CIRI | CRITICAL INFRASTRUCTURE RESILIENCE INSTITUTE

A DEPARTMENT OF HOMELAND SECURITY CENTER OF EXCELLENCE

Anomaly Detection on Raven II Surgical Robot

Uchenna Ezeobi, Key-whan Chung, Zbigniew Kalbarczyk

Introduction

- Improve resiliency (reliability and security) of teleoperated surgical robots
- Minimize patient injuries and/or death accidents caused by accidental system failures and malicious tampering with surgical robots by attackers
- Demonstrate the following on the Raven II
  - Use of fault injection to mimic operational failures
  - Develop an algorithm for preemptive detection of failures

Problem

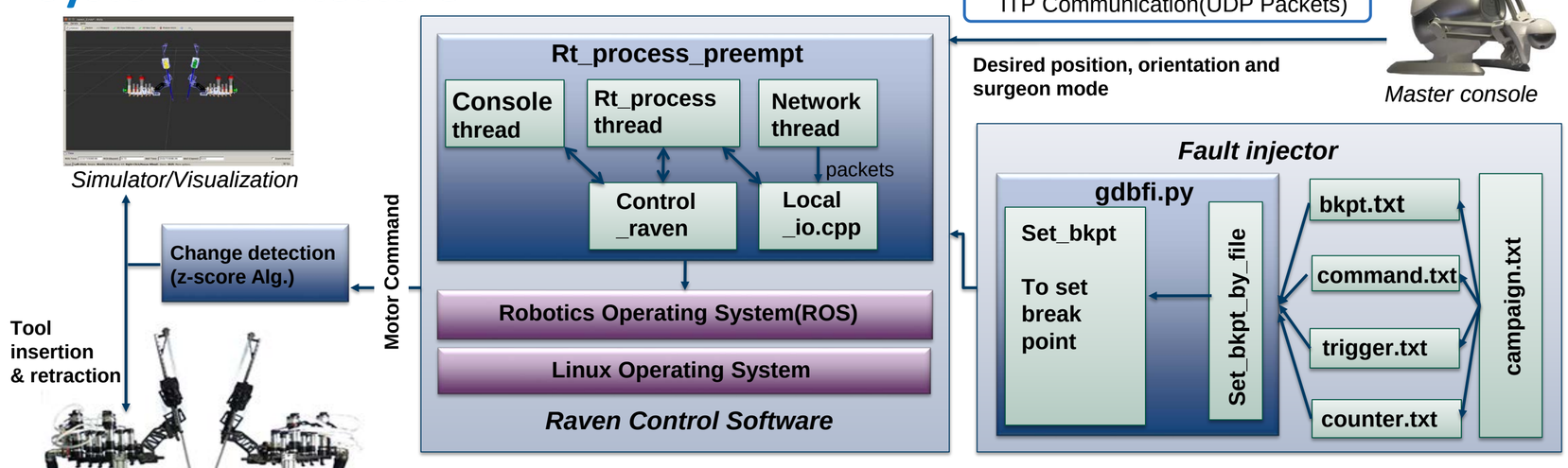
- Raven II is an open source tele-operated surgical robot designed to support research in advancing techniques of robot-assisted surgery
- According to the study done on FDA(U.S food and drug administration) data (2000 ~ 2013):
  - 144 deaths (1.4 % of the 10624 reports)
  - 1391 patients injuries (13.1%)
  - 8061 device malfunctions (75.9%)

  in robot-assisted surgery
- Improved resiliency can reduce deaths, injuries and device malfunctions

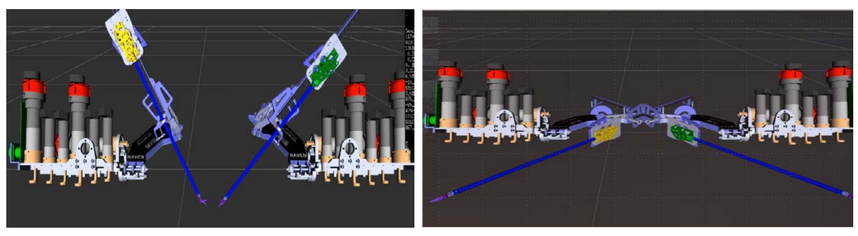
Approach

- Monitor a critical parameter of the robot:
  (i) elbow joint position
  (ii) shoulder joint position
  (iii) digital to analog (DAC) sent to the controllers
- Model the parameters as independent quantities and use a change detection alg. to monitor abrupt jump
- Use a moving mean & std. to detect deviation from expected range of arm position

System Architecture



Fault Injection Simulation

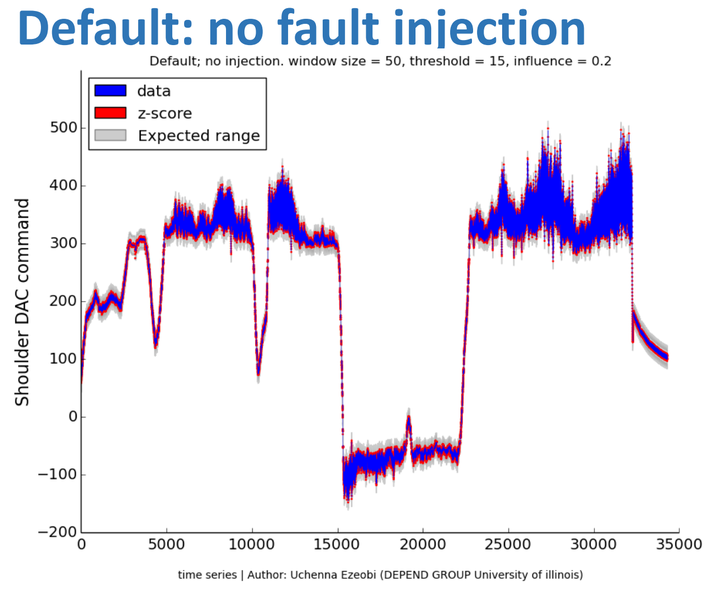


No Injection: arm position normal **Fault Injected**: abrupt jump

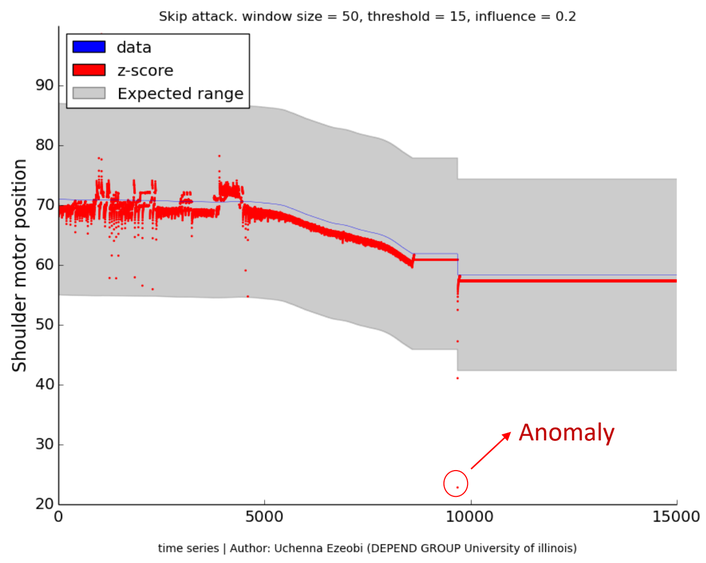
Results: Fault Injection / Detection

Fault injection	Description of Attacks	Degree of variation	Malicious Effects	Dyn. sim. detection	Z-score detection
Delay packets attacks	Incoming packets from the master console are delayed in the network layer by choosing a range of packets within a sequence number to be delayed	Small sequence delay range	No observed effect on robot or significant jump	✗	✗
		Large sequence delay range	Jump, IK fails, Skipped packets	✓	✓
Skip packets attack	Incoming packets from the master console are international skipped in the network layer within a certain sequence number range by setting the sequence number to 0.	Small seq. skip range	Small jump in the robot	✗	✓
		Large seq. skip range	Large jump in the robot, IK fails	✓	✓
Change desired position attack	Change the desired position of the robot arm in the network layer	Small position	No observed effect in the robot or significant jump in the robot	✗	✗
		Large position	Jump in the robot.	✗	✓
Change DAC command attack	Change the DAC command(digital to analogy converter command sent to the motor controller) in the rt_process layer	Small seq. range	Jumps the joint of the robot	✗	✓
		Large seq. range	Jumps the joint of the robot.	✓	✓
Change rotational matrix attack	Change the orientation of the robot	small rot. Mat.	Small jumps to the joint	✗	✓
		Large rot. Mat.	Large jumps to the joint	✓	✓

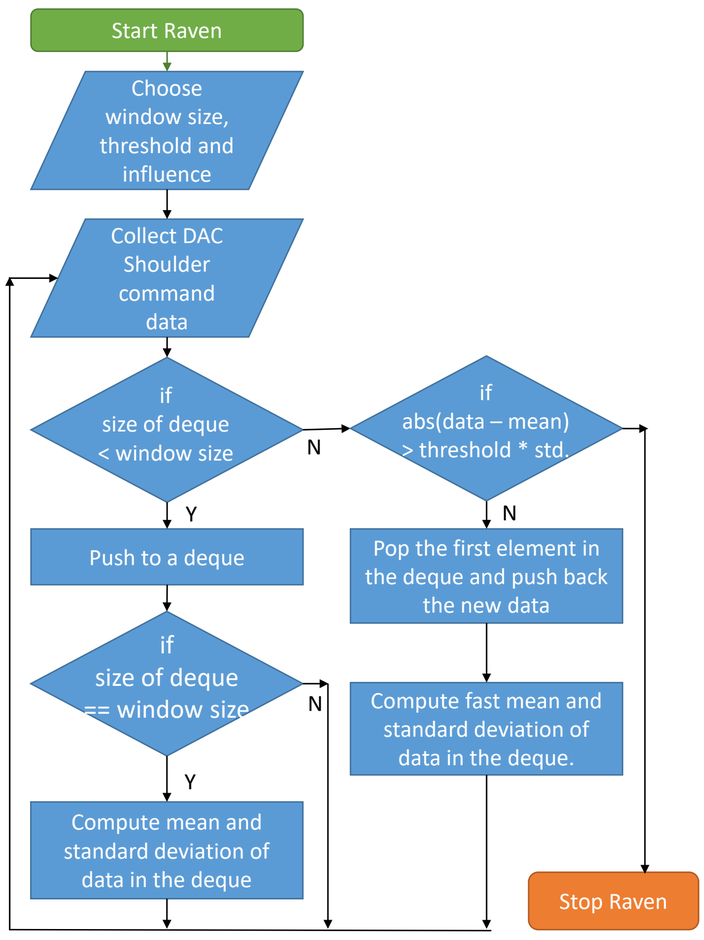
Default: no fault injection



Skip (Network) Packets



Change Detection: Z-score Alg.



Evaluation: Detection Accuracy

Detection Algorithm	True Positive Ratio (%)	False positive ratio (%)	F1-score
Dynamic Simulation	89.8	12.4	74.8
Z-score Algorithm (thres = 10)	90	0	64.28

Future Work

- Show an effective way of selecting threshold, influence and window size.
- Application of anomaly detection framework to other Teleoperated Surgical robots.

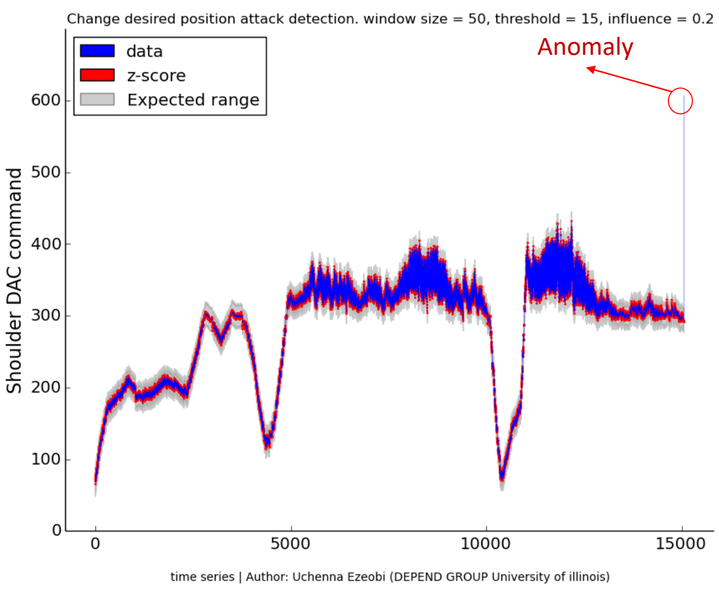
Conclusion

- Security is a significant issue within surgical teleoperated robots
- **Change detection algorithm** can help improve resiliency of Surgical robots
  - Improved detection accuracy
  - Keep the timeliness

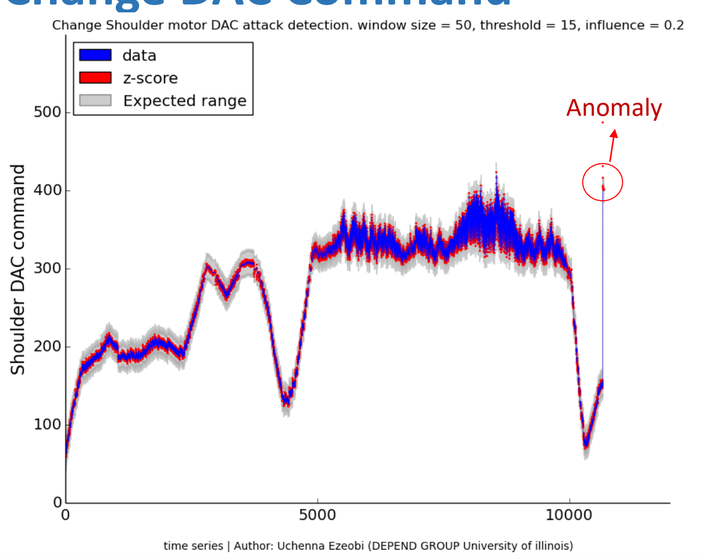
References

[1] H. Alemzadeh, D. Chen, Z. Kalbarczyk, R. Iyer, X. Li, T. Kesavadas, and J. Raman, "A software framework for simulation of safety hazards in robotic surgical systems," 05 2015.

Change in Desired Position



Change DAC Command



*This material is based upon work supported by the **U.S. Department of Homeland Security** under Grant Award Number, 2015-ST-061-CIRC01.*