V2X Communication Protocols:
Survey Implementation Slides

Group 1C: Opeyemi Ajibuwa, Robert Brown, Ching-Shian Chen, and Wenxuan Zhu

OBJECTIVES

- Motivation
- Recap the issues identified from the previous survey
- Discuss Experiments and Case Studies
- Open Issues

Survey Recap: DSRC and C-V2X Security Vulnerabilities

- Authenticity
  - Man-in-the-Middle Attacks
  - GPS spoofing
  - False packet injection
- Network Attacks
  - Denial-of-Service attacks
- Privacy
  - Location tracking

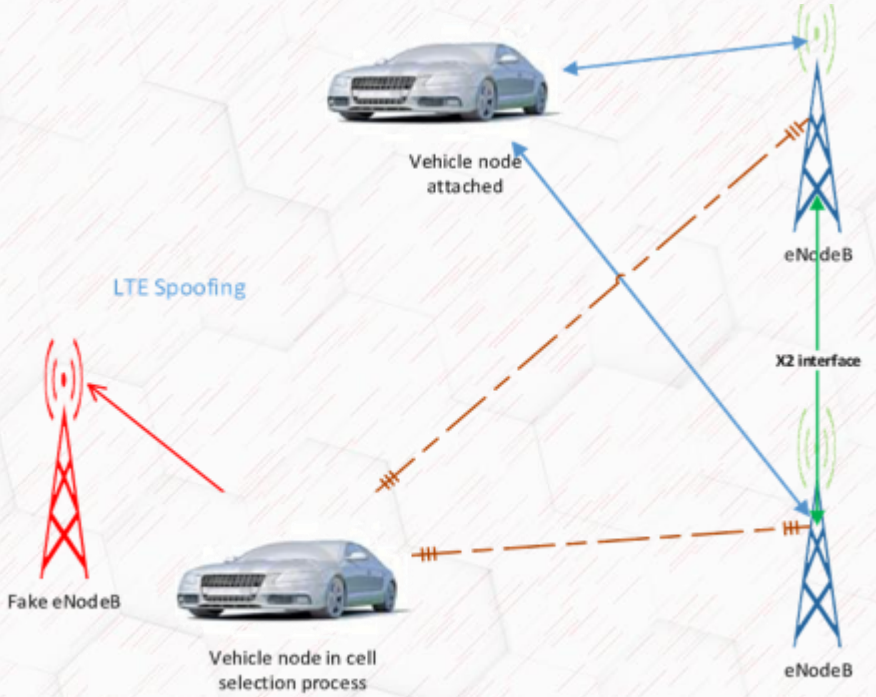
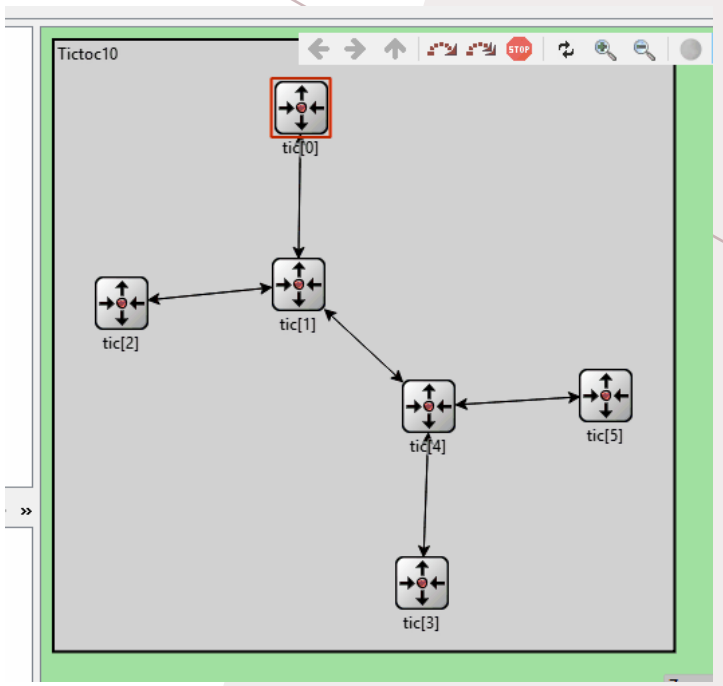


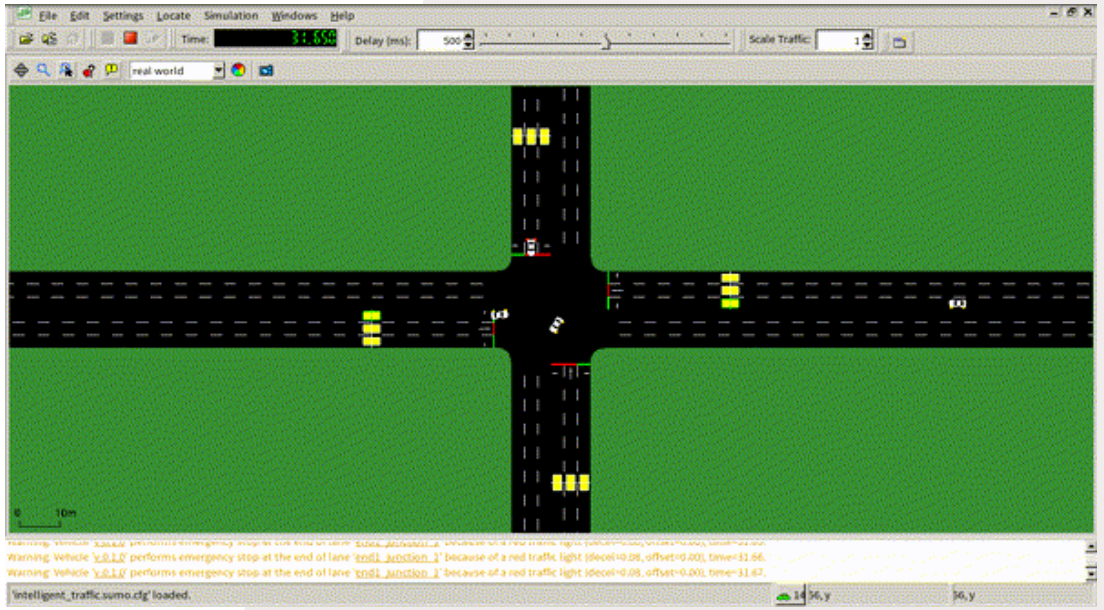
Fig. 9. LTE spoofing attack.

EVALUATION TOOLS

- Network Simulators:
  - OMNet++
- Traffic Tools:
  - Simulation of Urban MObility (SUMO)

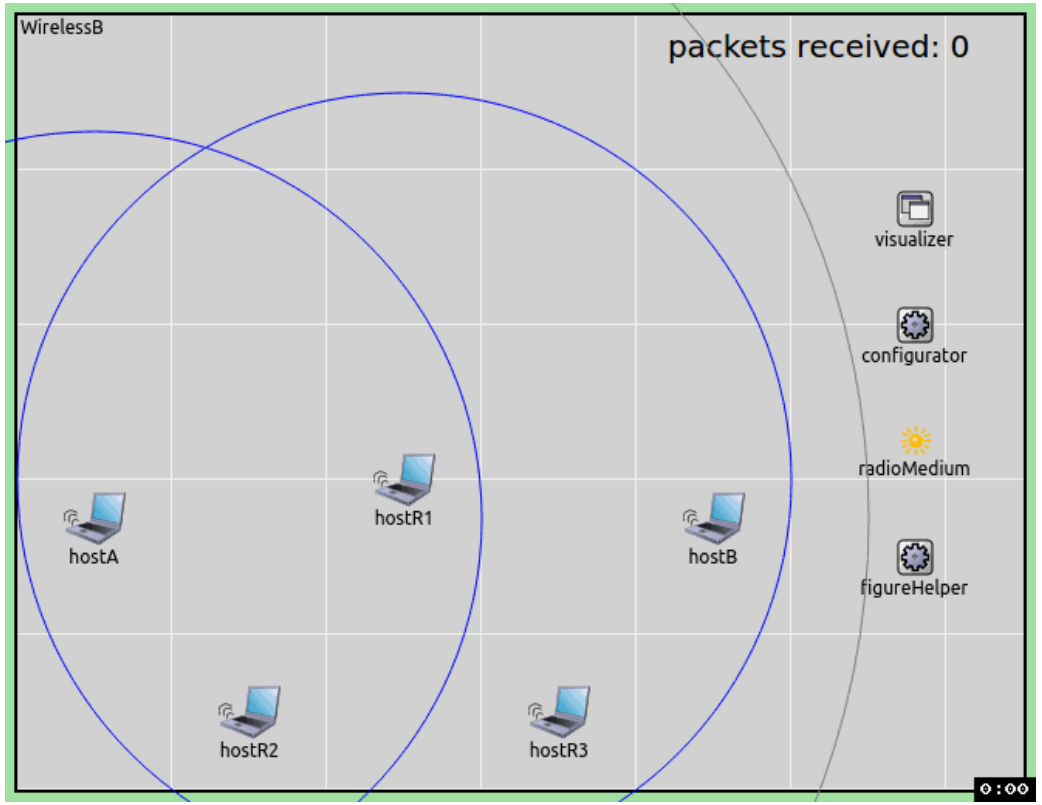
- Together, these tools can provide a robust testing framework for VANETs





EVALUATION TOOLS

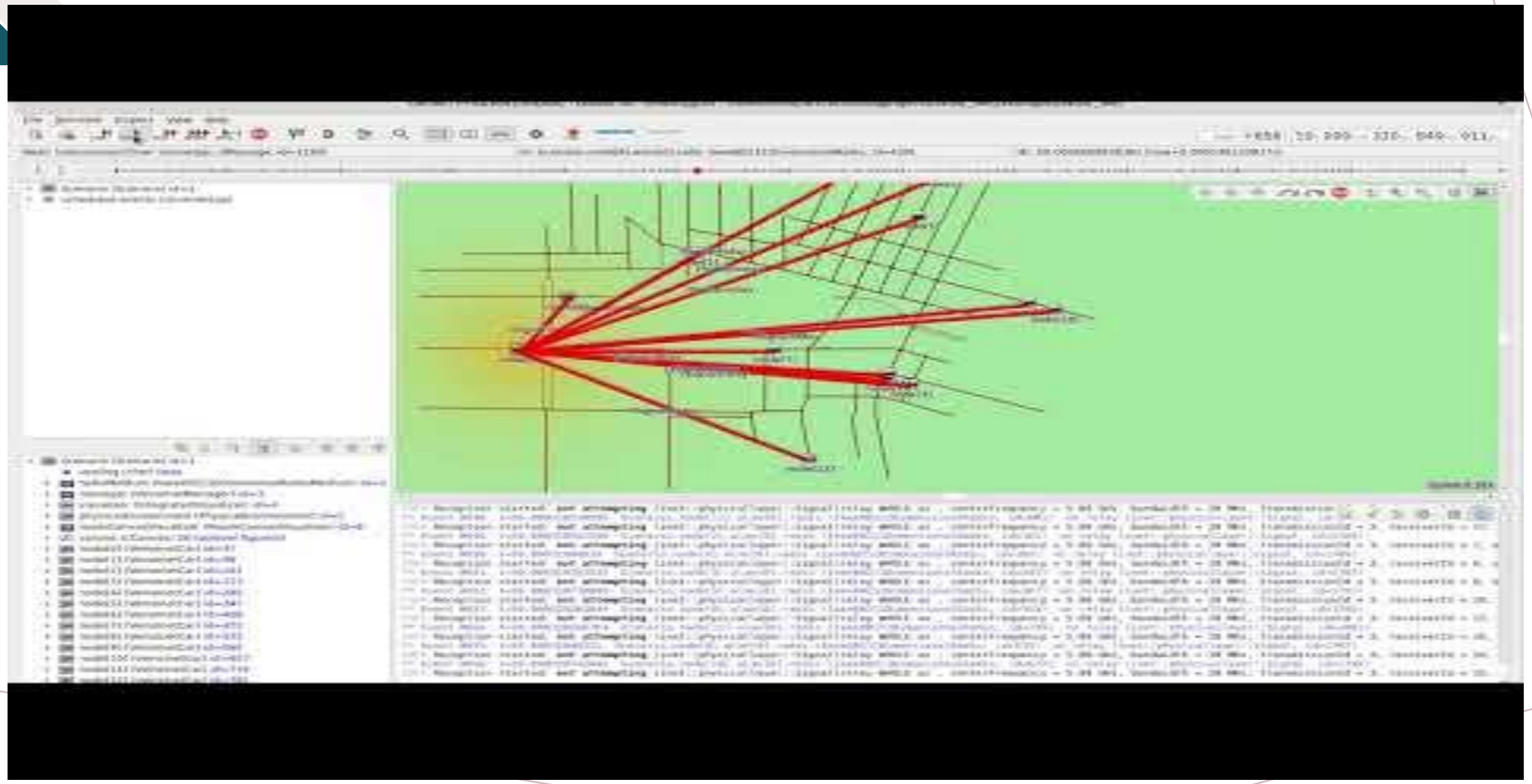
- Submodules of OMNet++
  - INET Framework
  - VEINS Framework
- INET extends OMNET++ by implementing radio and network protocol (i.e., 802.11)
- VEINs combines SUMO and OMNet++
  - Uses motions in SUMO to move network nodes in OMNet++
  - Uses network events in OMNet++ to control vehicles in SUMO



EXPERIMENT 1: TRAFFIC ACCIDENTS COMMUNICATION

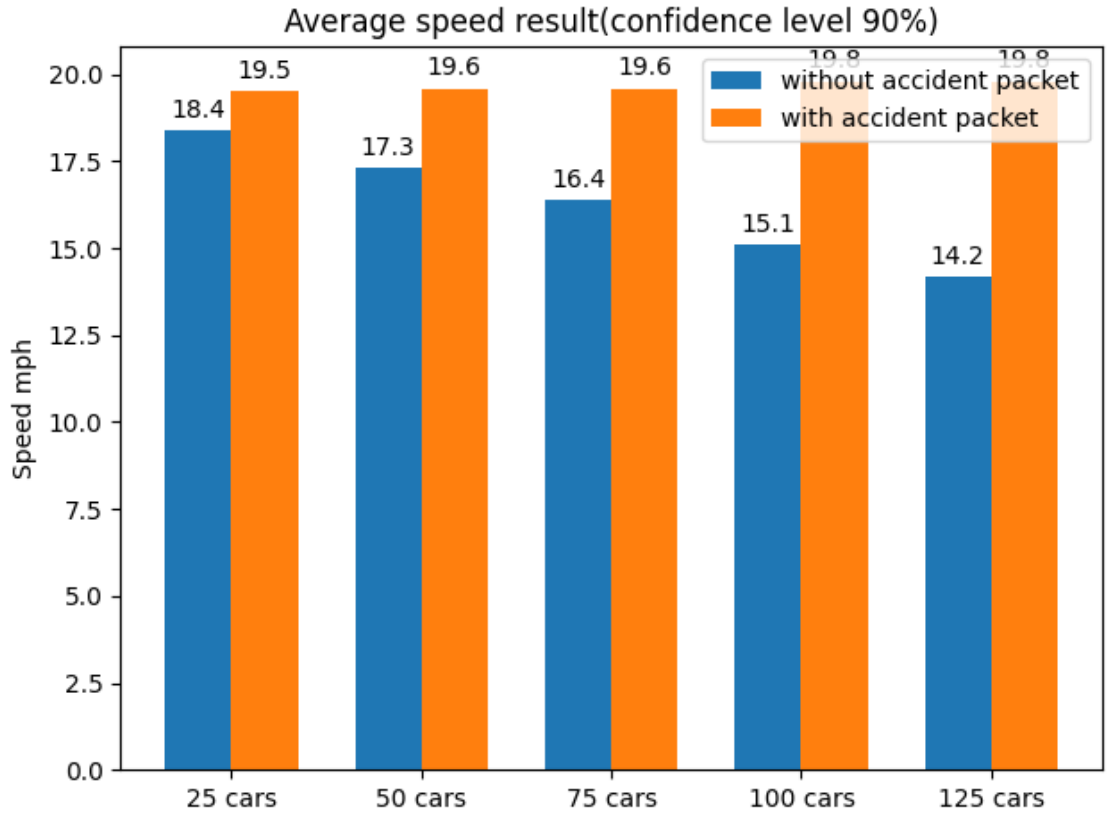
- Report to other vehicle if there are any accident
- Avoid traffic jam
- Cons

EXPERIMENT 1: SIMULATION DEMO VIDEO



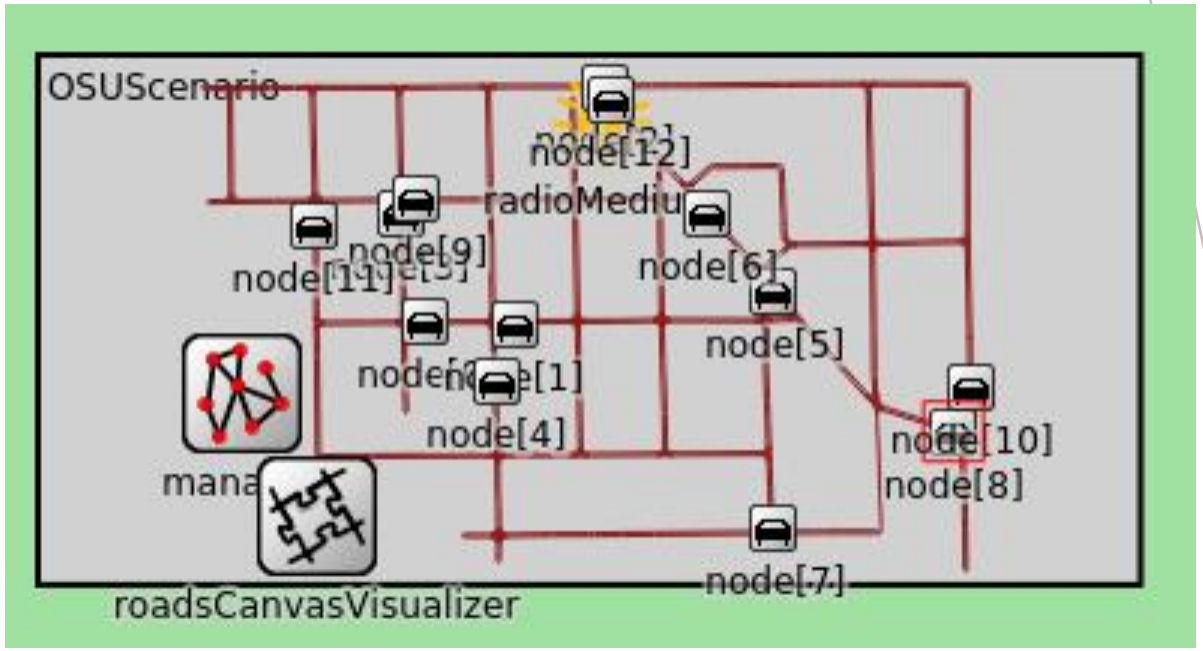
EXPERIMENT 1: RESULTS

- More cars, lower average speed if there are no accident packet.
- Improvement

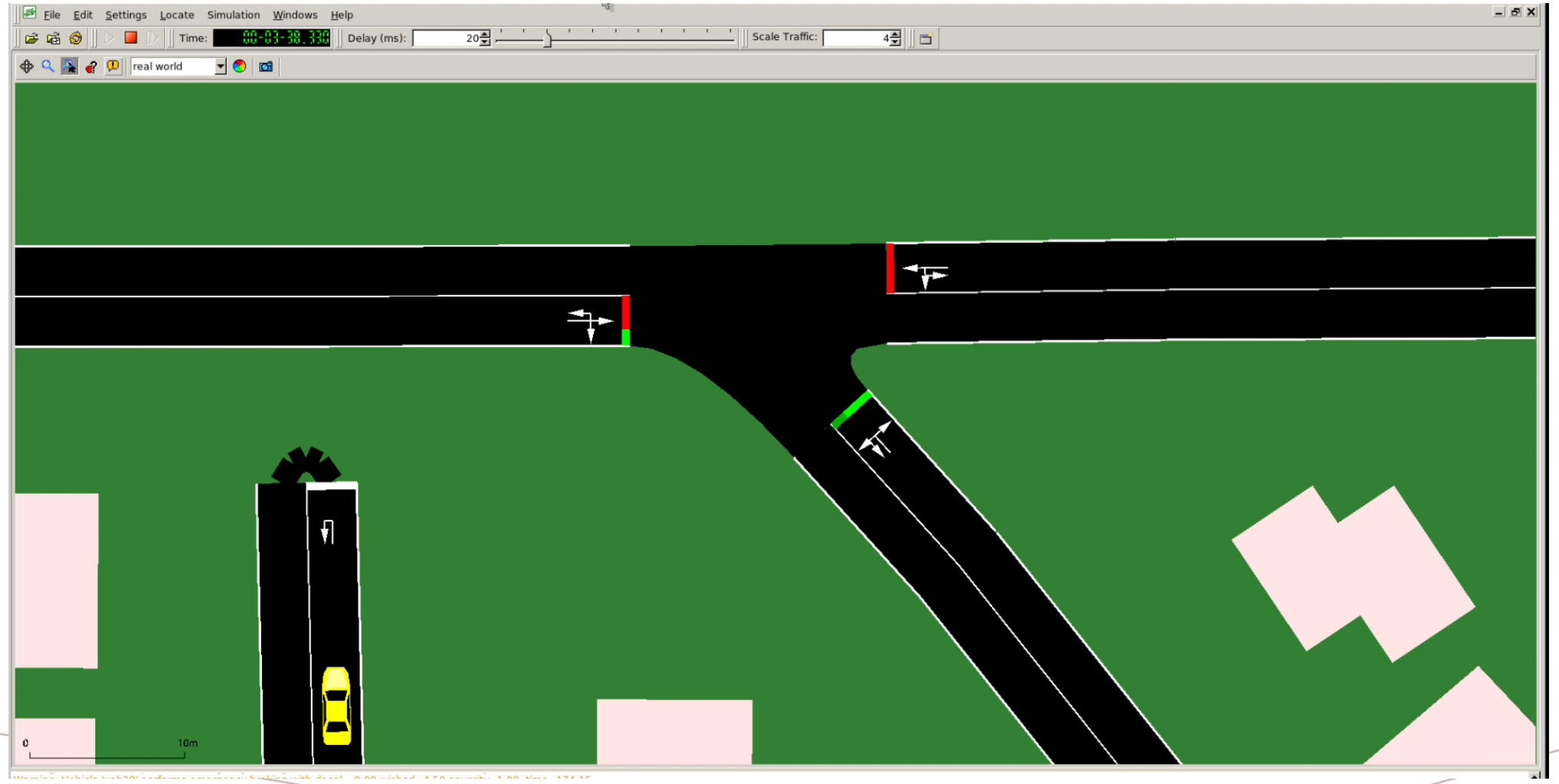


EXPERIMENT 2 : 802.11P PARAMETER STUDY

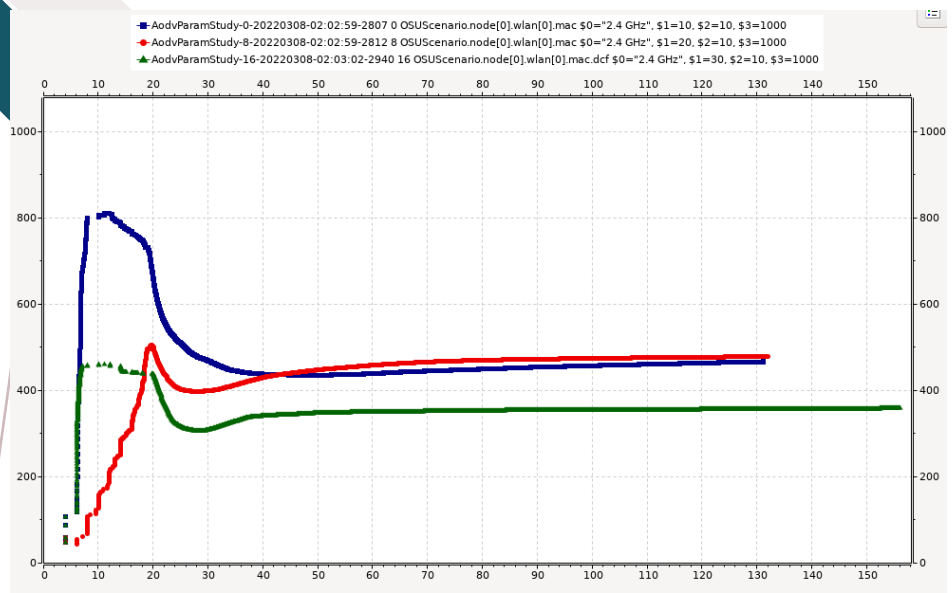
- Multiple cars drove around and periodically shared data-packets
- Independent Variables:
  - Center Freq: 2.4GHz or 5.9 GHz
  - Bandwidth: 10 and 20 MHz
  - TX Power: 10, 20, 30, and 40 mW
  - Packet Size: 1, 10, 100, 1000 kB
- Dependent Variables:
  - Network Throughput
  - Dropped Packets
  - Collisions

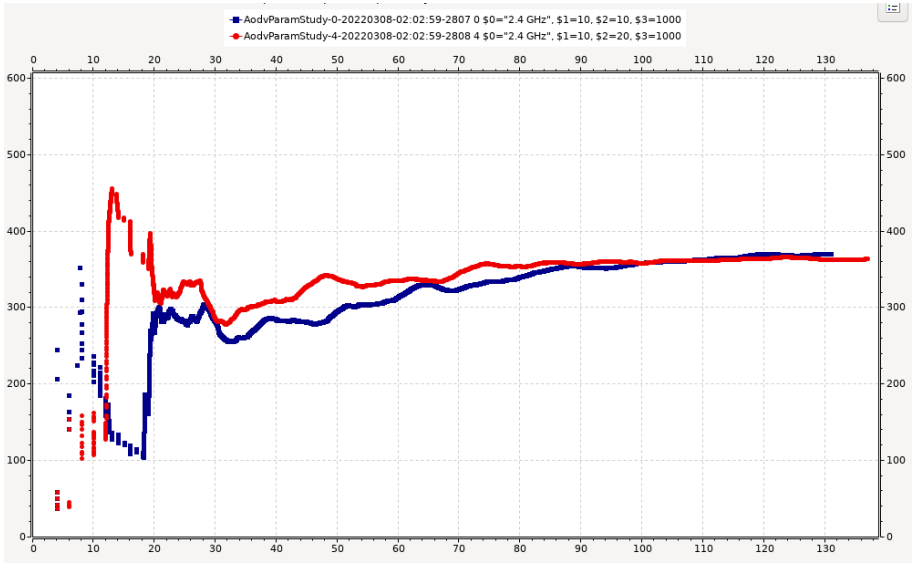


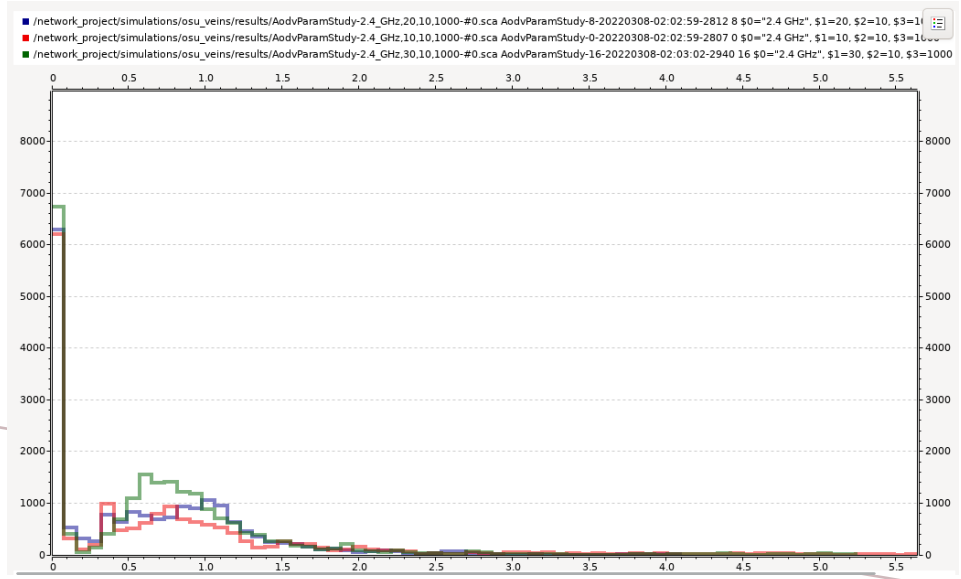
EXPERIMENT 2: SIMULATION DEMO VIDEO

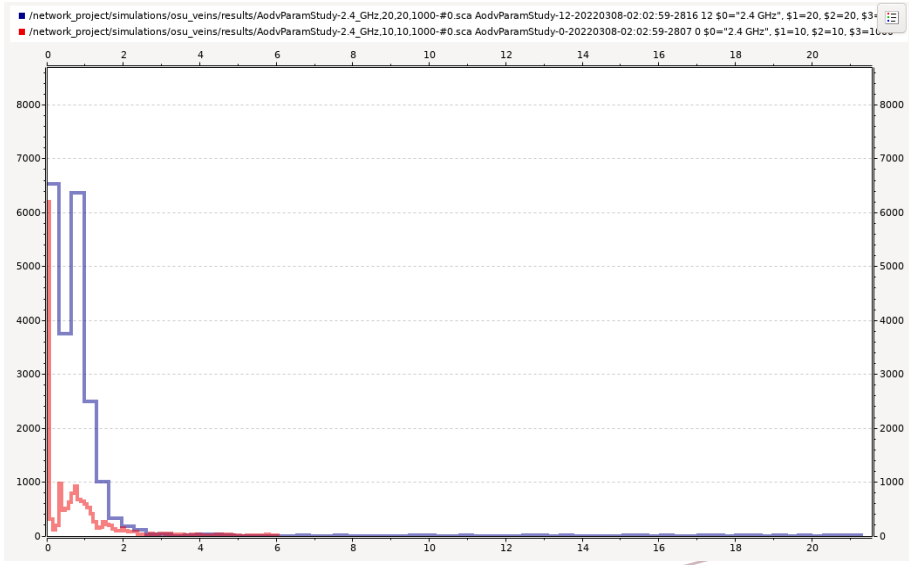


EXPERIMENT 2 RESULTS









Experiment 3: Attack Messages Detection in V2X communication

Challenge

Correctly detecting/predicting attack messages remains a lingering issue in V2X communication

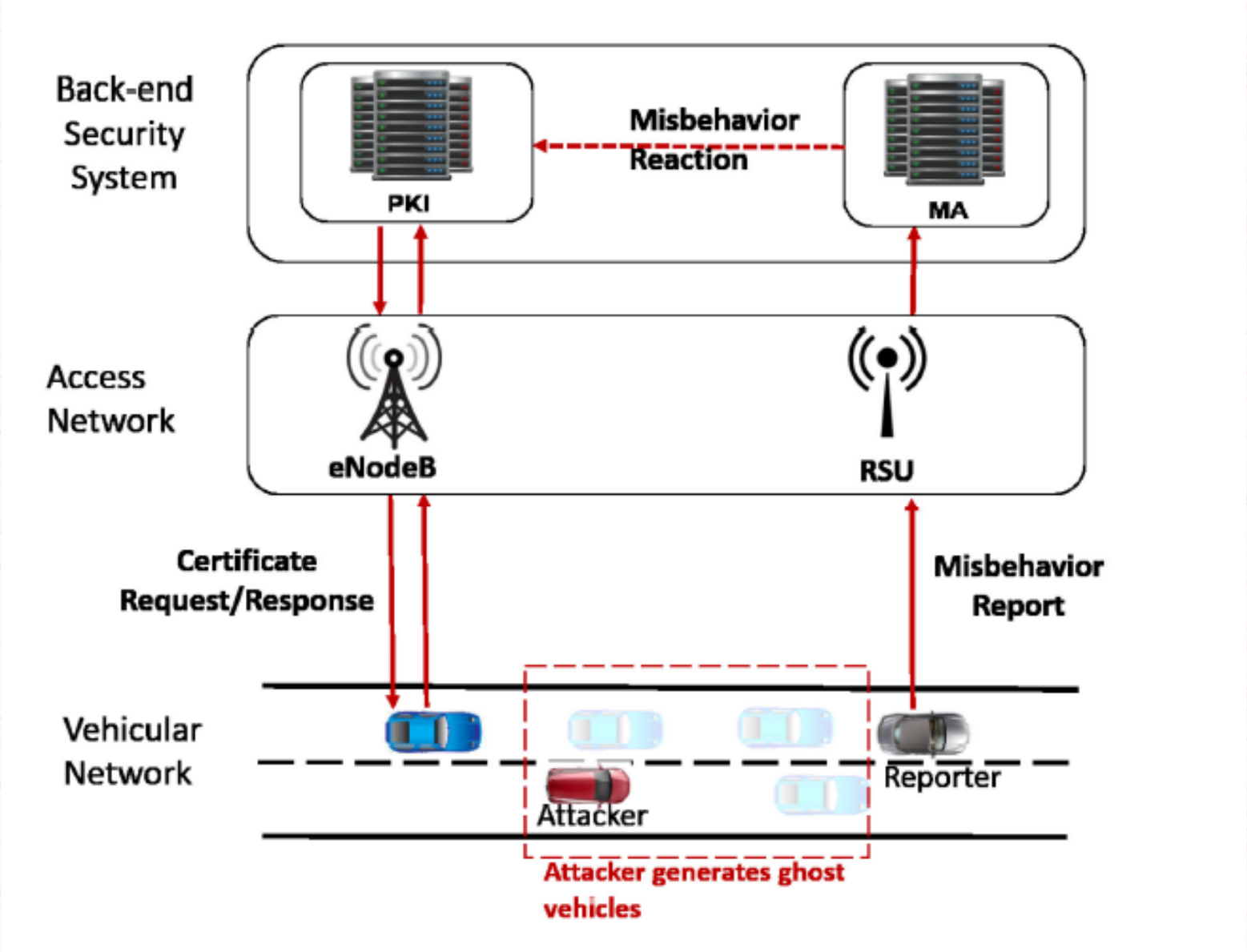
Existing Approach: Thresholding detectors

- Sudden appearance warning (SAW), acceptance range threshold (ART), distance moved verifier (DMV) and simple speed check (SSC) are detectors that have been proposed in [1].
- Each of these detectors employs different threshold values to identify different attacks.
- However, the performance of these detectors relies on these threshold values and these detectors should be tune to different threshold values depending on the vehicular environment.

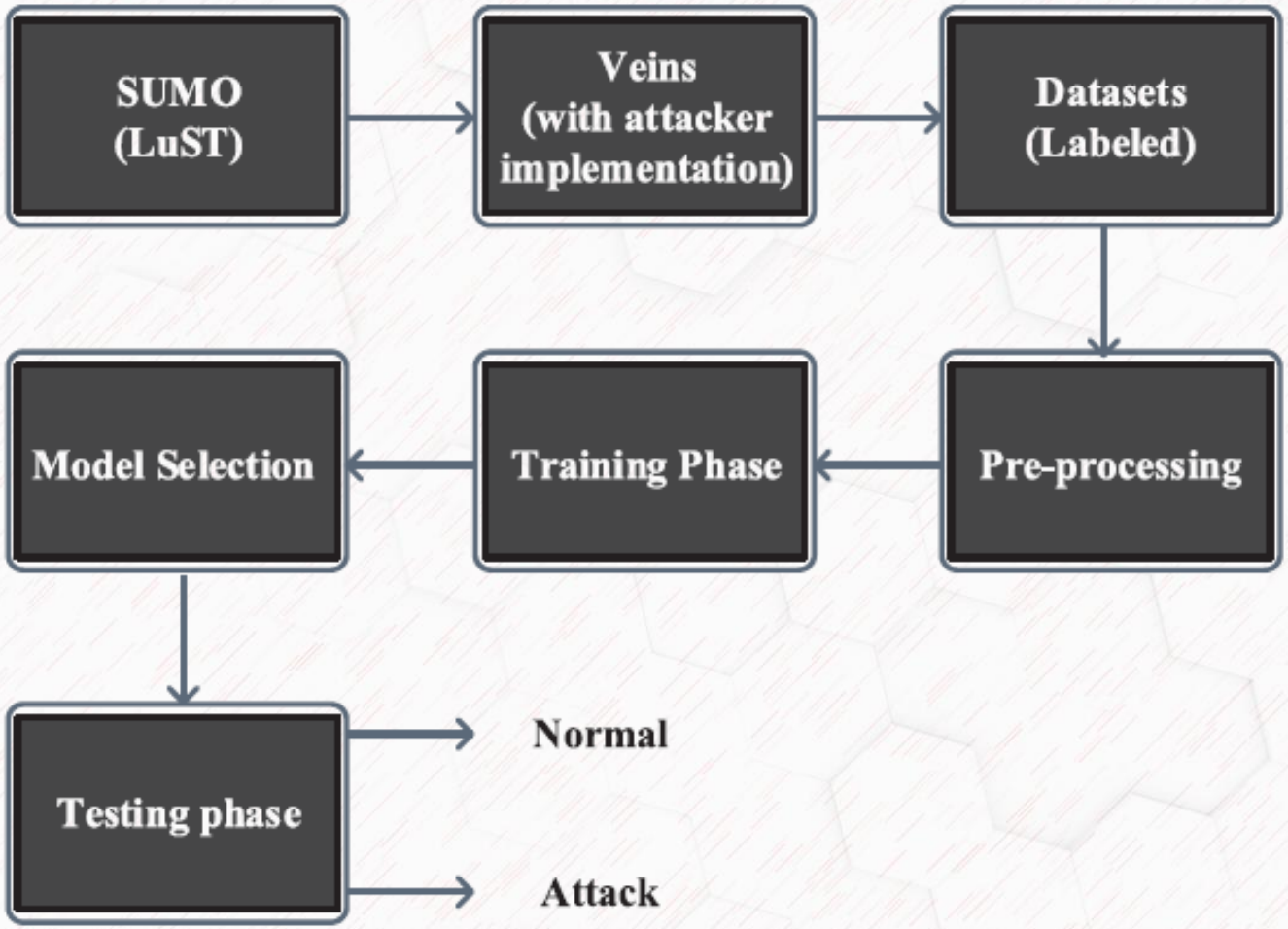
Proposed Solution

Here, we explored three different machine learning models as detectors that is free of different threshold values and can be easily deployed in the dynamic vehicular network environment.

Experiment 3: Attack Messages Detection in V2X communication



Methodology of the Machine Learning based Analysis



Evaluation Metrics

- *Accuracy* is the proportion of correctly predicted vehicle behaviors to the total vehicles.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{21}$$

- *Precision* shows the proportion of correctly predicted malicious vehicles to the total predicted malicious vehicles.

$$Precision = \frac{TP}{TP + FP} \tag{22}$$

- *Recall* shows the proportion of correctly predicted malicious vehicles to the total actual malicious vehicles.

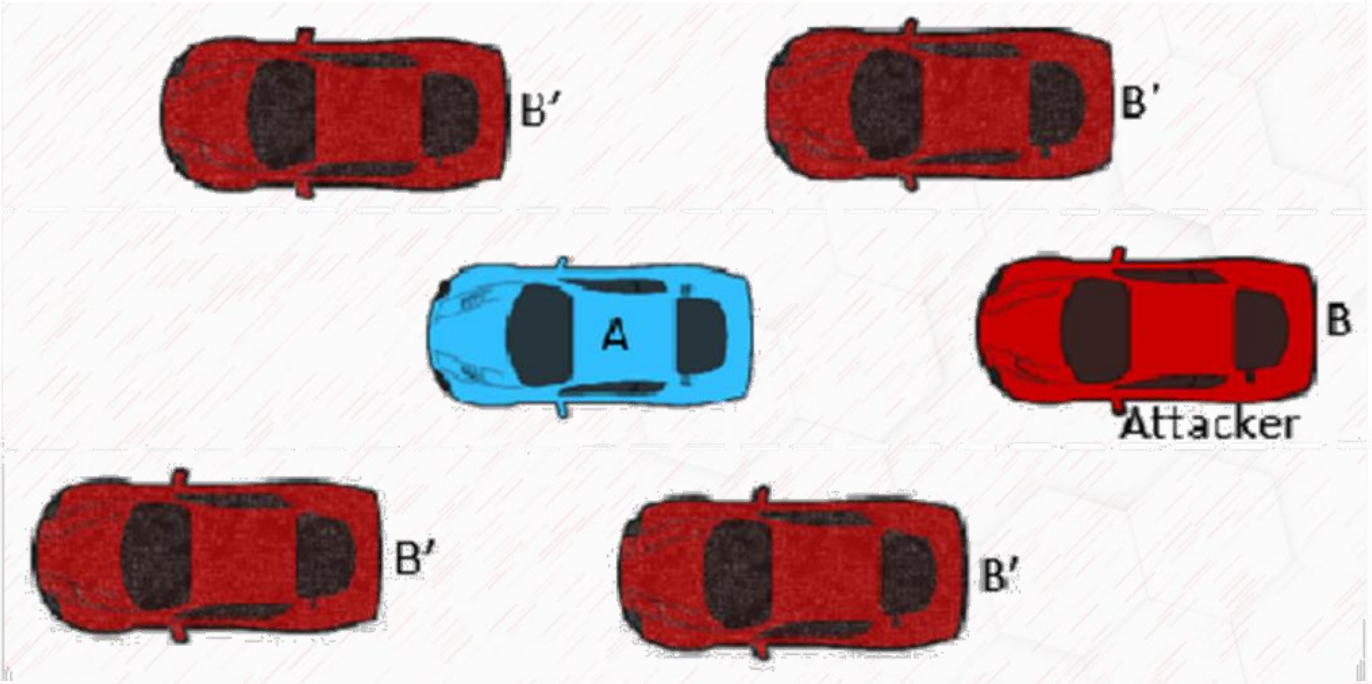
$$Recall = \frac{TP}{TP + FN} \tag{23}$$

- *F1-score* is the weighted average of precision and recall.

$$F1\text{-}score = 2 \times \frac{precision \times recall}{precision + recall} \tag{24}$$

Evaluation metrics

Attack Model



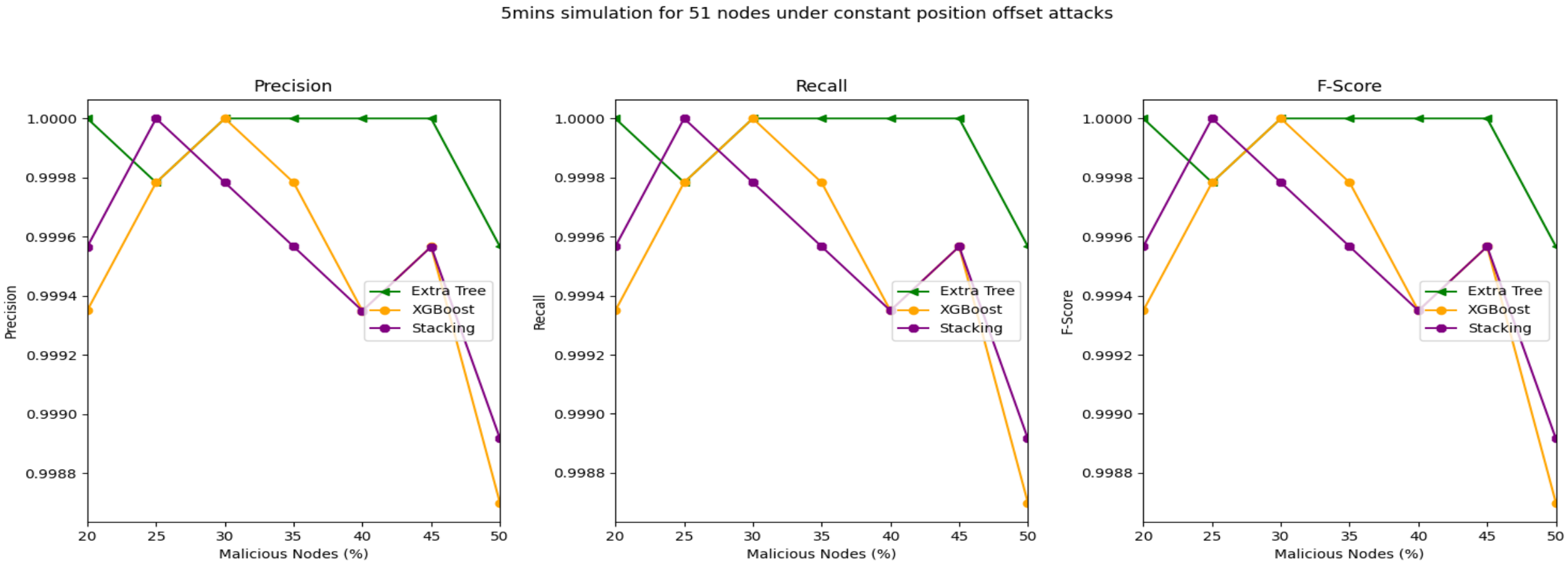
Considered Attacks:

1. Constant Position Offset: The misbehaving node emits its sensor location with a fixed offset on the X and Y axis.

2. The Sybil Attack: The attacker generates and transmits a virtual grid of vehicles using the plausible data of an existing vehicle in the network. The attacker generates an identity and manages a correct transmission frequency for each ghost vehicle.

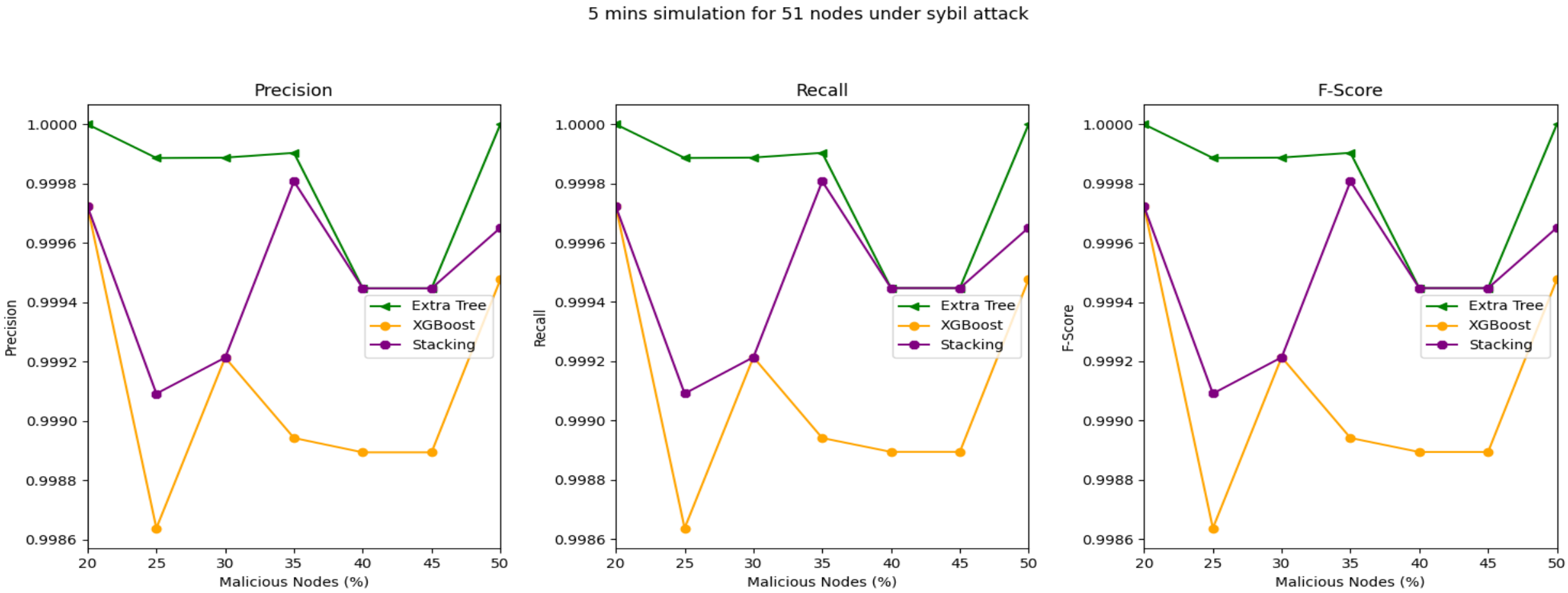
```
# Local Attack Types ... 0:Genuine, 1:ConstPos, 2:ConstPosOffset, 3:RandomPos, 4:RandomPosOffset, 5:ConstSpeed
# Local Attack Types ... 6:ConstSpeedOffset, 7:RandomSpeed, 8:RandomSpeedOffset, 9:EventualStop, 10:Disruptive,
# Local Attack Types ... 11:DataReplay, 12:StaleMessages, 13:DoS, 14:DoSRandom, 15:DoSDisruptive, 16:GridSybil,
# Local Attack Types ... 17:DataReplaySybil, 18:DoSRandomSybil, 19:DoSDisruptiveSybil
```

Simulation Results



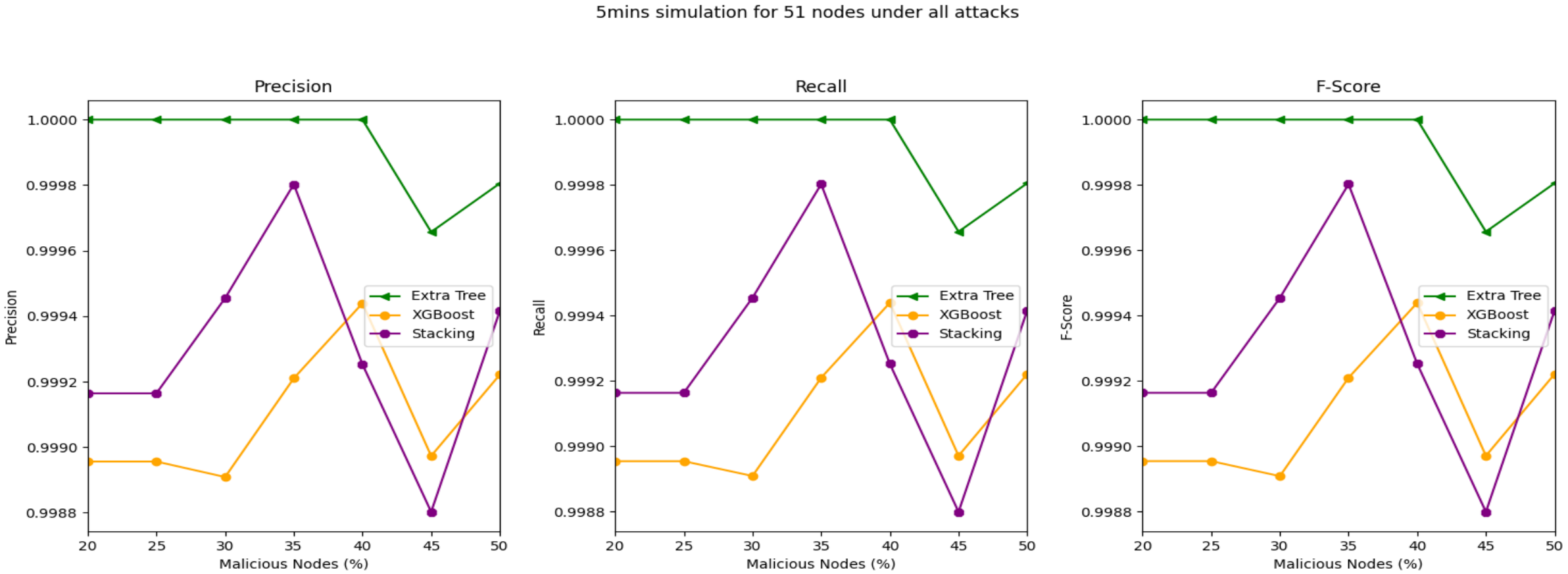
Parameters: 5mins, 51nodes, Constant position offset attacks

Simulation Results



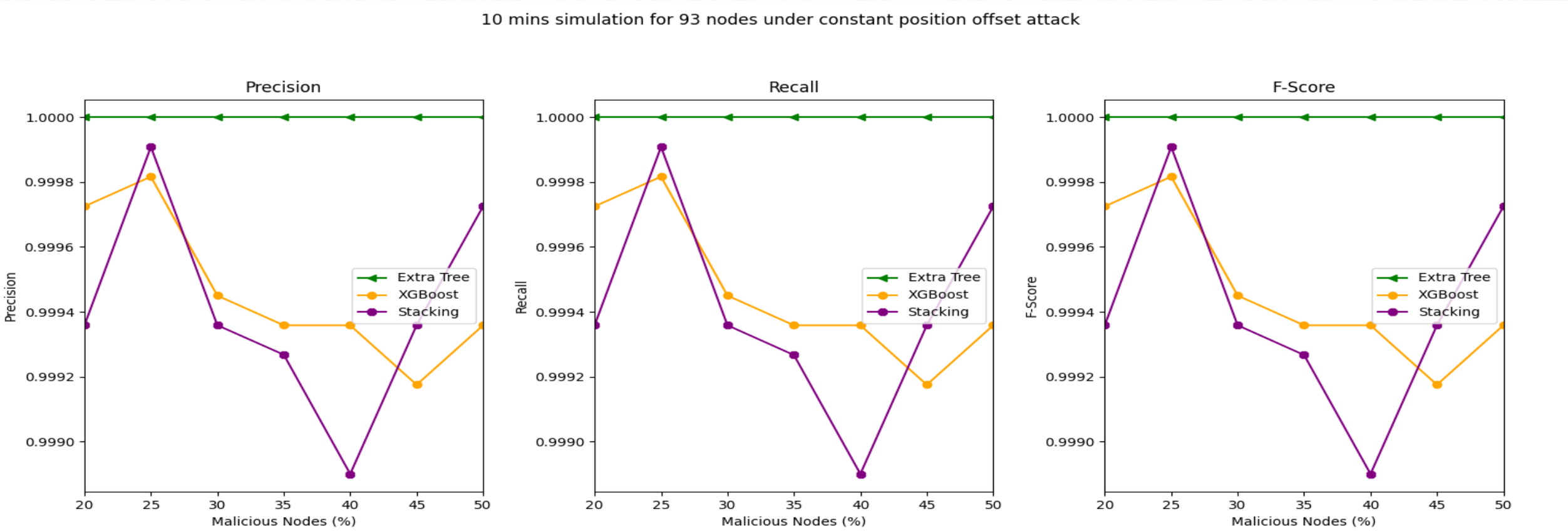
Parameters: 5mins, 51nodes, Sybil attacks

Simulation Results



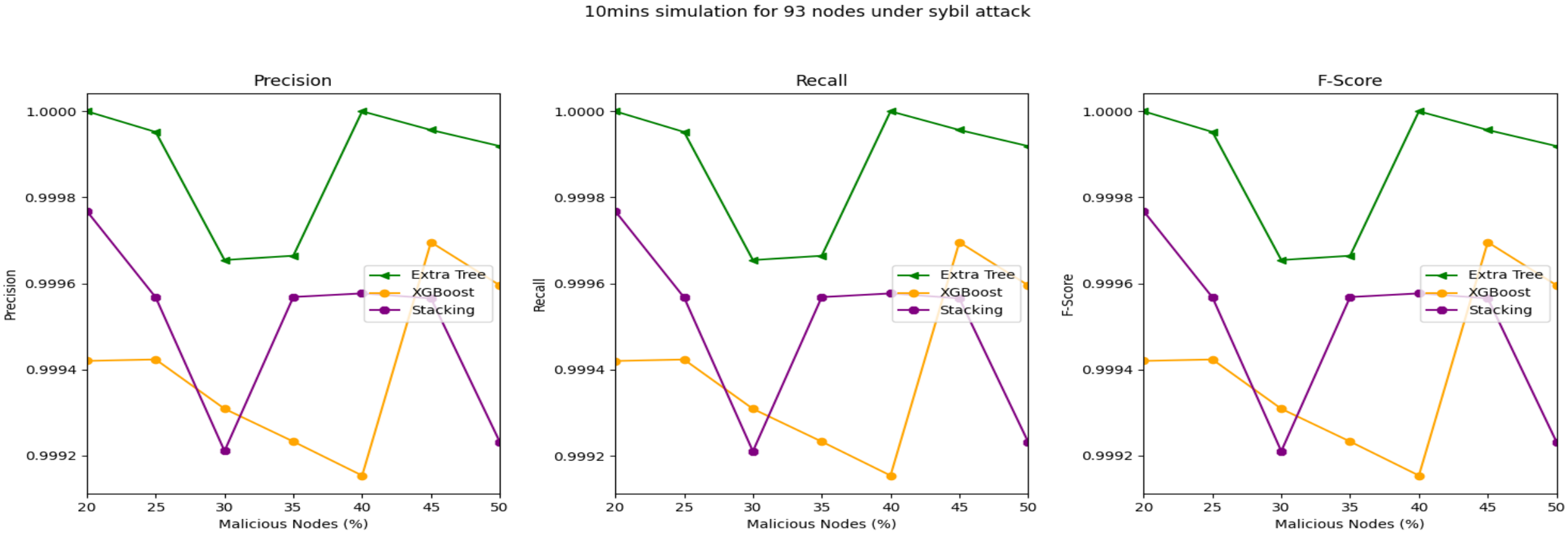
Parameters: 5mins, 51nodes, All attacks

Simulation Results



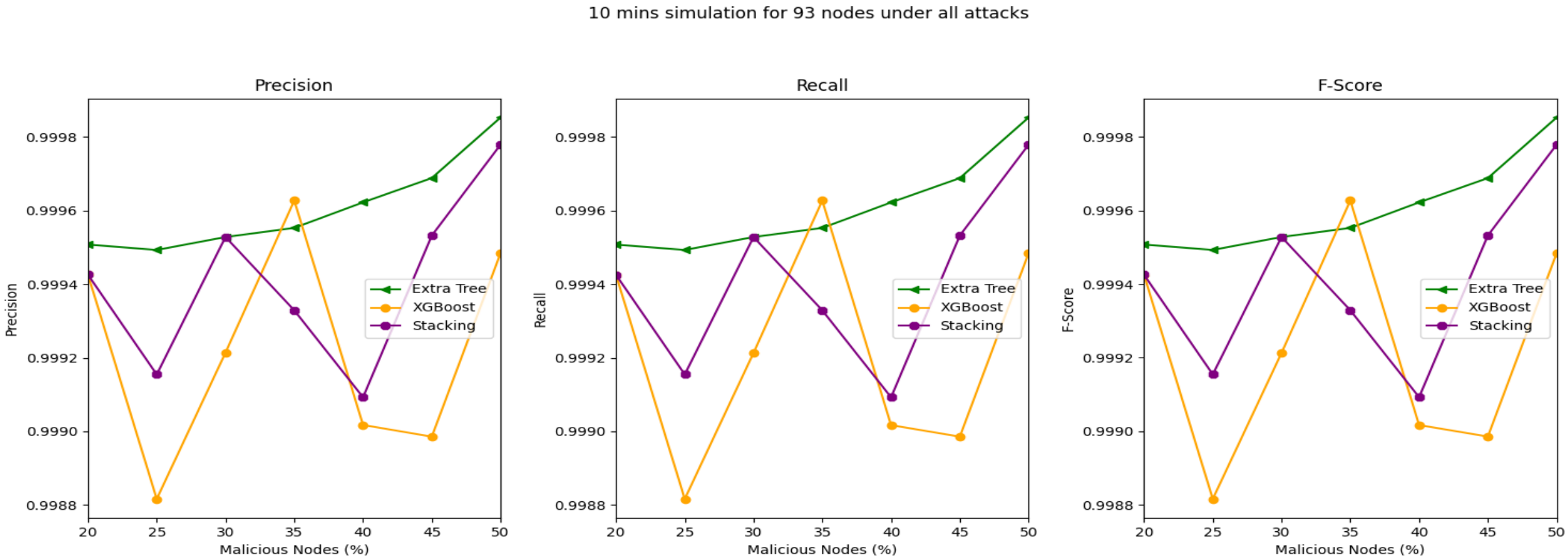
Parameters: 10mins, 93nodes, Constant position offset attacks

Simulation Results



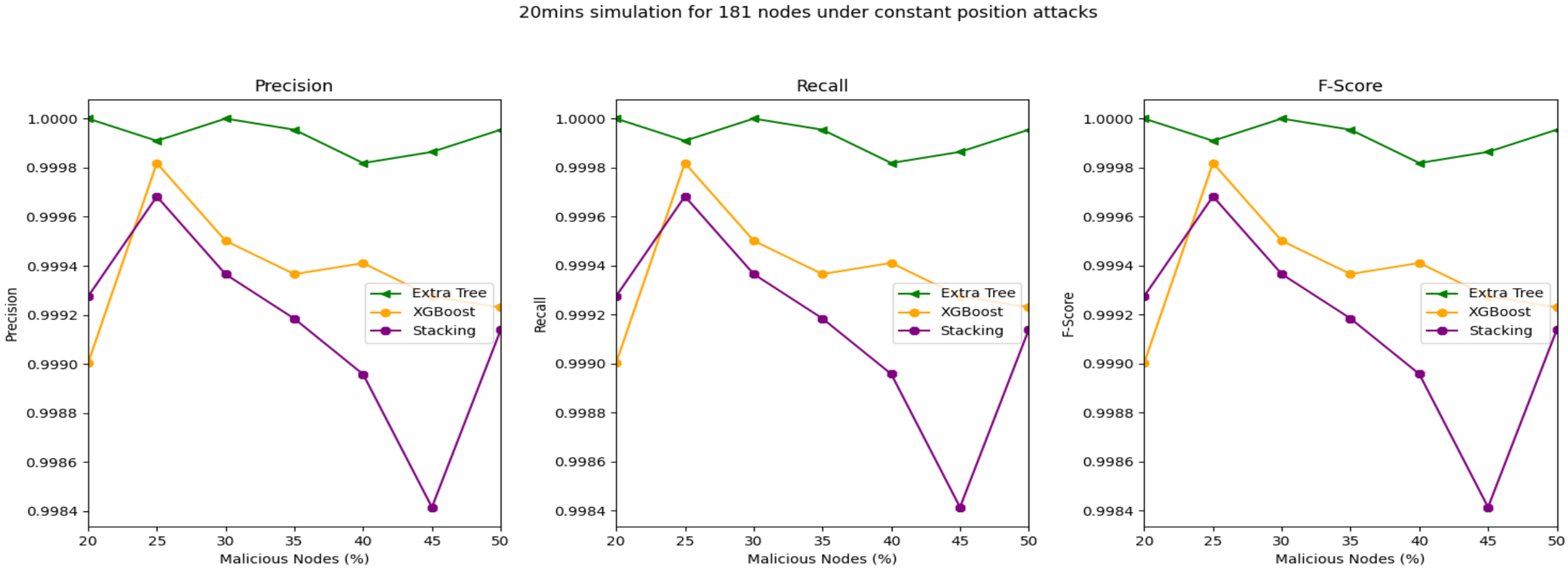
Parameters: 10mins, 93nodes, Sybil attacks

Simulation Results



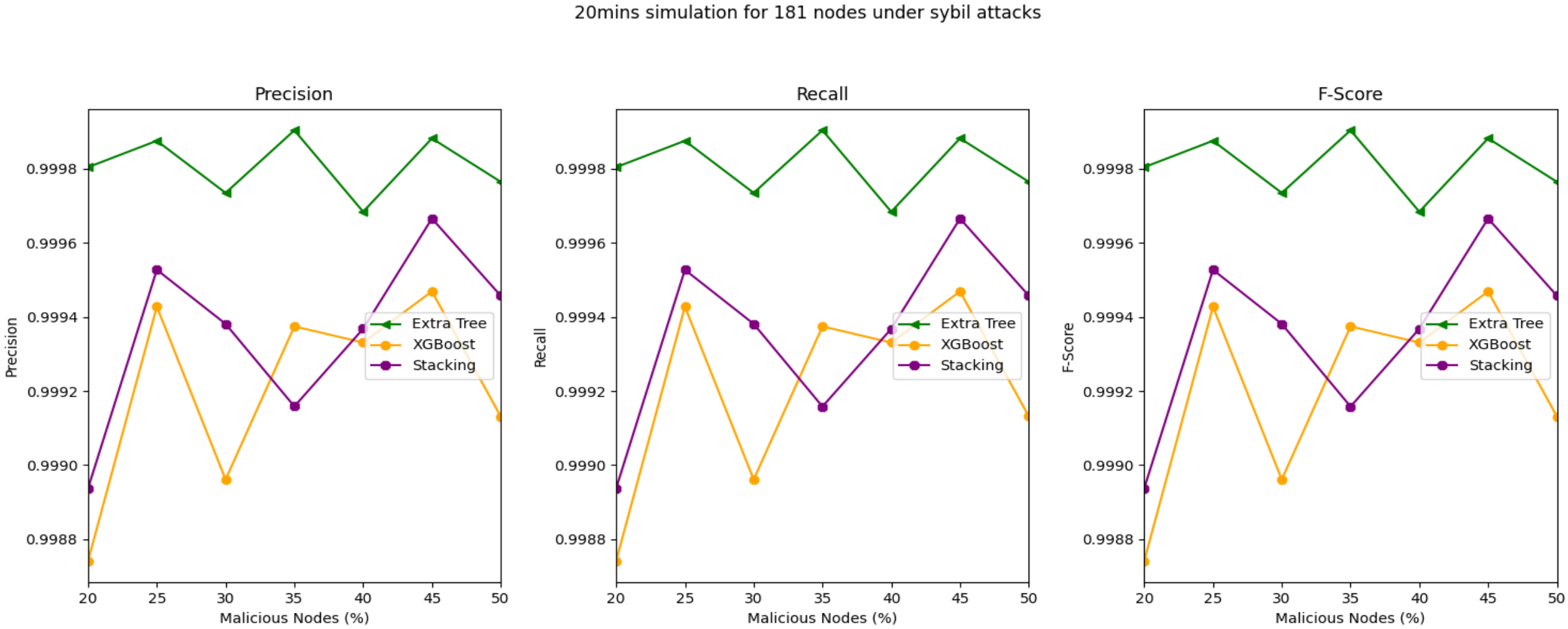
Parameters: 10mins, 93nodes, All attacks

Simulation Results



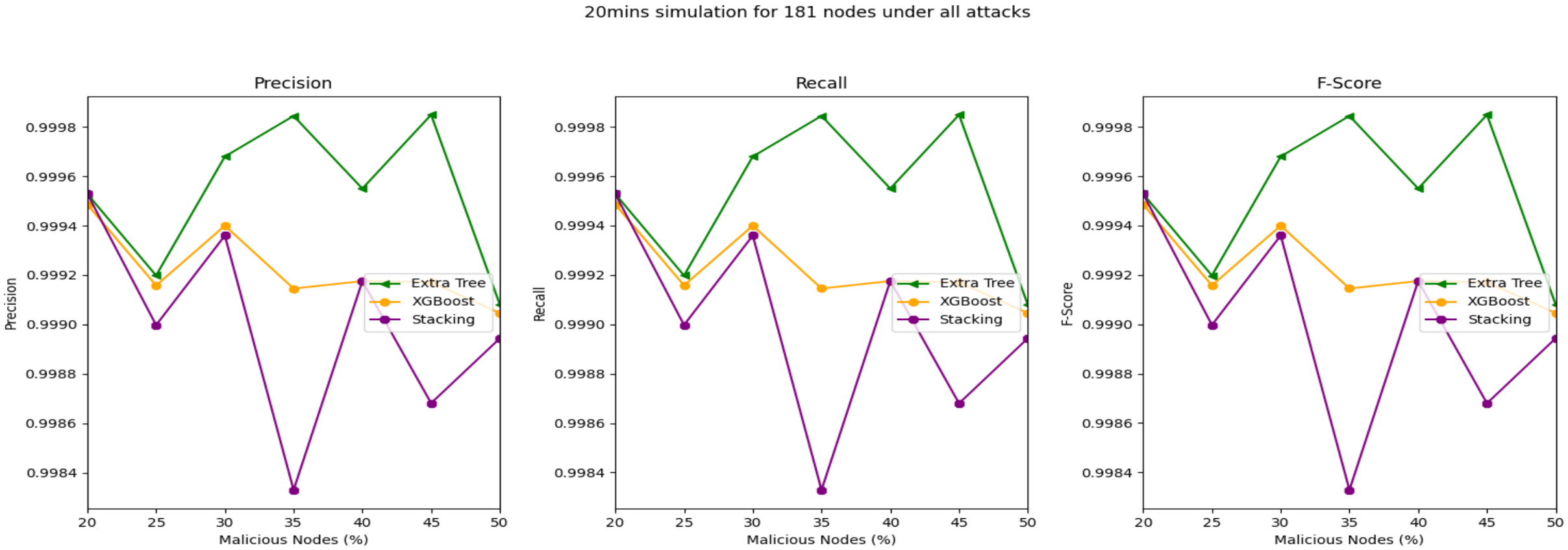
Parameters: 20mins, 181nodes, Constant position attacks

Simulation Results



Parameters: 20mins, 181nodes, Sybil attacks

Simulation Results



Parameters: 20mins, 181nodes, All attacks

Conclusion and Next Steps

- The Extra Tree model perform best among the ML models considered obtaining high precision, recall and F1-score under varying attackers node densities.

- For the final report, we hope to compare our model's performance with the results of an existing approach in the literature.