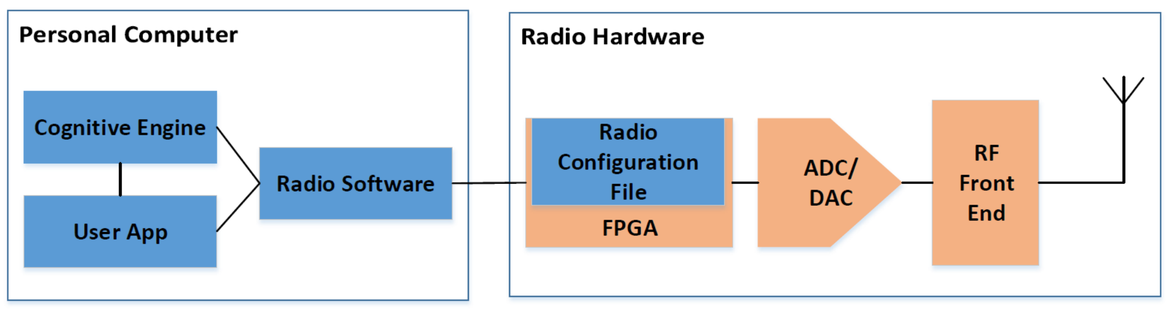
Correlation-based Malware Detection for Cognitive Radio Networks

Yanzhi Dou, Ph.D. Student
Advisor: Dr. Yaling Yang

Introduction:

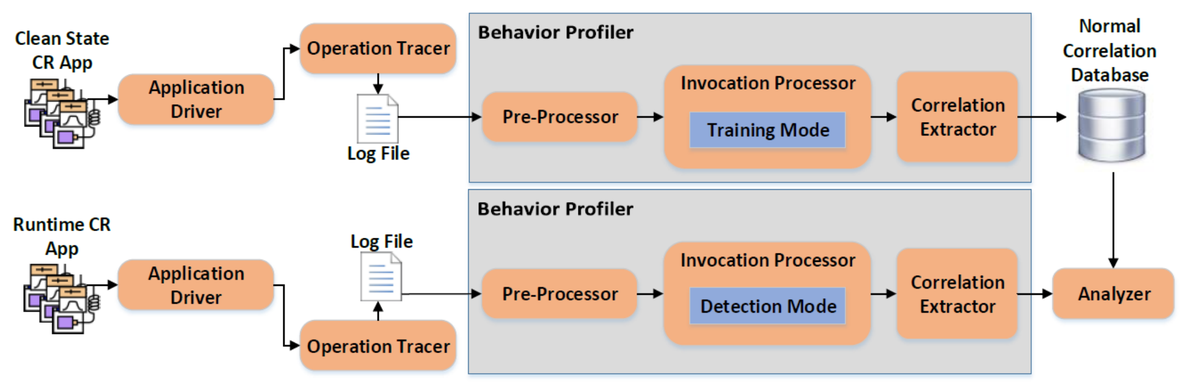
- Flexibility of CR introduces challenging security and information assurance issues.
- Existing proposals for CR security all have their limitations.
- We propose a new mechanism, called *CoMDCR,* to enhance the security of CR device itself by monitoring CR applications' behaviors.



Attack Model:

Malicious modification to CR software during download, initialization, and runtime.

System Design

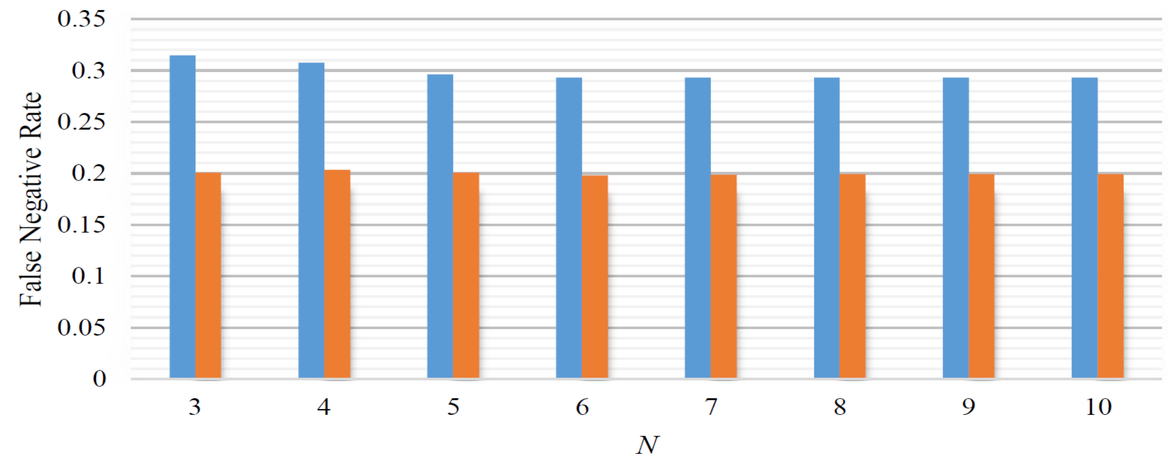


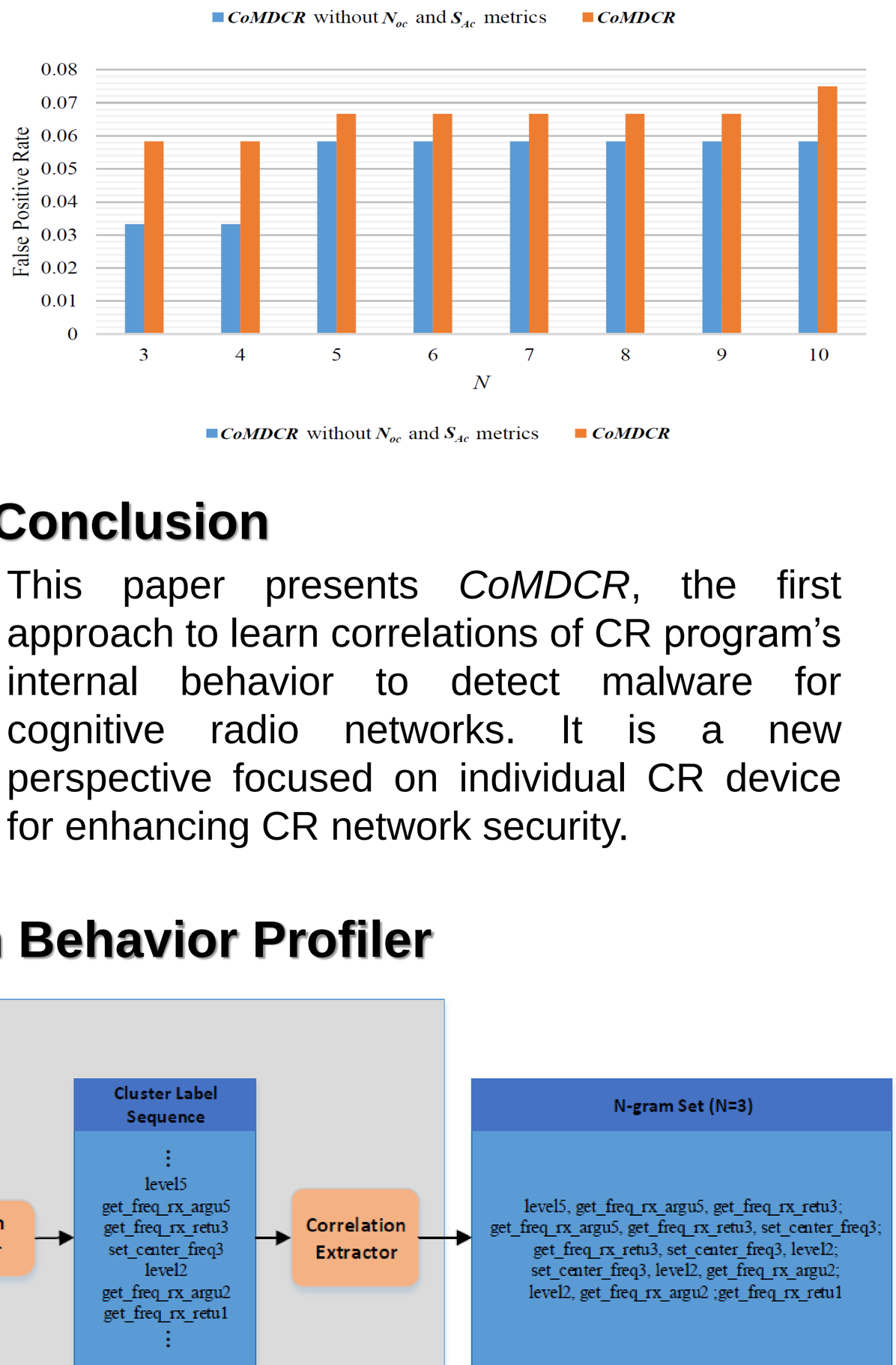
Evaluation Method

- A lack of real malware cases in the field.
- Adopt mutation testing techniques to artificially generate malware-infected versions of CR application programs.

Mutation Operator	Original Number	Processed Number	Description
JMP	92	74	Reverse Jump Condition
JPT	476	460	Randomize Jump Target
VAR	462	449	Change Variable Value
ARI	799	734	Replace Arithmetic Operator
CMP	308	231	Replace Comparison Operator

Prototype & Evaluation





Conclusion

This paper presents *CoMDCR*, the first approach to learn correlations of CR program's internal behavior to detect malware for cognitive radio networks. It is a new perspective focused on individual CR device for enhancing CR network security.

Data Processing in Behavior Profiler