Analysis of Malicious Traffic in Modbus/TCP Communication

Tiago H. Kobayashi, Aguinaldo B. Batista Jr,
João Paulo S. Medeiros, José Macedo F. Filho,
Agostinho M. Brito Jr, Paulo S. Motta Pires

LabSIN - Security Information Laboratory
Department of Computer Engineering and Automation - DCA
Federal University of Rio Grande do Norte - UFRN

Agenda

- Objectives
- Introduction
- Method
  - Tools
- Experiments and Results
  - Testbeds
- Final Considerations

Objectives

- Presents a study about the influence of common IT malicious traffic on Modbus/TCP communications

Introduction

- The interconnection between SCADA and corporate networks brings security concerns
- Usage of IP-based protocols
  - Modbus/TCP, DNP3 over TCP, Ethernet/IP
- Modbus/TCP
  - Widely used automation protocol
  - TCP/IP variation of Modbus protocol

Introduction

- We analyse the influence of IT malicious traffic over the latency of Modbus/TCP transactions between Modbus/TCP clients and server
  - Modbus/TCP clients: PCs
  - Modbus/TCP server: Modbus/TCP-enable Programmable Logic Controller (PLC)
- Use of well known latency measurement techniques:
  - Round-Trip Time (RTT)
  - TCP Time-sequence Graph

Method

- We established two testbeds to illustrate different situations
- We simulated the behavior of common malicious traffic in testbeds
- To analyse the influence of malicious traffic we utilized two TCP latency measurement techniques: RTT and TCP Time-sequence Graph
- So we infer some considerations about these measurements

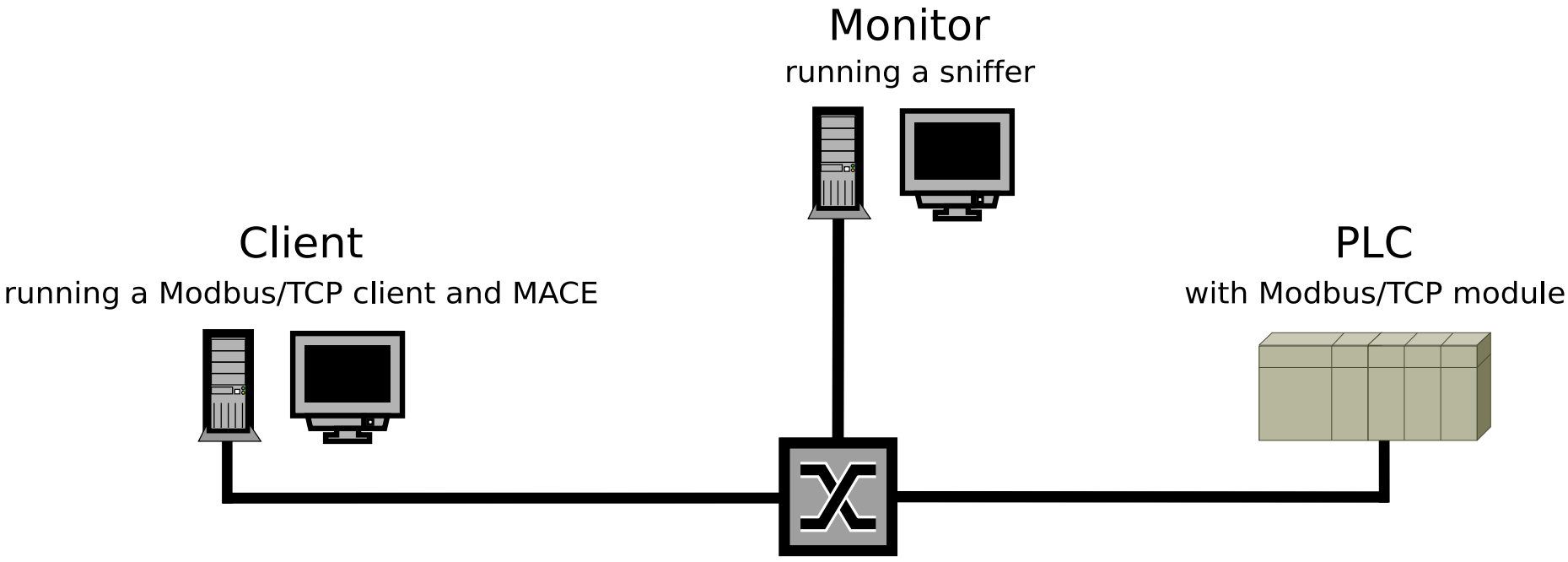
Method - Tools

- We have implemented a Modbus/TCP client application
- MACE (Malicious trAffic Composition Environment) was utilized to simulate IT malicious traffic
- We used Wireshark for monitoring and latency measurements

Experiments and Results

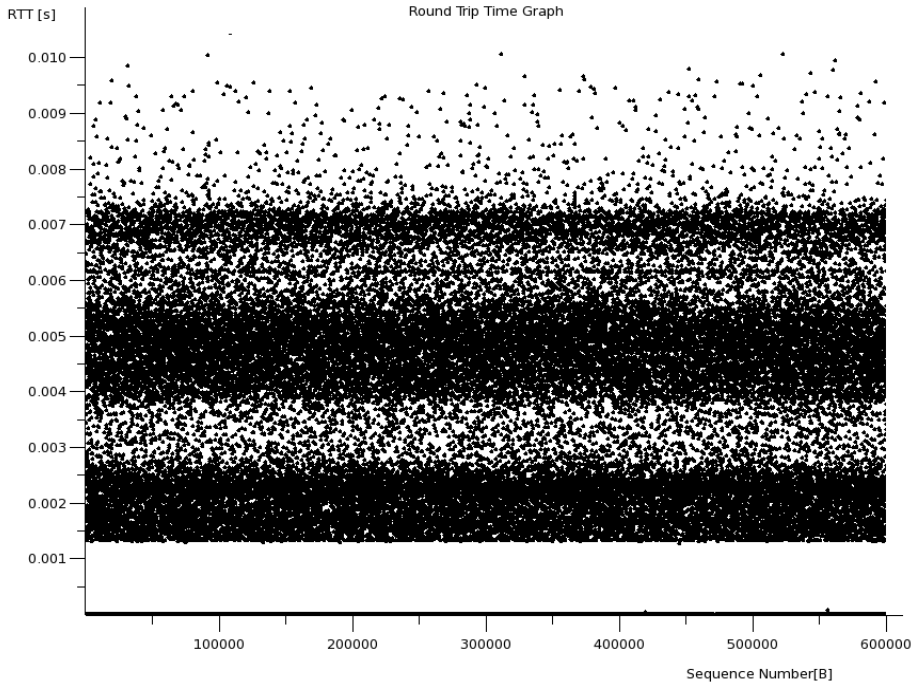
- RTT and TCP Time-sequence graphs for the two testbeds were plotted with Wireshark
- We plotted graphs for a malicious-traffic free Modbus/TCP communication to use as reference
- We plotted graphs for Modbus/TCP communications affected by the traffic of several IT common threats
- The comparison of these graphs with the reference ones can clearly show the influence of malicious traffic over Modbus/TCP communications

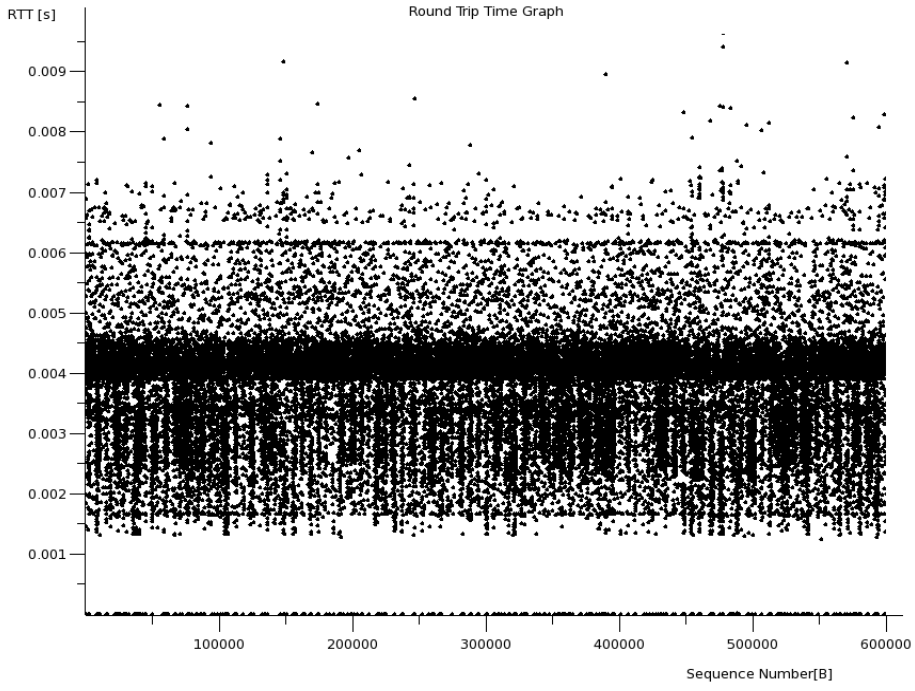
Experiments and Results - Testbed 1



- This testbed represents a case where a infected Modbus/TCP client communicates with the server

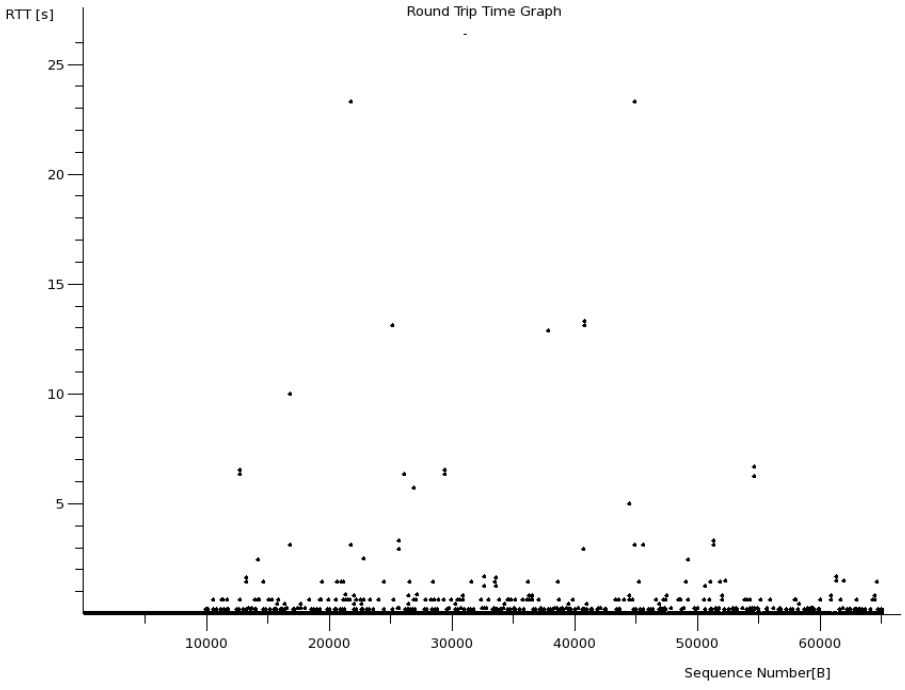
Experiments and Results - Testbed 1

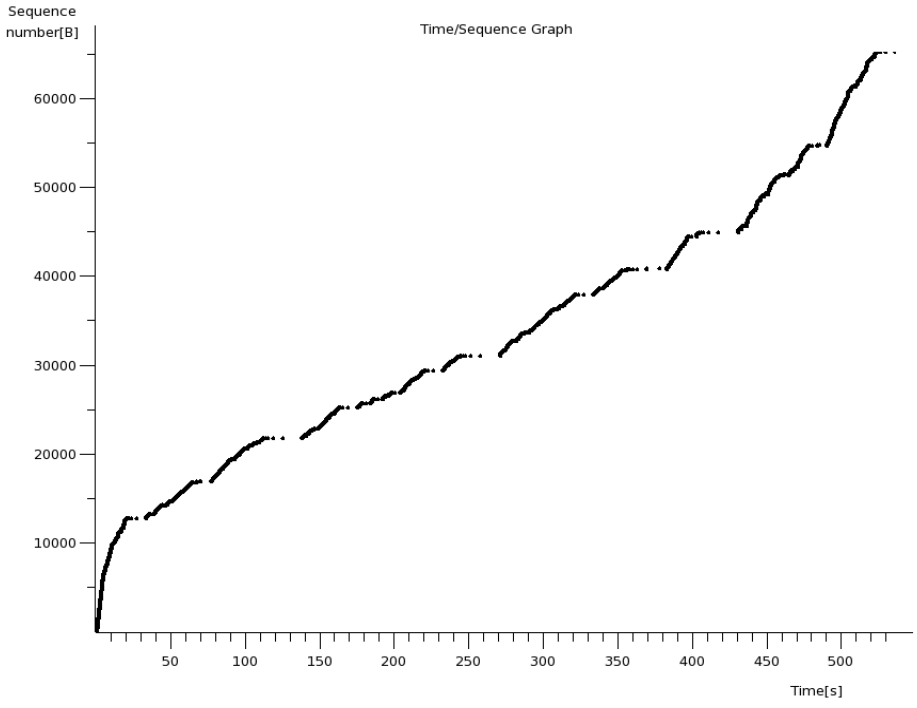




- RTT graph for a malicious-traffic free Modbus/TCP communication
- RTT graph for a Modbus/TCP communication influenced by Blaster worm traffic

Experiments and Results - Testbed 1



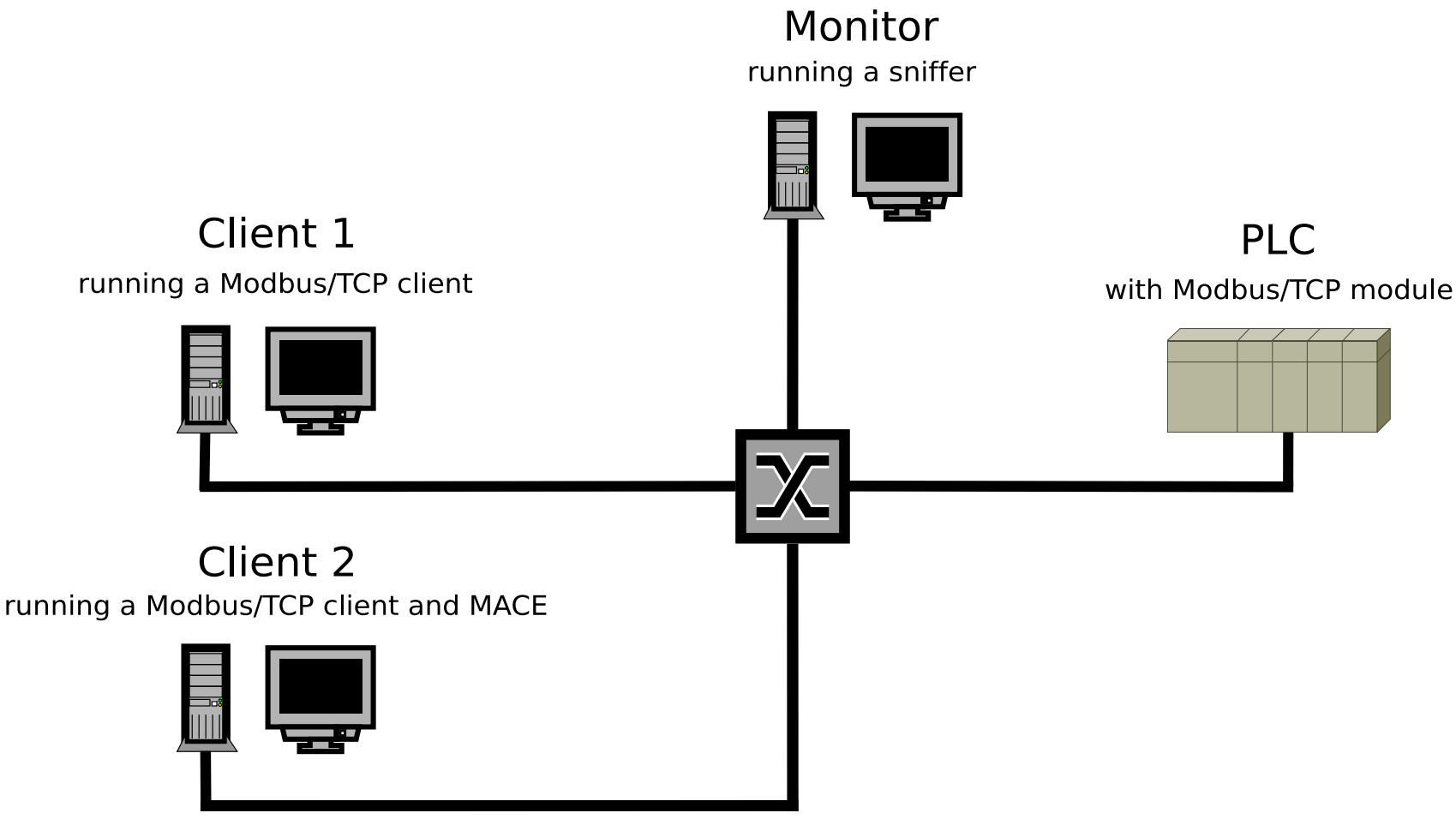


- RTT graph for a Modbus/TCP communication influenced by traffic of 21 common threats
- TCP Time-sequence graph for a Modbus/TCP communication influenced by traffic of 21 common threats

Experiments and Results - Testbed 1

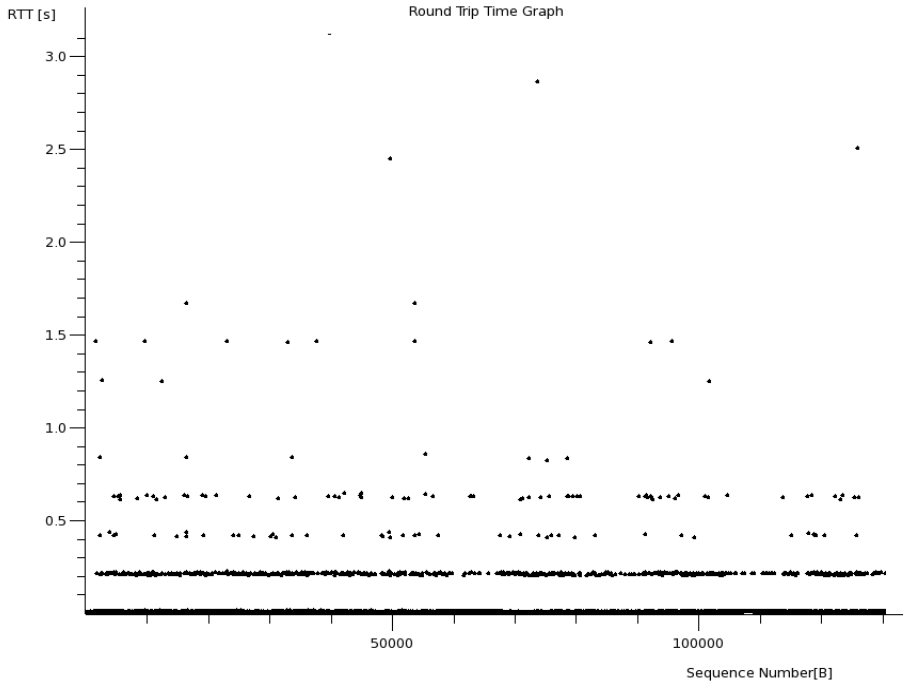
- We analysed the influence of IT malicious traffic generated by the client over its own connection with the server
- RTT graphs showed the latency increase
- TCP Time-sequence graph showed that there were delays on TCP segments despatch

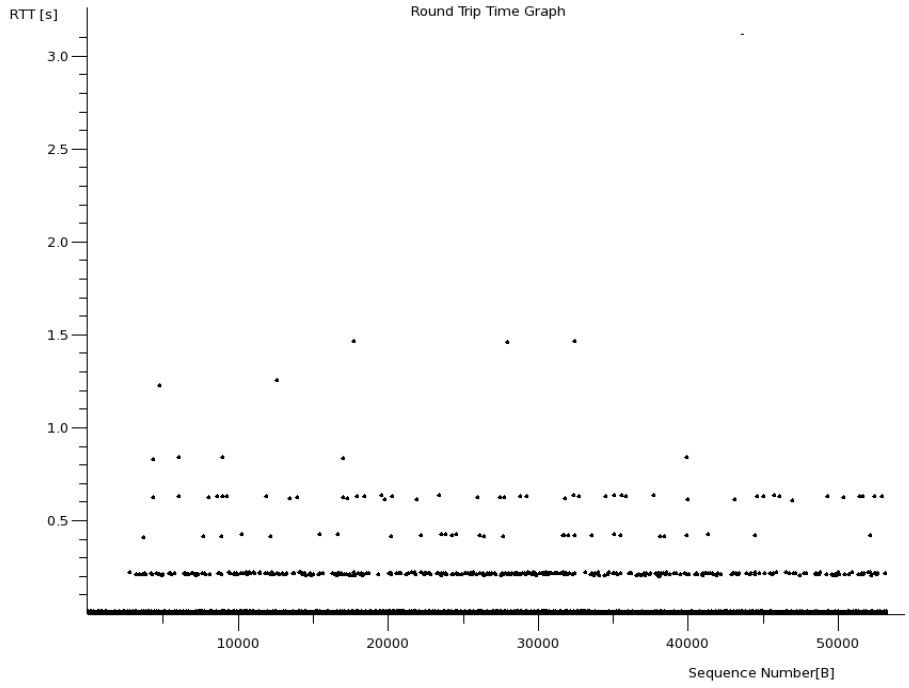
Experiments and Results - Testbed 2



- Two clients communicate with Modbus/TCP module, but one of them injects malicious traffic in the network

Experiments and Results - Testbed 2

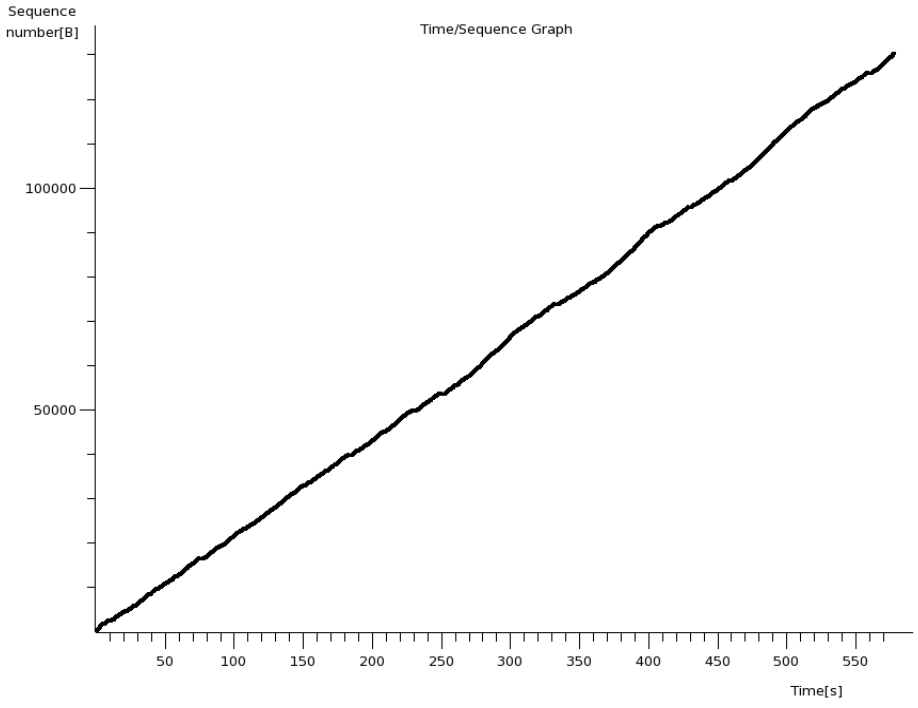


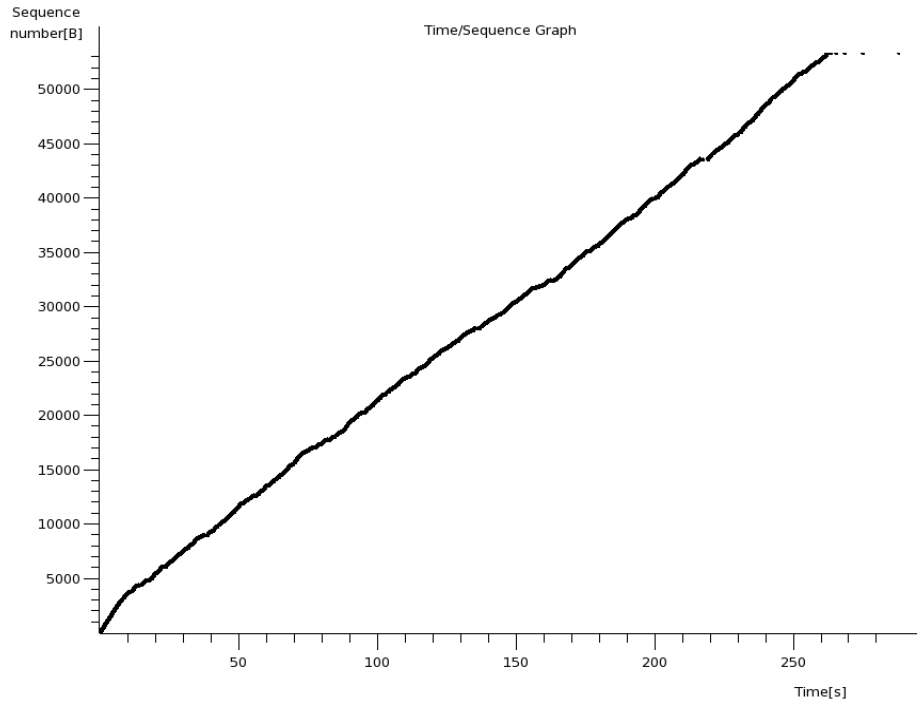


- RTT graph for a Modbus/TCP communication with Client 1 when Client 2 injects the oshare attack traffic in the network

- RTT graph for a Modbus/TCP communication with Client 1 when Client 2 injects 20-threat traffic

Experiments and Results - Testbed 2





- TCP Time-sequence graph for a Modbus/TCP communication with Client 1 when Client 2 injects oshare traffic in network

- TCP Time-sequence graph for a Modbus/TCP communication with Client 1 when Client 2 injects 20-threat traffic

Experiments and Results - Testbed 2

- We analysed the influence of the malicious traffic generated by a client over the connection of another
- The RTT graphs showed that the threats increase latency in the communication between Client 1 and Modbus/TCP module
- TCP Time-sequence graphs showed the delays in the despatch of TCP segments by Client 1 caused by malicious traffic injected by Client 2
- Some threats alone can be as harmful as a set of other threats
- The Modbus/TCP PLC module got out of communication in some tests

Final Considerations

- This work presented an analysis of IT malicious traffic influence in Modbus/TCP networks
- We show how harmful IT malicious traffic can be to AT networks
  - Major performance degradation of communications (latency increase)
  - Some threats can put devices out of communication (DoS)
- The utilization of security countermeasures can avoid this influence of malicious traffic in AT networks
  - Firewalls
  - VPN

Contact

hiroshi@dca.ufrn.br