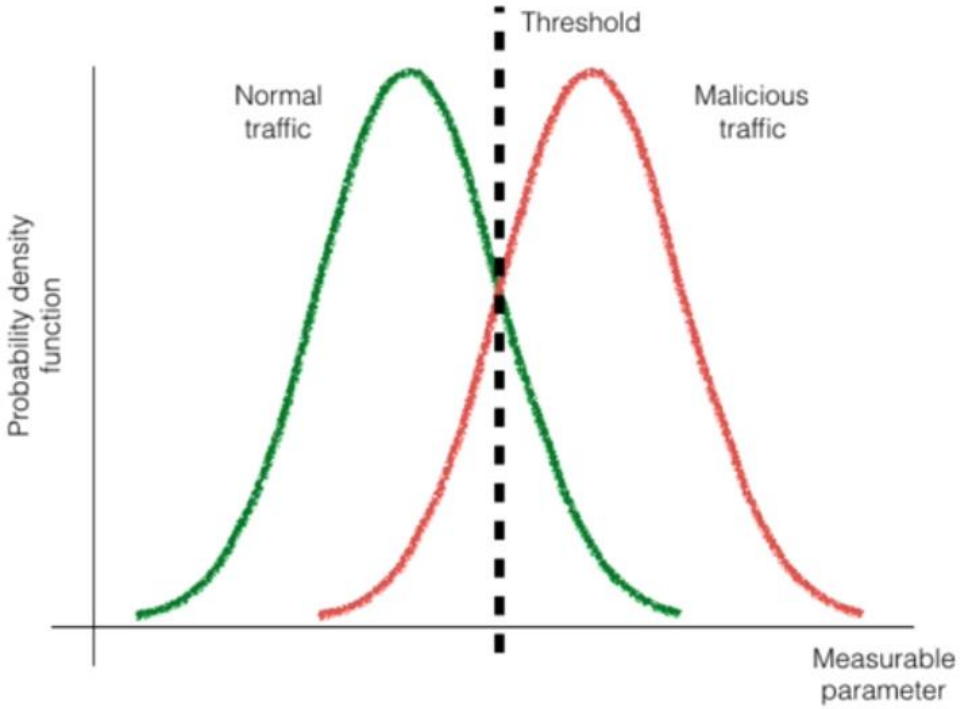


IDS Performance

- Traffic distinction

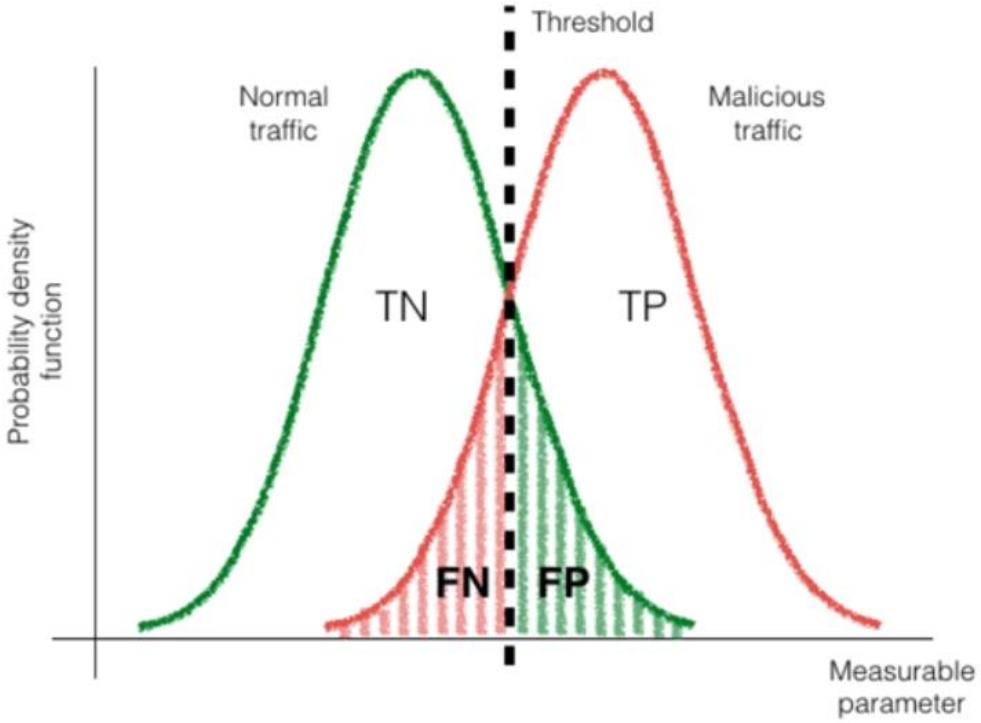


IDS Performance



Ground truth	IDS output: Positive	IDS output: Negative
Malicious		
Benign		

IDS Performance



IDS output

Ground truth	Positive	Negative
Malicious	True Positive (TP)	False Negative (FN)
Benign	False Positive (FP)	True Negative (TN)

Confusion matrix

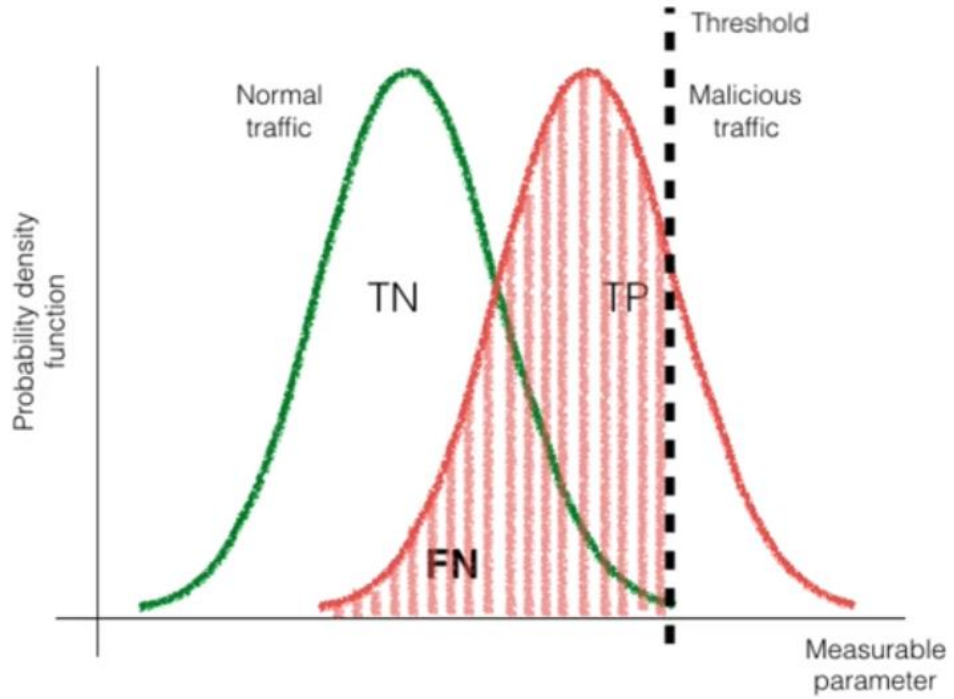
IDS Performance

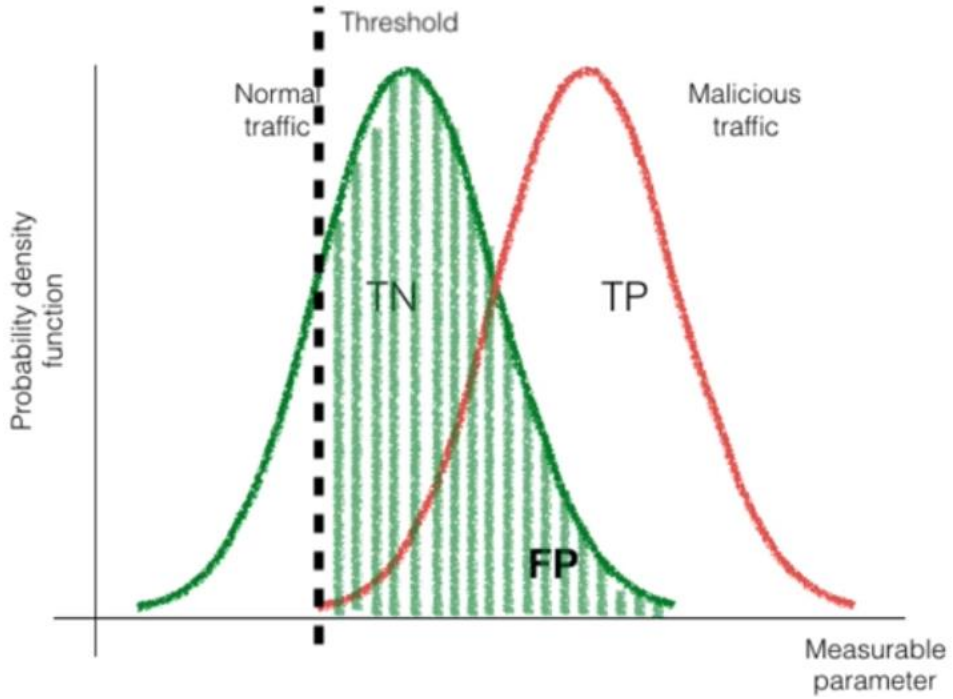
- **Confusion matrix:**
  - quantifies the performance of an IDS
  - allows to compare different IDSs

- **Underlying goal:** keep FP and FN as low as possible

IDS Tuning

- **parameters** will need to be adjusted to a specific network
- **error rates** can be controlled by tuning the parameters





IDS Tuning

- **parameters** will need to be adjusted to a specific network
- **error rates** can be controlled by tuning the parameters

- error rates are **interleaved measures**
- the **acceptable rates** of false positives and false negatives depend on the level of security we wish to implement in a network

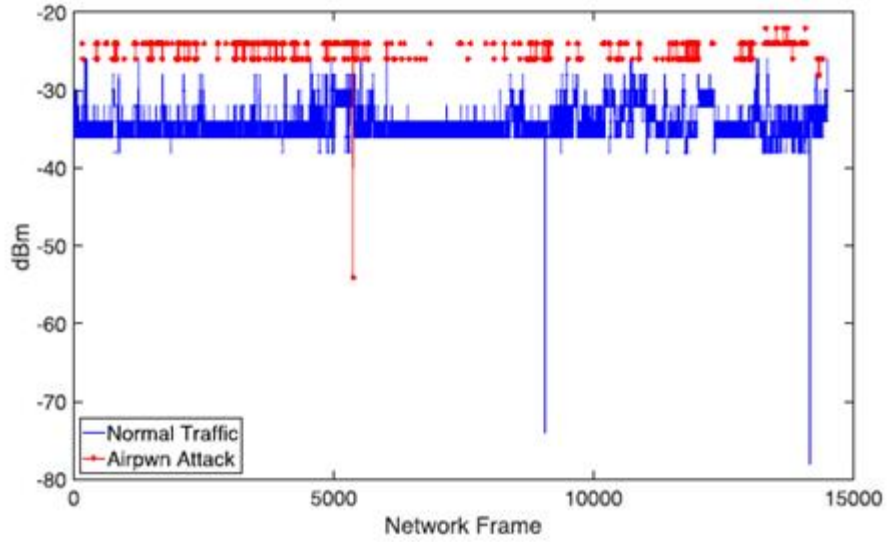


FIGURE 6. RSSI - Received signal strength measured by the victim machine during implementation of the MitM attack.

VI. EVALUATION OF RESULTS

This section describes the off-line detection results, and compares the results generated by the proposed methodology using all the possible combinations of metrics. There are two main purposes of these results. First, to evaluate the efficiency of the proposed methodology in identifying the presence of attacks, and producing reduced number of false alarms. Second, to identify which of the possible combinations of metrics produces the best detection results.

The effectiveness of the proposed methodology has been evaluated using the following performance metrics, which provide evidence of how effective an IDS is at making correct detections:

Performance Metrics

- True Positive Rate (TPR) or Detection Rate - Proportion of malicious frames correctly classified among all the malicious data:

$$TPR = \frac{TP}{TP + FN} \tag{18}$$

- False Positive Rate (FPR) - Proportion of normal data misclassified as malicious among all the normal data:

$$FPR = \frac{FP}{TN + FP} \tag{19}$$

- Overall Success Rate (OSR) or Accuracy - Proportion of frames correctly classified among all the data:

$$OSR = \frac{TP + TN}{TP + FP + TN + FN} \tag{20}$$

- *Precision* - Proportion of malicious frames correctly classified among all the alarms generated:

$$Precision = \frac{TP}{TP + FP} \tag{21}$$

- *F*-score - Tradeoff between *Precision* and TPR, used to compare two distinctive classification methodologies:

$$F\text{-}score = \frac{2 \cdot Precision \cdot TPR}{Precision + TPR} \tag{22}$$

Performance Metrics

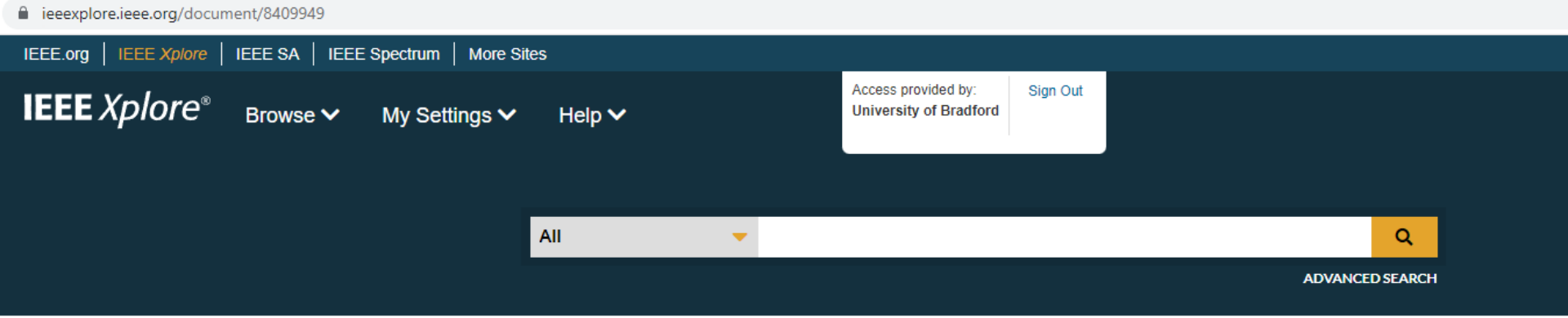
where True Positive (TP) represents attacks classified as attacks; True Negative (TN) represents normal instances classified as normal; False Positive (FP) represents normal instances misclassified as attack; and False Negative (FN) represents attacks misclassified as normal.

We have divided the datasets in 80% for training (i.e. *train* data) and 20% for testing (i.e. *test* data). The training dataset was used to build the normality and attack baselines (i.e. *baseline* data), whereas the remaining data were used to generate the beliefs and evaluate the proposed methodology.

Since the attacker would use a low transmission rate, the NAV value set by the attacker would equivalently be larger than the NAV value set by the legitimate wireless devices.

From the presented results, it would be expected to use the single metric methodology using either *Rate* or *NAV* to defend the wireless network against MitM attacks at the physical layer. Nonetheless, the detection system cannot assume the implementation parameters chosen by the attacker. More importantly, it is impossible to anticipate the particular type of attack implemented by the attacker. Hence, basing the wireless injection attack detection on the use of single metric may be prone to a high number of misclassification results.

I. Ghafir et al., "A Basic Probability Assignment Methodology for Unsupervised Wireless Intrusion Detection," IEEE Access, vol. 6, pp. 40008-40023, 2018. https://ieeexplore.ieee.org/document/8409949



I. Ghafir et al., "A Basic Probability Assignment Methodology for Unsupervised Wireless Intrusion Detection," IEEE Access, vol. 6, pp. 40008-40023, 2018. https://ieeexplore.ieee.org/document/8409949

Recommended reading:

- Developed IDS … IDS evaluation
- Structure of the paper

Summary

- Intrusion Detection Systems (IDSs) aim to distinguish between malicious traffic and normal traffic
- Intrusion Prevention Systems (IPSs) can filter malicious traffic
- Classification of intrusion detection systems
  - By scope
  - By mode of operation
- IDSs should detect all attacks correctly and monitor systems effectively with minimum overhead
- IDSs can monitor the attack, reduce exposure or alert a human
- The underlying goal is to keep FP and FN as low as possible