

Report on IDS Algorithm Test Cases

1. Previous Test Cases

1.1 Inject High `stNum` , High `sqNum`

Overview:

This test case involved injecting GOOSE messages with abnormally high values for the state number (`stNum`) and sequence number (`sqNum`). The purpose was to evaluate the IDS's ability to detect anomalous increments that deviate significantly from the normal progression.

Execution:

The script modified the GOOSE messages by setting `stNum` and `sqNum` to high values far beyond typical operational ranges.

1.2 Inject Low `stNum` , Low `sqNum`

Overview:

In this test case, GOOSE messages were injected with abnormally low `stNum` and `sqNum` values. The goal was to test the IDS's ability to identify messages with values that are suspiciously low and potentially indicative of a rollback or replay attack.

Execution:

The script altered the GOOSE messages by setting `stNum` and `sqNum` to values significantly lower than expected.

1.3 Data Manipulation (DM) in `stNum` , `sqNum` , and Boolean

Overview:

This test case involved direct manipulation of the `stNum`, `sqNum`, and boolean data within the GOOSE messages. The aim was to see how well the IDS could detect a combination of multiple manipulated fields.

Execution:

The script simultaneously modified `stNum`, `sqNum`, and boolean data in the GOOSE messages.

2. 26 June Test Cases

2.1 Data Manipulation in `stNum`, `sqNum`, and GOOSE Length

Overview:

This test case focused on manipulating `stNum`, `sqNum`, and the length of the GOOSE message. The objective was to test the IDS's ability to detect inconsistencies in multiple parameters, including the overall message length.

Execution:

The script adjusted `stNum`, `sqNum`, and modified the length of the GOOSE message to create an anomalous packet.

2.2 Data Manipulation in `stNum`, `sqNum`, and Boolean

Overview:

Similar to the previous multi-field manipulation, this test case targeted `stNum`, `sqNum`, and boolean values within the GOOSE messages. The aim was to validate the IDS's detection capabilities for these specific fields.

Execution:

The script altered `stNum`, `sqNum`, and boolean values in the GOOSE messages.

2.3 Data Manipulation in GOOSE Length

Overview:

This test case isolated the manipulation to the length of the GOOSE message. The purpose was to see if the IDS could detect anomalies based solely on the length of the messages.

Execution:

The script modified the length field of the GOOSE messages without altering any other parameters.

2.4 Data Manipulation in `sqNum` and `stNum`

Overview:

In this test case, the focus was on manipulating `sqNum` and `stNum` without altering any other fields. The goal was to evaluate the IDS's sensitivity to changes in these sequence-related parameters.

Execution:

The script modified `sqNum` and `stNum` values in the GOOSE messages.

Impact

In all test cases, the IDS successfully detected the manipulations.

Conclusion

The IDS algorithm demonstrated robust detection capabilities across a variety of test cases, successfully identifying all simulated attacks. The comprehensive testing, including manipulation of individual and multiple fields, confirmed the IDS's effectiveness in safeguarding the real-time system against various types of GOOSE message anomalies.