Joint Iterative Decoding and Authentication (JIDA)

David Carman

Michael Jordan

Dr. Charles Boncelet, Renwei Ge, Dr. Gonzalo Arce

Dr. Giovanni Di Crescenzo

Prepared through collaborative participation in the Collaborative Technology Alliance for Communications & Networks sponsored by the US Army Research Laboratory under Cooperative Agreement DAAD19-01-2-0011

email: *dcarman@nai.com*

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
01 DEC 2007	**N/A**	

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Joint Iterative Decoding and Authentication	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **McAfee Research, Network Associates**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited.

13. SUPPLEMENTARY NOTES

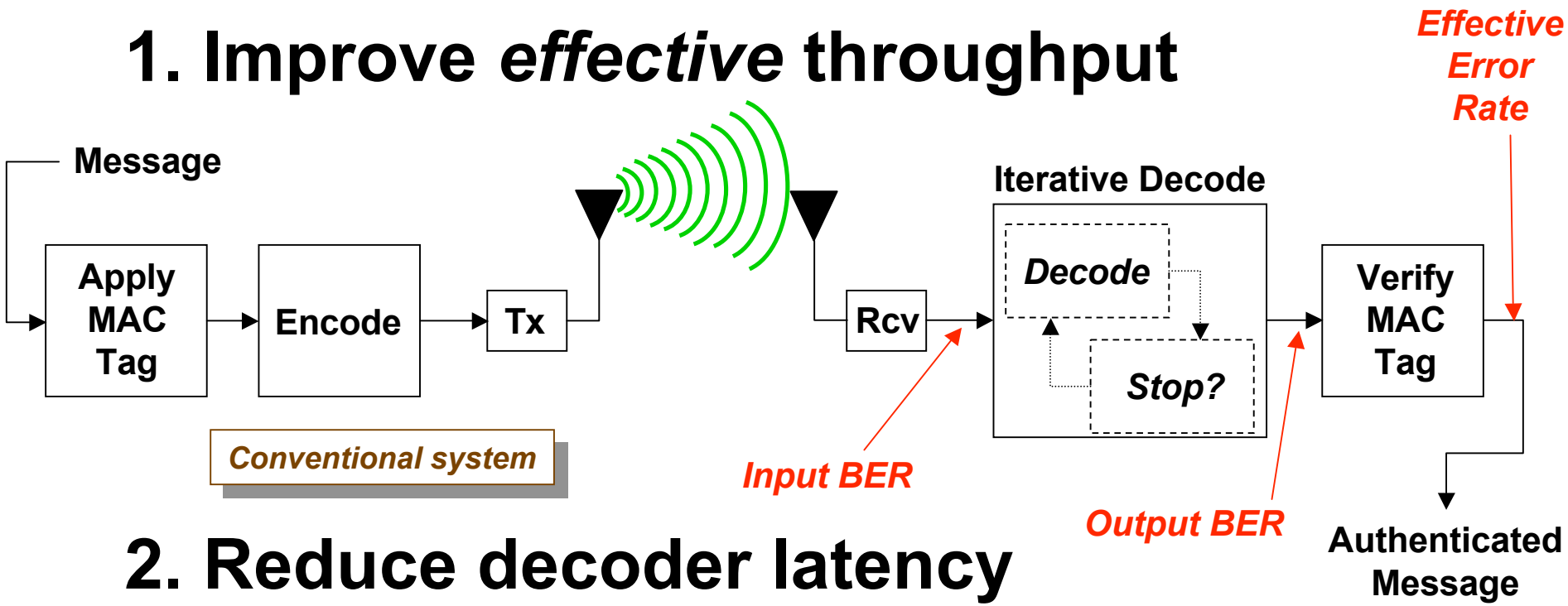
14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**UU**	**9**	

JIDA Objectives

1. Improve *effective* throughput

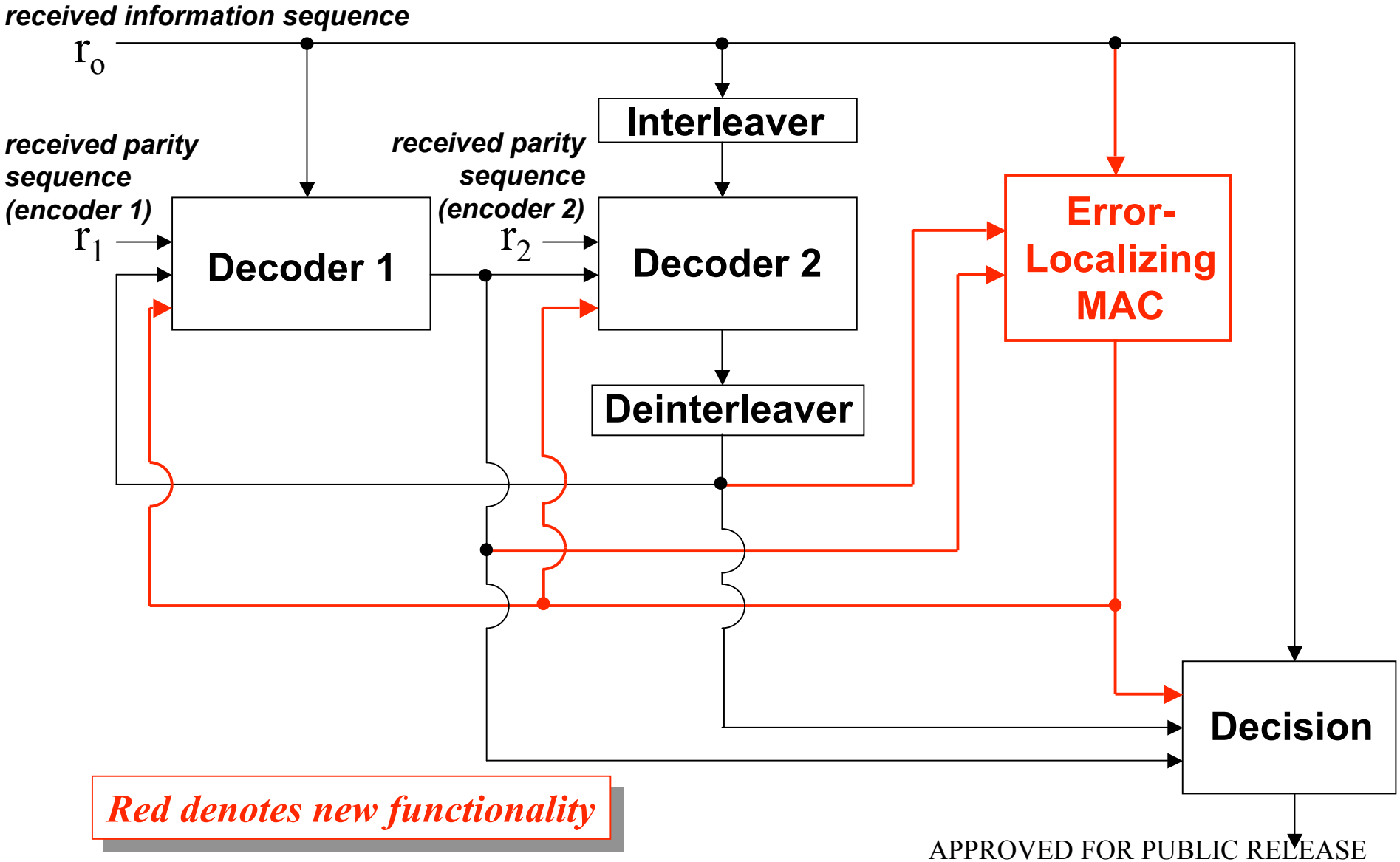


2. Reduce decoder latency

– Reduce number of decoder iterations by having the authentication module declare packet “authentic” or “correct” packet

email: dcarman@nai.com

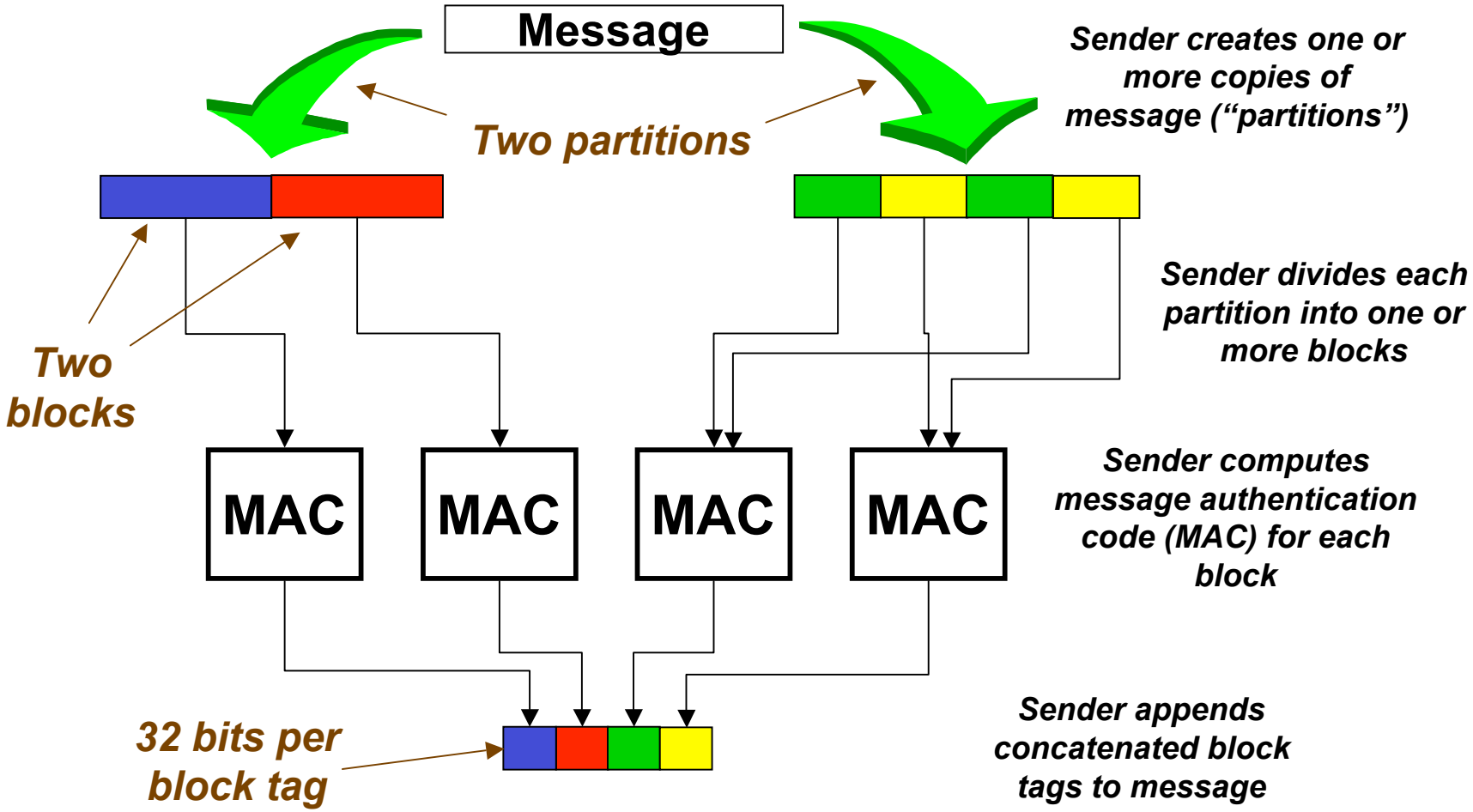
High-Level Approach



email: dcarman@nai.com

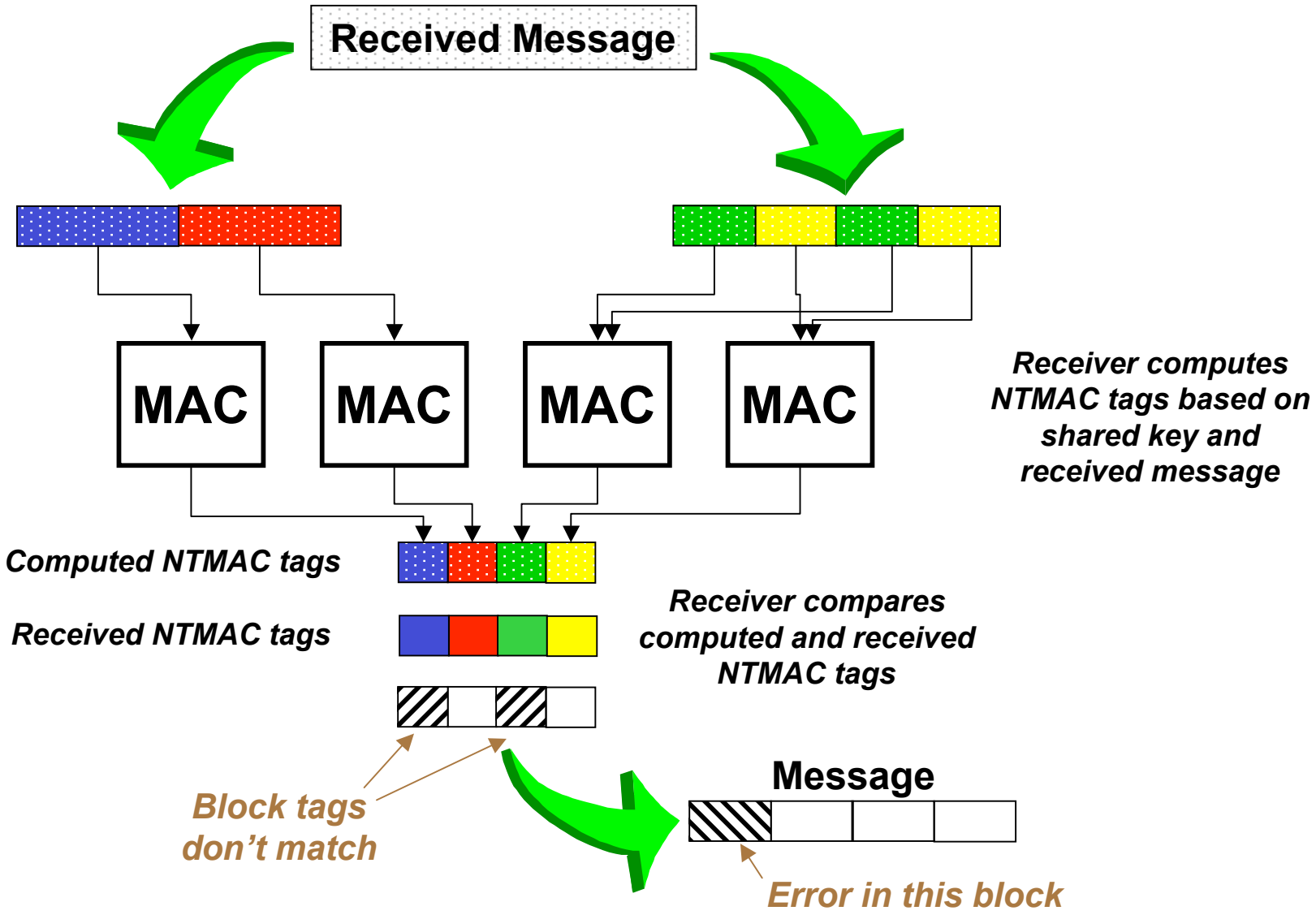
Noise-Tolerant MAC (NTMAC)

- Invented by Dr. Charles Boncelet



email: dcarman@nai.com

NTMAC Receive Processing



email: dcarman@nai.com

7/8/4 NTMAC

- Tradeoff single-bit forgery security for error localization
  - 7 partitions, 8 blocks/partition, 4-bit block tags → 224-bit NTMAC authentication tag
  - 32-bit BCH parity check over the NTMAC tag (n=255, k=223, t=4 errors)
  - Probability of a *single-bit* forgery is 2^{-28} per attempt
    - security increases for multiple-bit forgery attempts
- Authentication module returns one of four "flags":
  - "**Authentic**" - the input data/tag pair is authentic
  - "**Authentic when corrected**" - the input data/tag pair is authentic when corrected as denoted
  - "**Estimate provided**" - can not correct the input data/tag pair to authentic result, but an estimate of the log-likelihood ratio of each bit is provided
  - "**Too many errors**" - cannot distinguish correct and error bits
- NTMAC/CE "Hybrid" Termination Criteria
  1. Total Iterations = 30, or
  2. NTMAC returns AUTHENTIC, or
  3. NTMAC returns AUTHENTIC_WHEN_CORRECTED, or
  4. NTMAC returns TOO_MANY_ERRORS ***and*** CE recommends termination

email: dcarman@nai.com

Monte Carlo Simulation

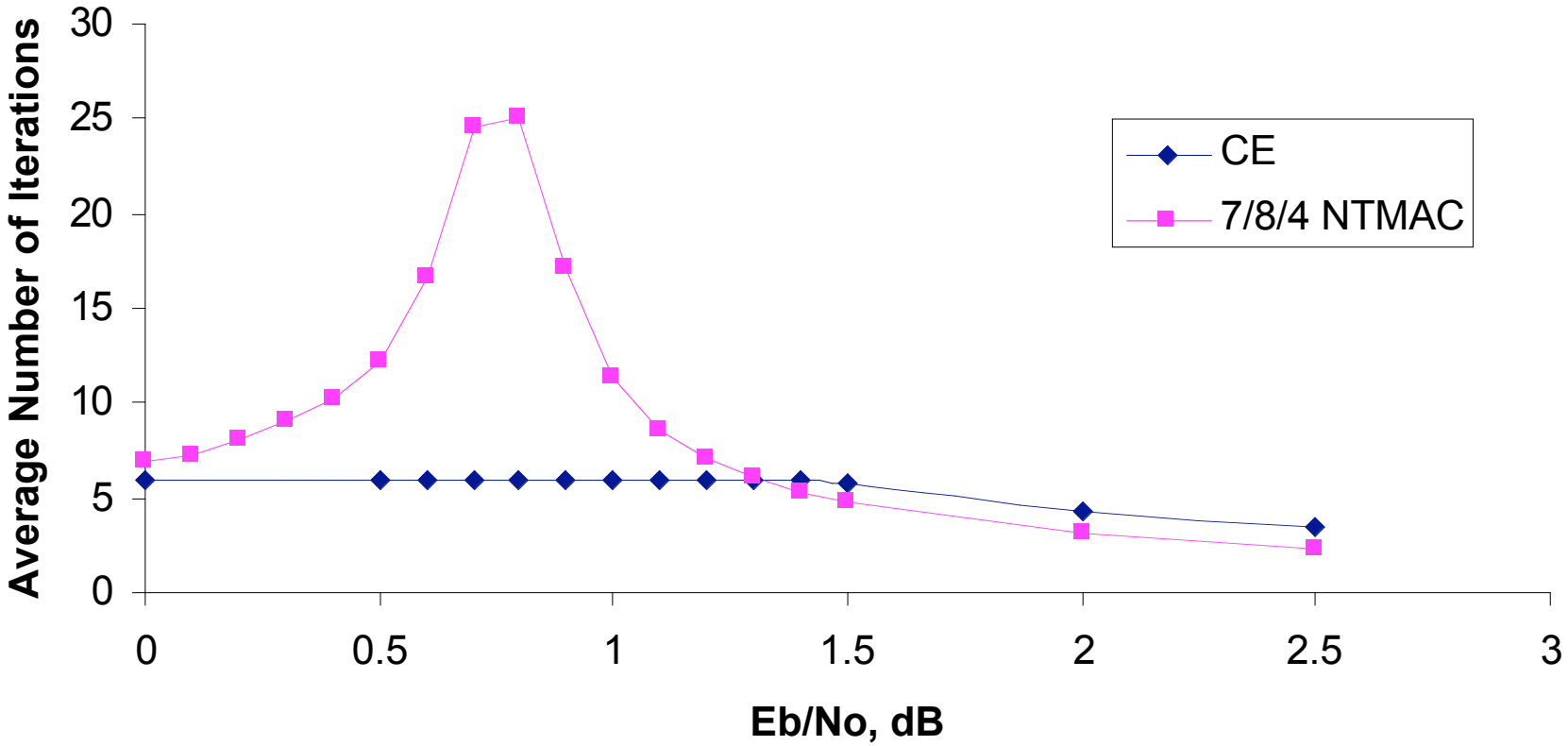
- Two parallel concatenated rate _ constituent convolutional coders (generating polynomial 7,5) produce net rate 1/3 (unpunctured) or rate _ (punctured) turbo code
- 16384-bit S-random interleaver with S=52
- Linear additive white Gaussian (AWGN) channel
- Compare Two Termination Criteria

1. **Cross-Entropy (CE)**
   - Calculates the approximate cross-entropy between the distributions at the end of successive iterations and terminates decoding of a data frame when the value falls below a user specified value
   - 16384 bits of data per frame (no checksum bits)
   - Terminate after six iterations even if CE threshold not met
2. **7/8/4 NTMAC/CE "Hybrid"**
   - 16128 bits of data plus 256 total tag/checksum bits per frame

– Errors occur in both data and tag/checksum portions

email: dcarman@nai.com

Average Iterations – 16384-bit Frames

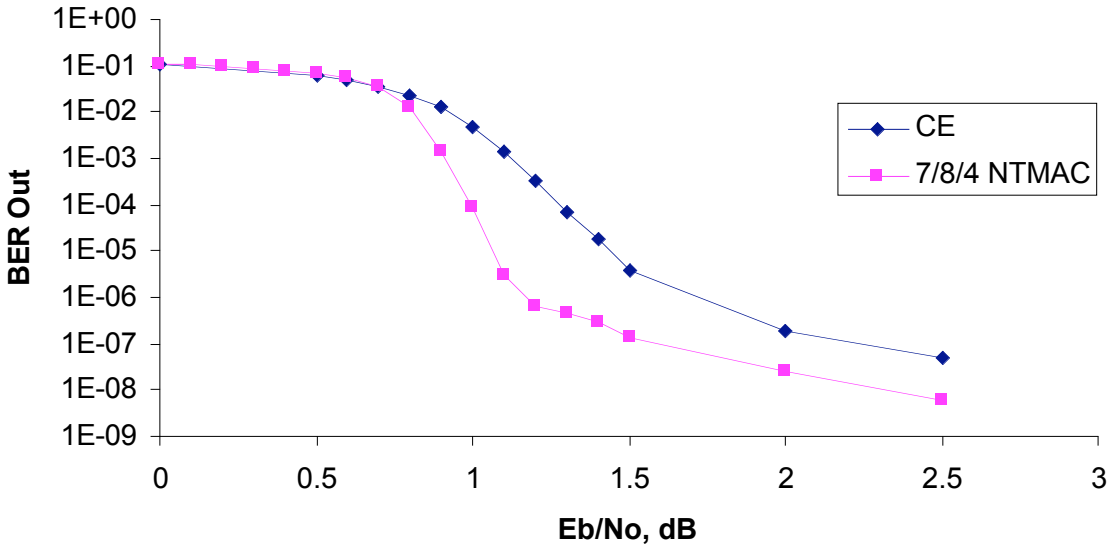


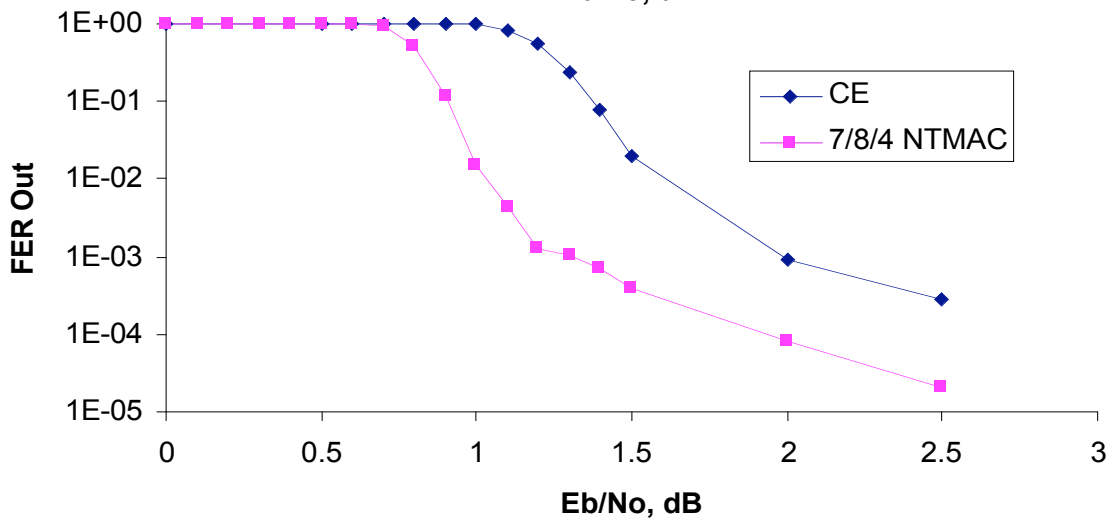
"Hybrid" termination method significantly increases average iterations per frame for low E_b/N_o

email: dcarman@nai.com

Bit and Frame Error Rates

16384-bit Frames





7/8/4 NTMAC significantly improves output bit error rate

7/8/4 NTMAC significantly improves output frame error rate

email: *dcarman@nai.com*