Error Correction Coding in Passive UHF Gen2 Communications

CSE 4344

Charlie A. Albright
Computer Science and
Engineering Department
Southern Methodist University
Dallas, Texas USA
calbright@smu.edu

Spencer A. Kaiser
Computer Science and
Engineering Department
Southern Methodist University
Dallas, Texas USA
skaiser@smu.edu

Luke W. Oglesbee
Computer Science and
Engineering Department
Southern Methodist University
Dallas, Texas USA
loglesbee@smu.edu

1. INTRODUCTION

The purpose of this study is to explore possible error-correcting alternatives to the simple Cyclic Redundancy Check (CRC) codes used in Ultra-High Frequency (UHF) Gen2 RFID communications. We will evaluate the complexity added to the RFID system when using various types of error-correcting codes and analyze their effects on the performance of the system.

Algorithm 1.1: PACKET ANALYSIS(*Parameters*)

```
while $Packet \in File$
  do { $Prepare\ Packet$
       $Encode\ Packet$
       $CALLNoisePacket,\ Probability$
       $Decode\ Packet$
```

As of current, RFID uses Cyclic Redundancy Checks (CRC) to detect errors that happen when the information is transmitted wirelessly from Tag to Reader and from Reader to Tag. However, even if these errors are detected, the system is not able to correct the error, so the result is thrown out and another request for the Tag's ID is made. We propose that if the RFID system was able to correct one-bit or even multiple-bit errors, RFID would benefit significantly. By having an error-correcting system implemented, the Reader would be able to identify the Tag in less reads on average, and it would potentially improve the range at which the Reader could identify the Tag.

2. METHODOLOGY

The first major milestone in approaching our research problem will be to develop a firm understanding of the implementation and execution of Cyclic Redundancy Check (CRC) in the context of RFID interrogators. This will be accomplished through an analysis of the Class-1 Generation-2 UHF RFID documentation provided by EPCglobal and by examining past work in the RFID communications field, specifically with regards to the use of CRC.

After establishing a thorough understanding of CRC, our next step will be to delve into the execution of error-correcting code. We will do this by reviewing past work that identifies the key differentiations and variations in performance between the two codes. We will then identify one or more specific error-correcting codes that we believe to be most applicable for use in RFID systems and conduct further research regarding these specific codes.

Finally, once we have developed a deep understanding of CRC and identified one or more error-correcting codes for use in an RFID system, we will transmission error rate metrics for RFID systems to simulate the effect of these error correcting codes in terms of tag reading efficiency, added complexity to the tag and interrogator, and overall performance increase for the system.

3. PREVIOUS WORK

In their article, A New Ultralightweight RFID Authentication Protocol with Permutation, authors Tian, Chen, and Li propose implementing a strong but relatively simple protocol that implements permutation in order to establish authenticity between Reader and Tag [4]. The last messages exchanged in their protocol are sent again by the reader to resist against desynchronization attacks.

Authors Grzegorz Smietanka, Jan Geldmacher and Jurgen Gotze proposed the implementation of Forward Error Correction (FEC) in their article, Error Detection Based on Correlation Analysis for BCH Encoded UHF RFID Communication [3]. They say the FEC could be implemented easily because of BCH code?s similarity to CRC.

A Secure RFID Authentication Protocol Adopting Error Correction Code talks about using a one-way hash to establish authenticity and prevent intentional transmission manipulation, which CRC is not capable of detecting. By hashing the Tag's ID, a secret key, and random challenge numbers, the authors claim that mutual authentication can be achieved [1].

Another lightweight protocol for de-synchronization is proposed by authors Zhou, Zhang, Luo, and Wong in their article A lightweight anti-desynchronization RFID authentication protocol. They claim that using the one-way hash and XOR functions while the backend server keeps a history of all shared secret keys prevents desynchronization and is capable of finding intentional errors [5].

Finally, On Error Performance Improvements of Passive UHF RFID Systems via Syndrome Decoding discusses using the existing CRC error detection implementation to correct single bit errors. Using a lookup table with various CRC codes and other information stored in it, CRC becomes capable of correcting single bit errors [2].

4. REVISED RESEARCH PLAN

11/11/14: Interim report

11/12 - 11/16: Implement missing Noise and ECC models

11/17 - 11/21: Perform final analysis on effectiveness on each Error Correcting Code for each Noise Model and collect data for comparison

11/22 - 11/27: FINAL WORK PERIOD - Make final additions to paper and revise

11/28: Assign presentation sub-sections to team members

11/28 - 12/1: Team members individually create presentation components

12/1 - TBD: Compile final presentation from components and practice delivery

TBD (12/2/14 - 12/4/14): Final Presentation

5. NECESSARY RESOURCES

We chose to conduct a theoretical analysis of the communication protocols at hand. Building our own RFID interrogator and RFID tags for each case would be exceedingly difficult considering the intricate electrical components that must be constructed. This time could better be devoted to a more complete theoretical analysis of the communication protocols in question. Because we are taking a purely theoretical approach, no hardware will be required; however, we would value any input from the instructor concerning resources and methods for analyzing the efficacy of communication protocols.

6. ROAD BLOCKS AND CONCERNS

The major road block we have is finding a quantitative method to measure the efficacy of a protocol in a theoretical environment. Most past work on efficacy of error-correcting protocols in RFID communication has been conducted in controlled laboratory environments. While a statistical analysis based on the chance of message bits being corrupted under various conditions is plausible, we have not yet found any pre-existing methods for conducting the analysis.

7. REFERENCES

[1] Chien-Ming Chen, Shuai-Min Chen, Xinying Zheng, Pei-Yu Chen, and Hung-Min Sun. A Secure RFID Authentication Protocol Adopting Error Correction Code. *The Scientific World Journal*, 2014:12, 2014.

[2] R. Morelos-Zaragoza. On Error Performance Improvements of Passive UHF RFID Systems via Syndrome Decoding. In *Internet of Things (iThings/CPSCom), 2011 International Conference on and 4th International Conference on Cyber, Physical and Social Computing*, pages 127–130, Oct 2011.

[3] G. Smietanka, J. Geldmacher, and J. Gotze. Error Detection Based on Correlation Analysis for BCH encoded UHF RFID Communication. In *Industrial Technology (ICIT), 2013 IEEE International Conference on*, pages 1666–1670, Feb 2013.

[4] Yun Tian, Gongliang Chen, and Jianhua Li. A New Ultralightweight RFID Authentication Protocol with Permutation. *Communications Letters, IEEE*, 16(5):702–705, May 2012.

[5] Shijie Zhou, Zhen Zhang, Zongwei Luo, and Edward C. Wong. A Lightweight Anti-Desynchronization RFID Authentication Protocol. *Information Systems Frontiers*, 12(5):521–528, 2010.