SAPIENTIA
HUNGARIAN UNIVERSITY
OF TRANSYLVANIA

CYBERATTACK DETECTION AND COMPENSATION FOR DISTANT-CONTROLLED MOBILE ROBOTS

Lehel Nagy, Lőrinc Márton

CINTI 2020
20th IEEE International Symposium on
Computational Intelligence and Informatics
November 5-7, 2020

OUTLINE

- Introduction
- Cyberattack Compensation Algorithm Design
- General System Description
- Software Implementation
- Measurements
- Conclusions

MOTIVATION

- In such industry brunches that apply distant-controlled mobile robots, cyber security has become an increasingly urgent issue, in such security-critical areas as transportation, military or health-care.
- In the case of a DoS (Denial of Service) attack the attacker overloads the communication channels of the networked control system by sending a high amount of extra communication packets.
- If this type of attack hits the system, the operator will no longer be able to monitor the robot's data and the robots will not be able to receive commands, which could even lead to a collision or other physical damages.

MOTIVATION

- The goal of this research is to develop and implement a resilient control algorithm that minimizes the effect of a DoS attack on the controlled motion of distant-controlled mobile robots.

CYBERATTACK COMPENSATION ALGORITHM DESIGN

- In the case of *Move and Wait* remote robot control strategy, the communication packets containing motion commands (such as prescribed speed), are sent to the remote robot repeatedly.
- The proposed resilient control approach must be able to *detect when the system is hit by a DoS attack*, it must recognize the severity of the attack.
- It has to *modify the sent robot command parameters*. During command execution, the robot must be able to receive new command packets as well and, if the new packet contains a different instruction, it must be able to overwrite the previous one.

CYBERATTACK COMPENSATION ALGORITHM DESIGN

- If the attack is detected, the *activity period will be increased*. The increase will be proportional to the attack magnitude. It is because if an attack occurs, the communication lag increase could lead to stop-go cycles in the robot's motion.

- If the attack is detected, the *robot velocity will be decreased*. The decrease will be proportional to the attack magnitude.

CYBERATTACK COMPENSATION ALGORITHM DESIGN

Measurement:

$$PDV\ [k] = |\Delta t[k] - \Delta t[k-1]|$$

- Round Trip Time (Δt)
- Packet Delay Variation (PDV)

CYBERATTACK COMPENSATION ALGORITHM DESIGN

Detector:

$$e\,[k] = \frac{Tf}{Tf + \Delta t[k]}\,e\,[k-1] + \frac{\Delta t[k]}{Tf + \Delta t[k]}\,PDV\,[k]$$

- e - filtered PDV value
- $T_f > 0$ - filter parameter

CYBERATTACK COMPENSATION ALGORITHM DESIGN

- Activity period computation: $\Delta t[k] = \alpha(e[k])\Delta t_0$

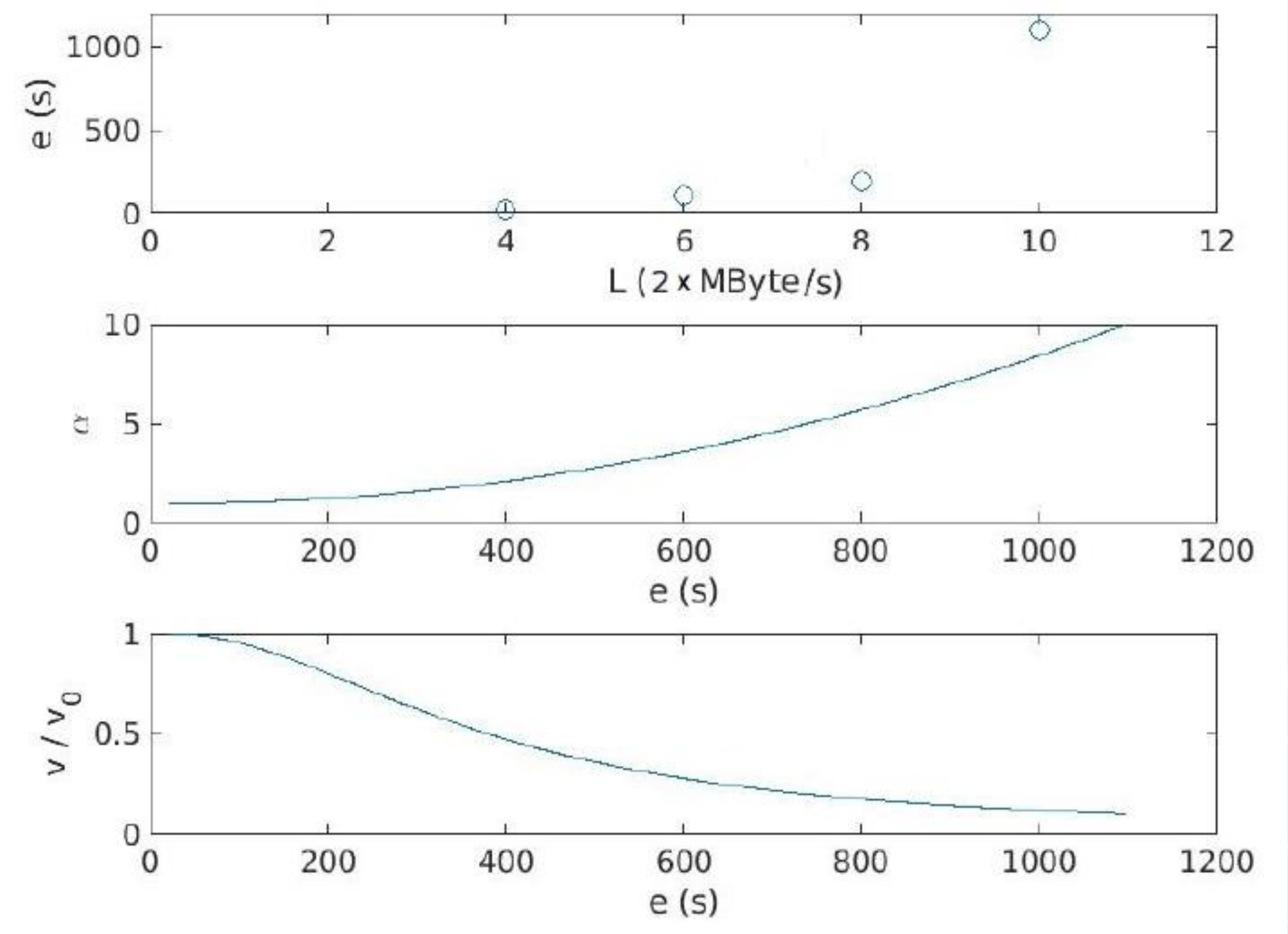
- Velocity computation: $v[k] = \frac{\alpha v}{\alpha(e[k])} v_0[k]$

- To catch the nonlinear characteristic of the cyberattack, consider that the gain function can be approximated by a second order polynomial:

$$\alpha(e) = ae^2 + be + c$$

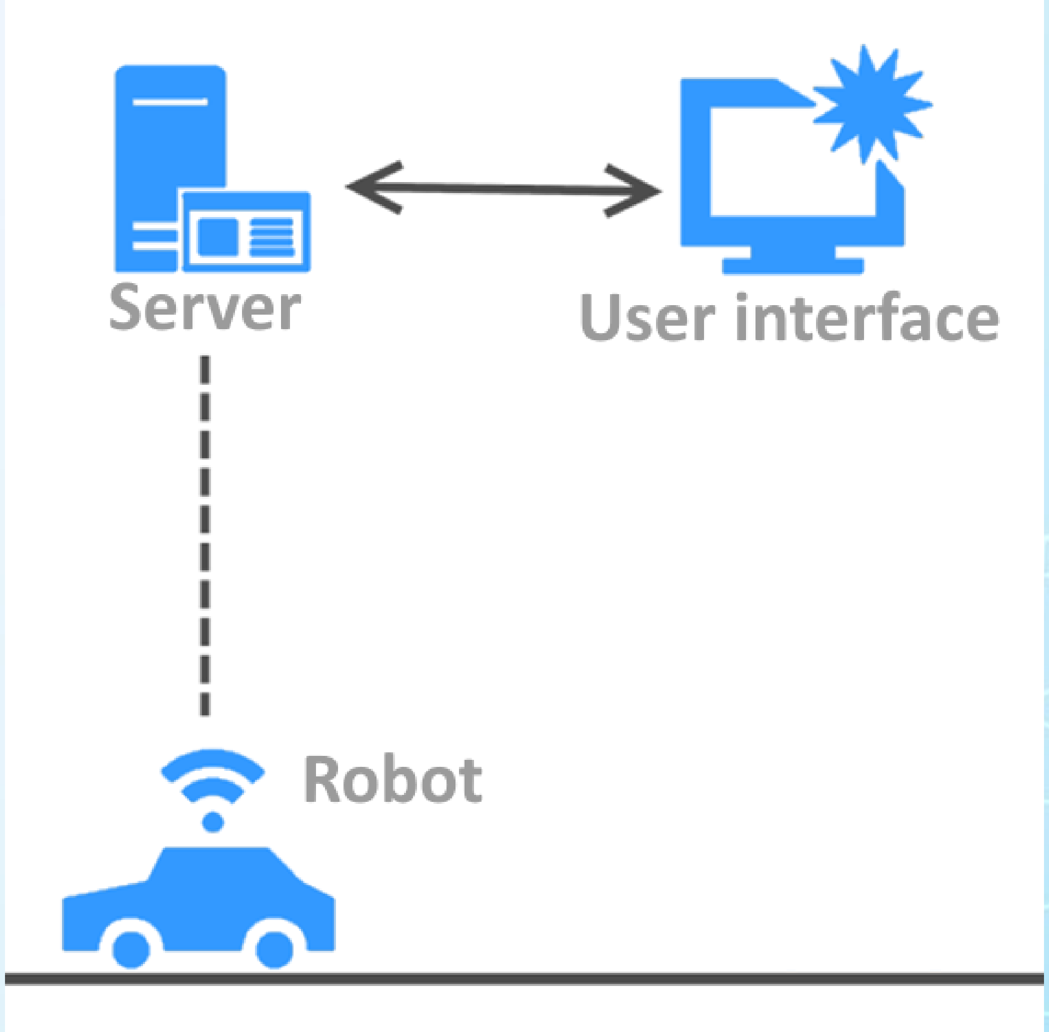
$$\text{where } \alpha(e_M) = \alpha_M, \alpha(e_0) = 1, \dot{\alpha}(e_0) = 0$$

Measurements for compensation algorithm calibration



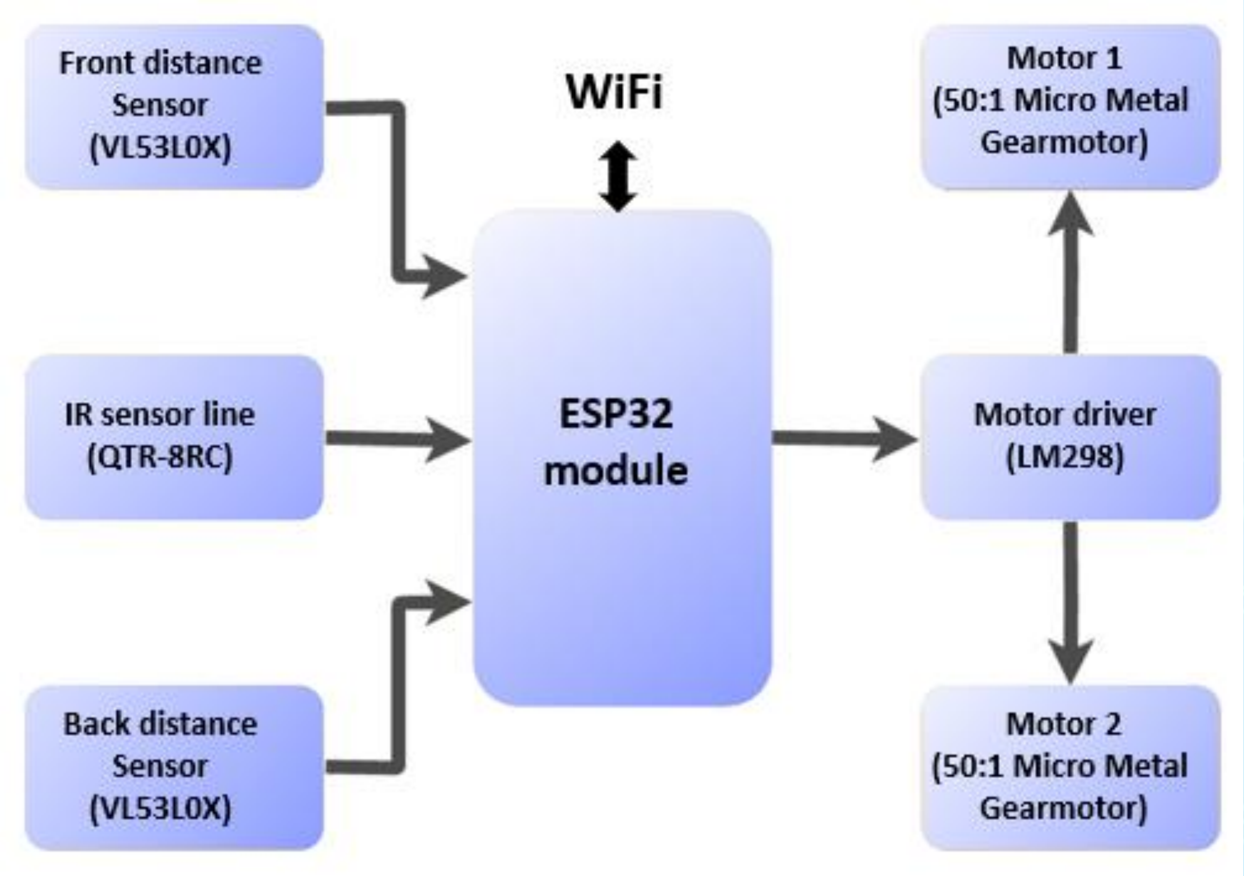
GENERAL SYSTEM DESCRIPTION

- The robot control system consists of a mobile robot equipped with an embedded system that maintains a wireless connection to a server.
- The server runs on a personal computer.
- Through the server, the operator sends the motion commands to the robot by applying the Move and Wait strategy and it receives back robot sensor data.

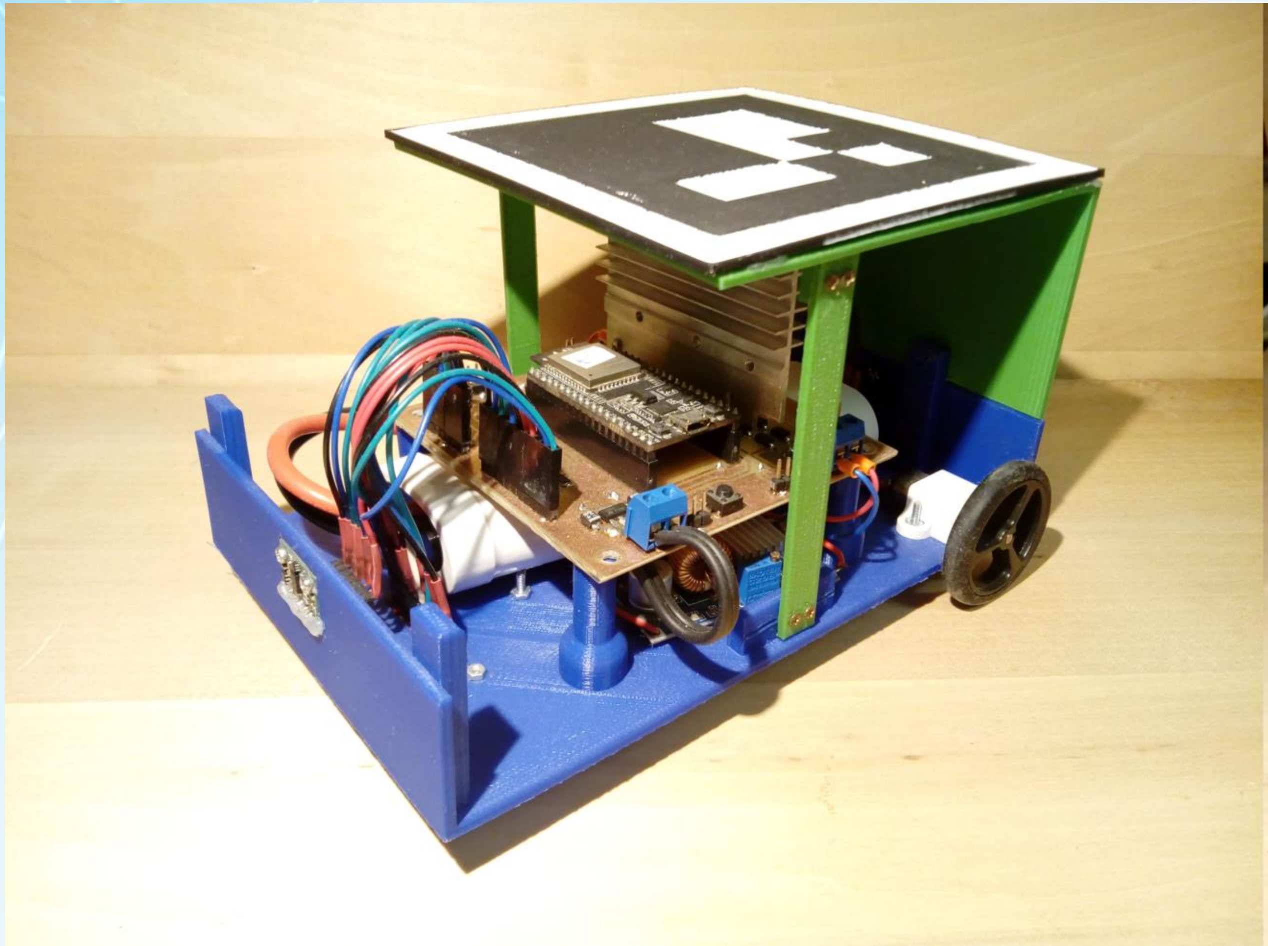


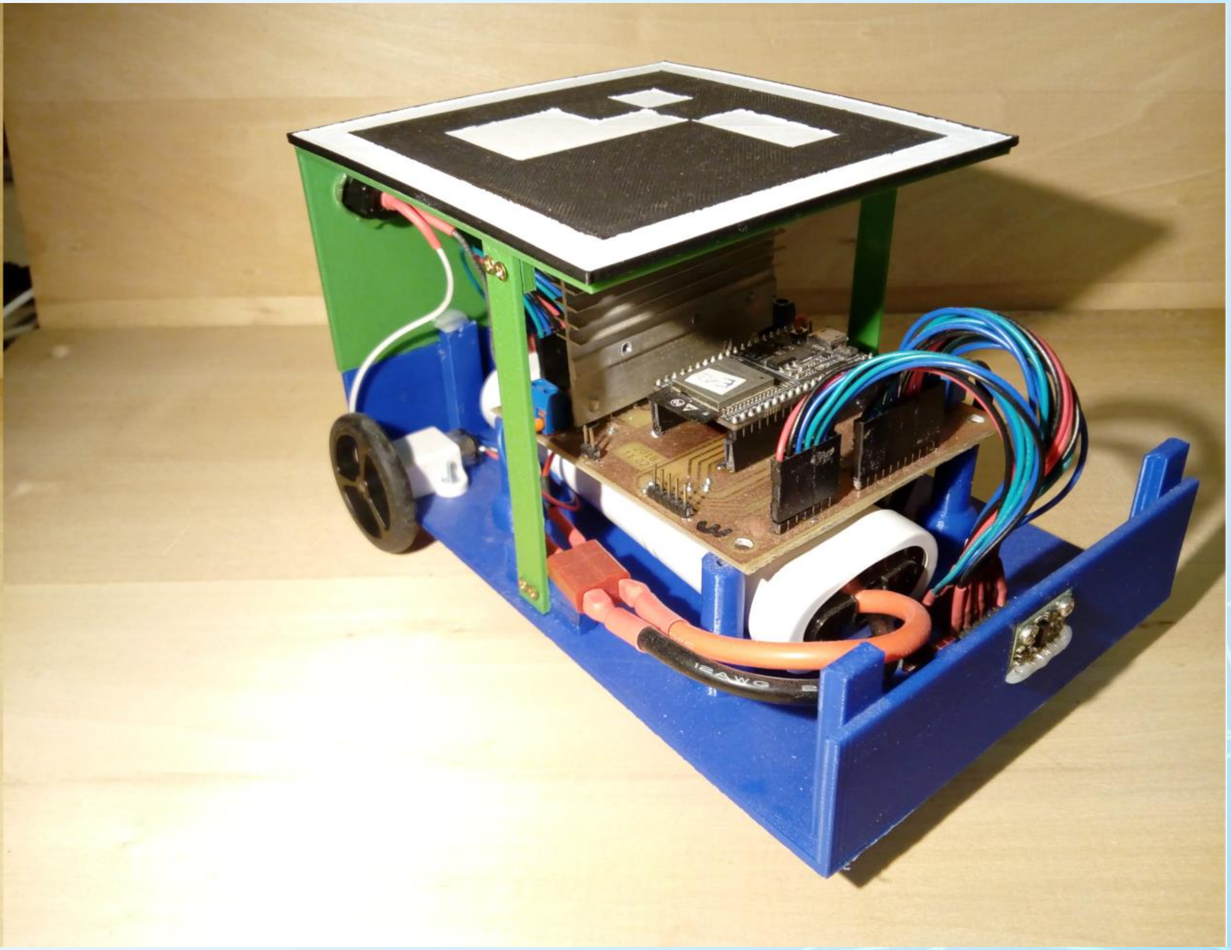
GENERAL SYSTEM DESCRIPTION

- ESP32 MCU (MicroController Unit)
- 3500mAh Nickel Metal (NiMH) battery
- Micro Metal motors with a 50: 1 ratio
- 3D printing technology
- ArUco code (indoor positioning)
- Laser based distance sensor


Front distance Sensor (VL53L0X)
IR sensor line (QTR-8RC)
Back distance Sensor (VL53L0X)
WiFi
ESP32 module
Motor 1 (50:1 Micro Metal Gearmotor)
Motor driver (LM298)
Motor 2 (50:1 Micro Metal Gearmotor)

GENERAL SYSTEM DESCRIPTION



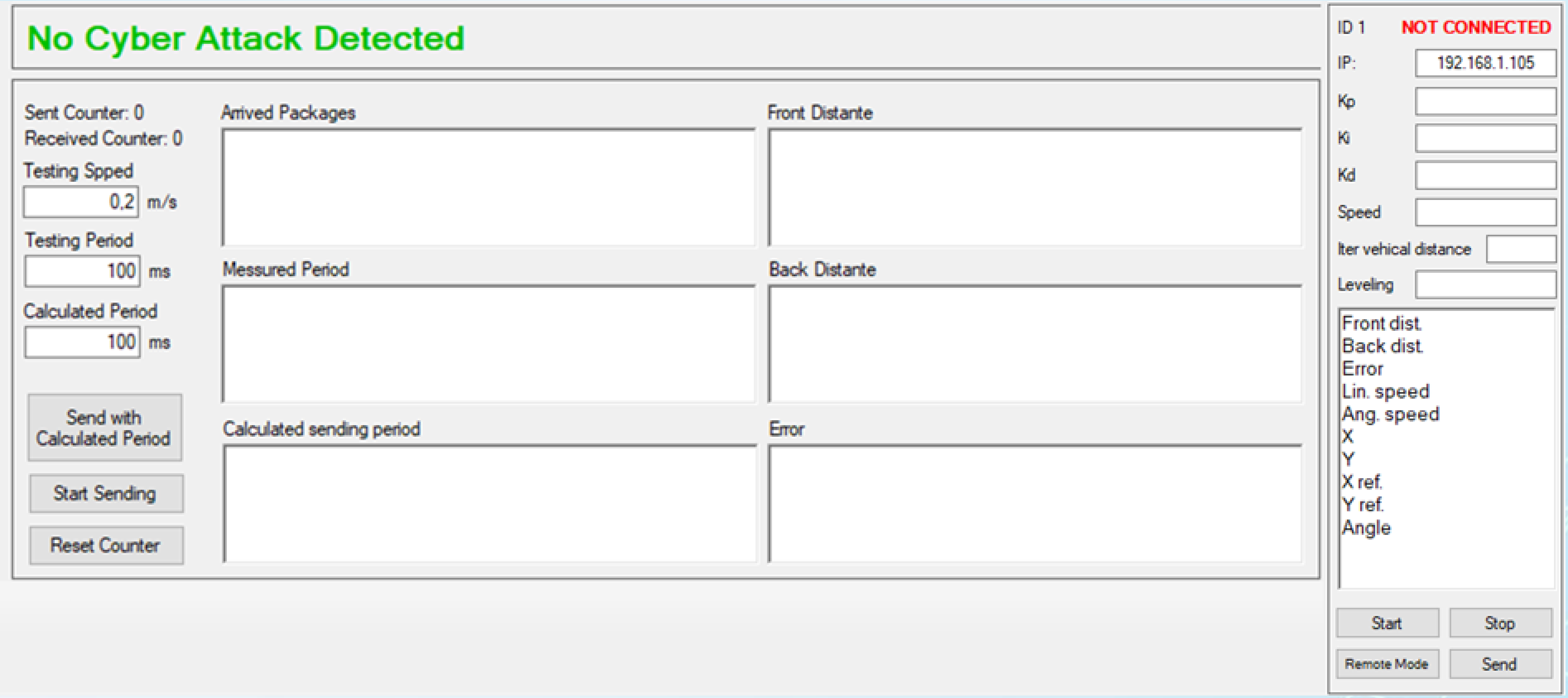


SOFTWARE IMPLEMENTATION

- Receiver
- Cyberattack Detector
- Cyberattack Compensator
- Sender
- User interface

SOFTWARE IMPLEMENTATION

User interface:



No Cyber Attack Detected

Sent Counter: 0

Received Counter: 0

Testing Spped 0,2 m/s

Testing Period 100 ms

Calculated Period 100 ms

ID 1 NOT CONNECTED

IP: 192.168.1.105

Kp

Ki

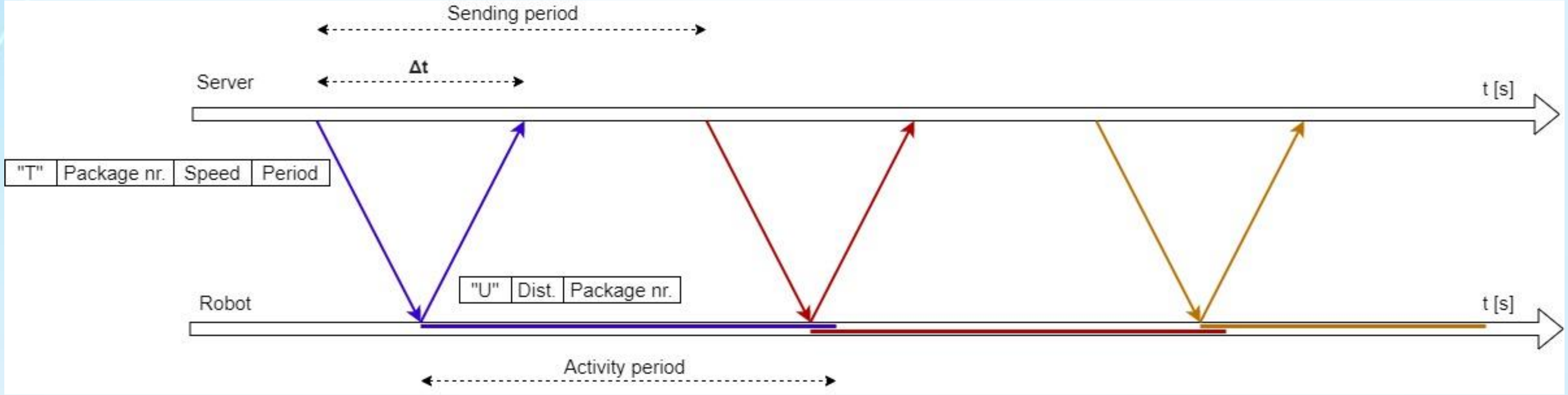
Kd

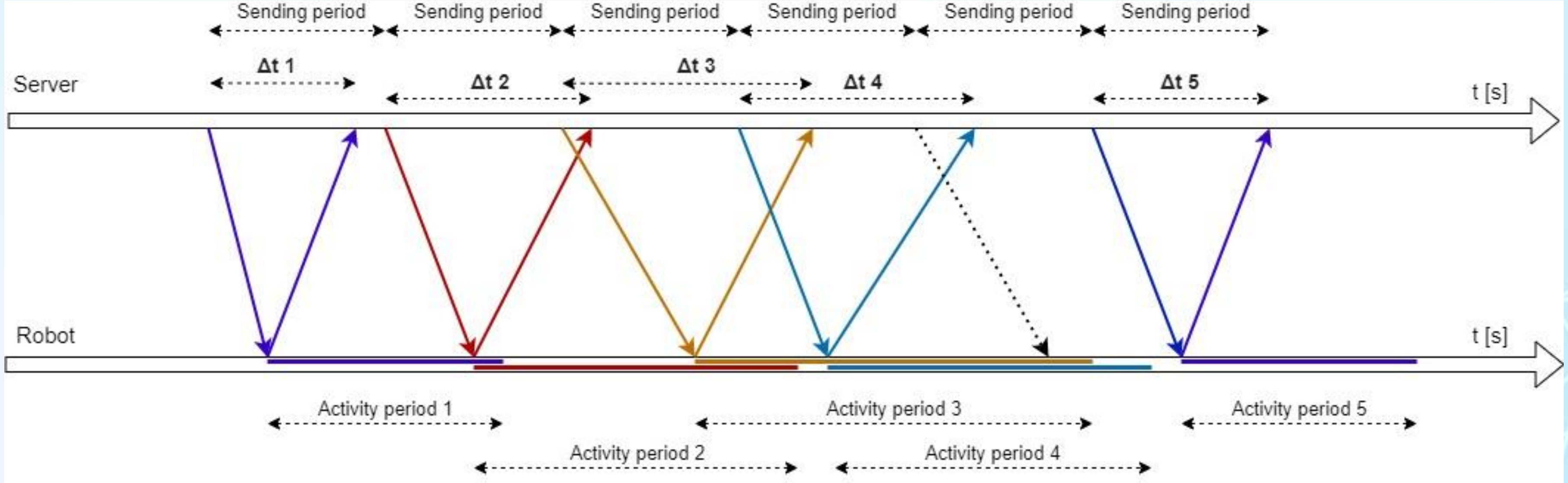
Speed

Iter vehical distance

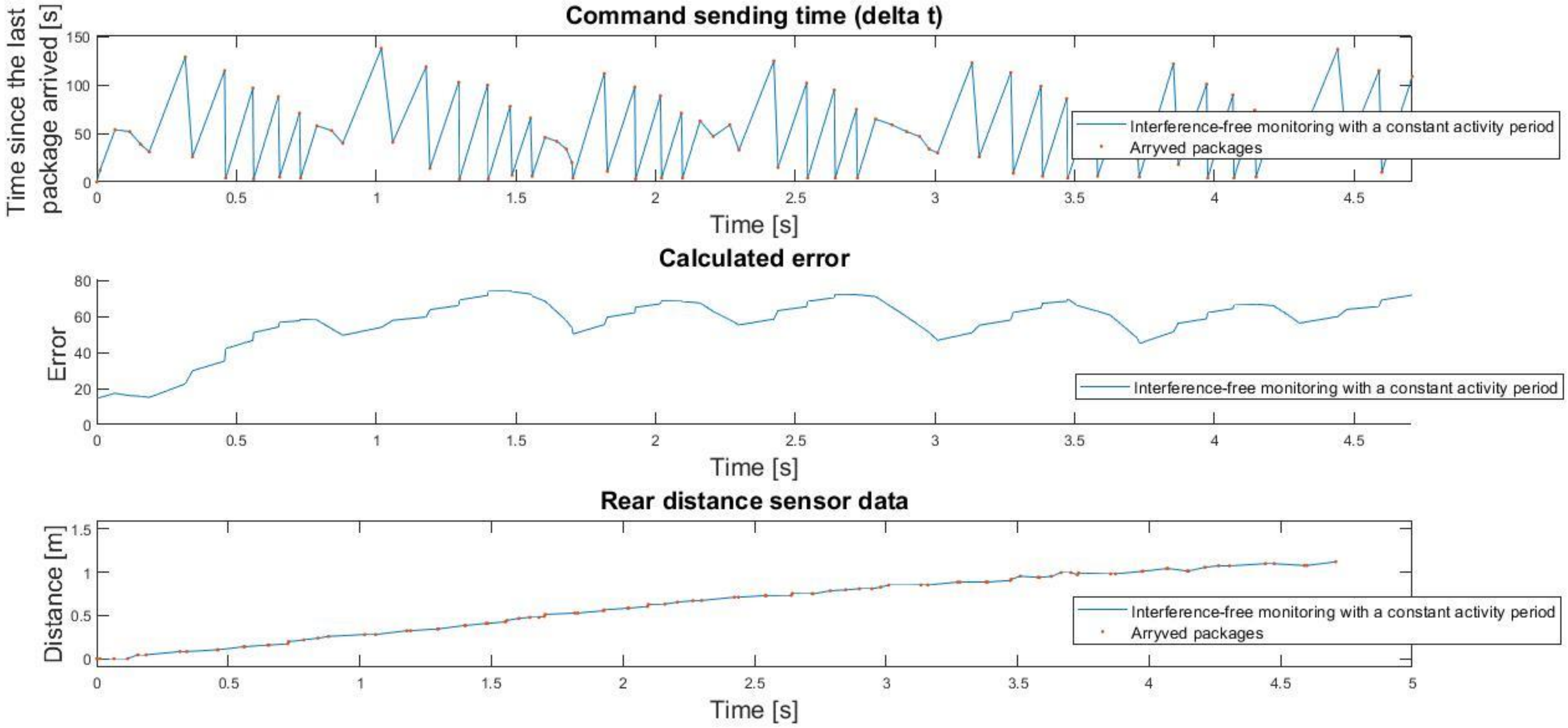
Leveling

COMMUNICATION DIAGRAM

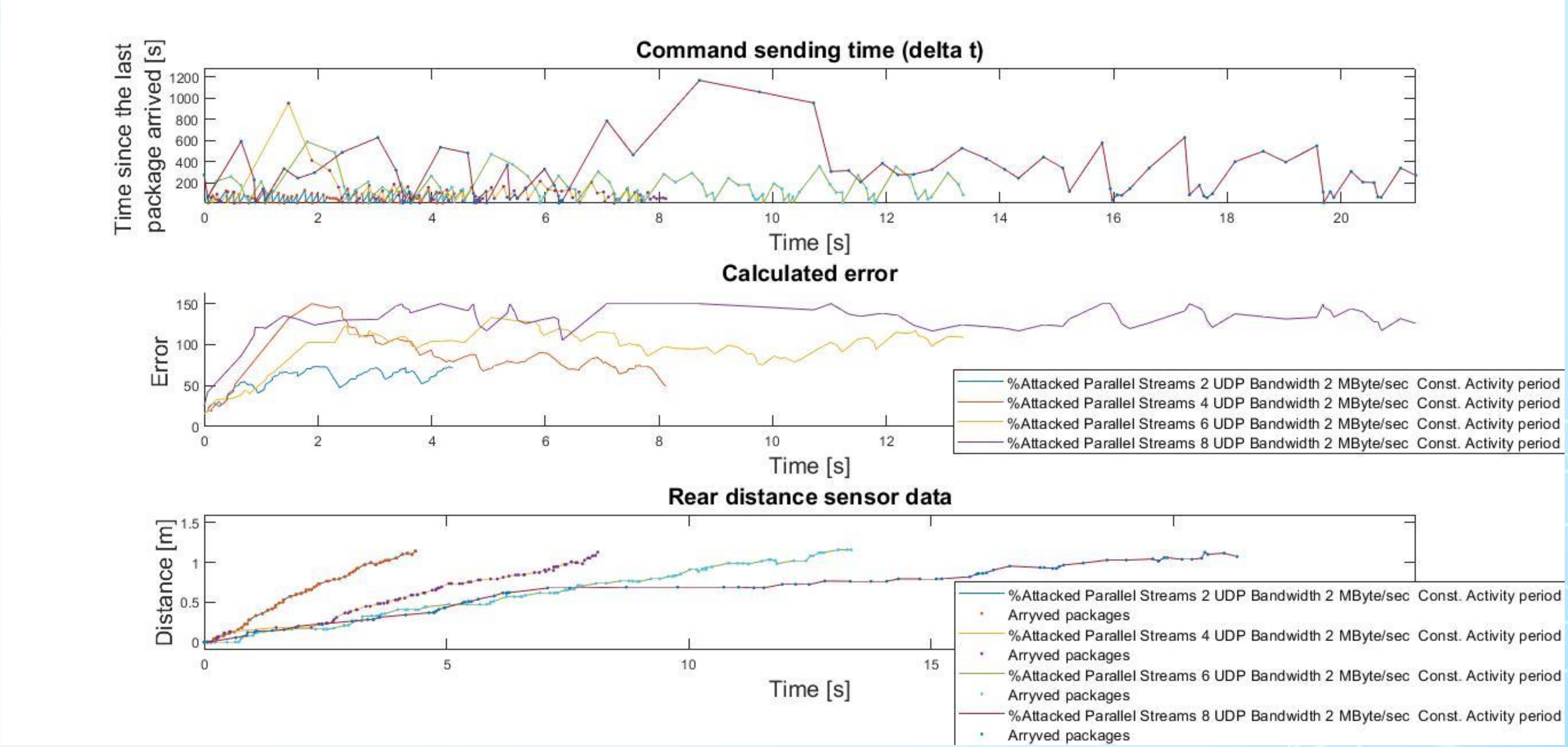




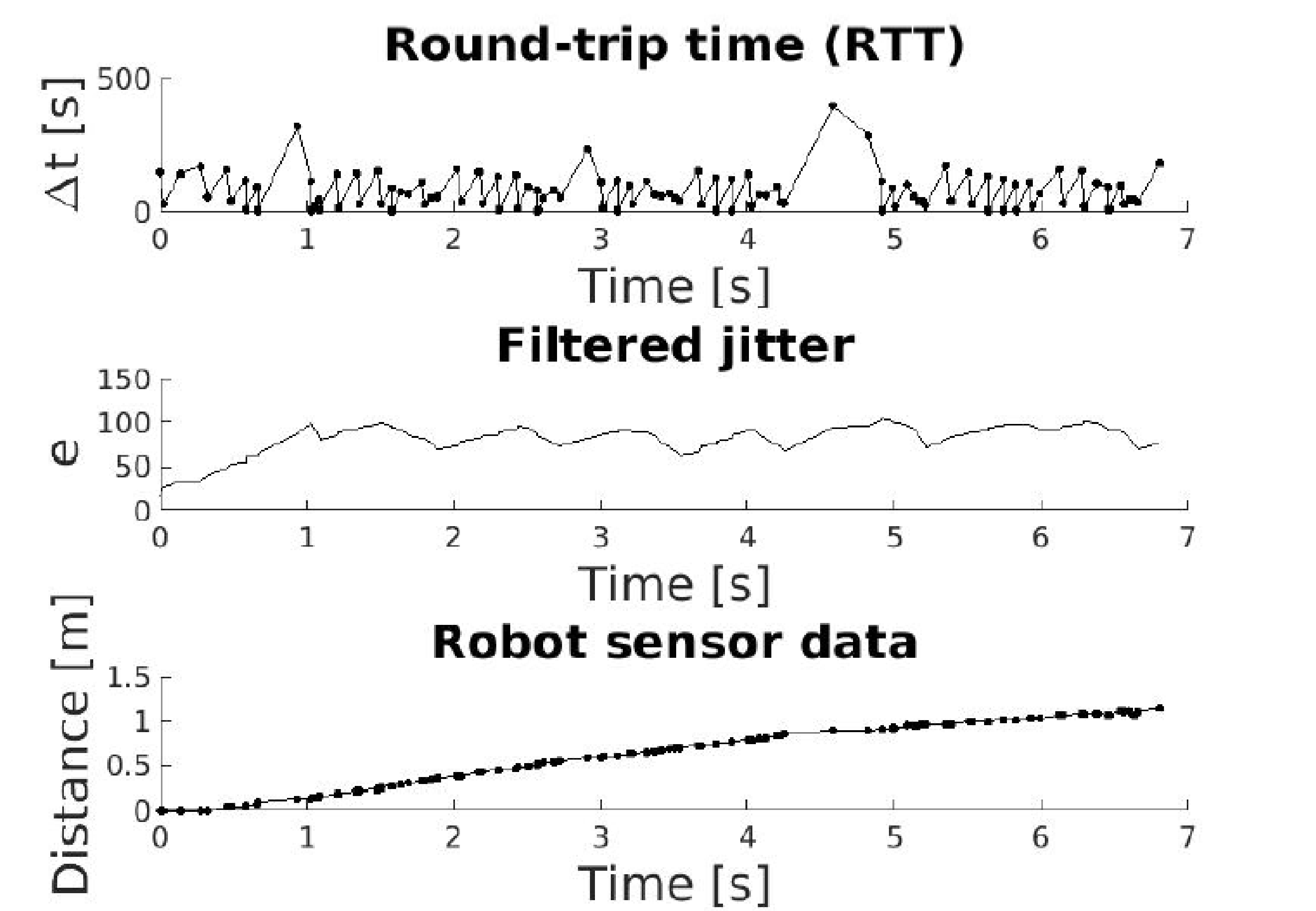
Measurements: No Attack Case



Measurements: Attacks Without Compensation



Measurements: Attacks With Compensation



CONCLUSIONS

- When distant-controlled robot systems are exposed to such cyberattacks that block the communication among the networked control system components. various network congestion methods can cause the robots to move intermittently, the connection between the robot and the operator could be temporarily lost, the robot motion could become intermittent.
- In this work, it was presented that, based on communication performance measurements, such as filtered jitter, the presence and the magnitude of the cyberattack can be detected.
- The proposed cyberattack compensator uses this communication parameter measurements and, based on this information, modifies the robot commands such as the speed and the activity period.
- Real-time experimental measurements indicate that with the proposed resilient distant control approach the robot is capable of detecting the presence of a cyberattack, and it can continuously operate even during a cyberattack.

SAPIENTIA
HUNGARIAN UNIVERSITY
OF TRANSYLVANIA

THANK YOU
FOR YOUR ATTENTION!

CINTI 2020
20th IEEE International Symposium on Computational Intelligence
and Informatics
November 5-7, 2020