# Short Notes on Communication with Byzantine Node Failures: Part I

Rachit Agarwal, Guanfeng Liang and Nitin Vaidya
Department of Electrical and Computer Engineering
University of Illinois at Urbana-Champaign
Champaign, Illinois, USA
Email: {agarwa16, gliang2, nhv}@illinois.edu

*(Technical Report, November 17, 2009)*

In our previous work [1] and [2] we showed by example that linear network coding cannot achieve secure network capacity for error detection. To the best of our knowledge, it was the first work that identified the insufficiency of linear network codes in achieving secure capacity, even for unicast. Some recent works [3], [4] also discovered (independently) the necessity of non-linear network codes to achieve secure capacity.

## I. Counter Example for Previous Conjecture in Reference [2]

In our earlier work [2], we formulated the problem of computing the maximum throughput a network can achieve with duplication and forwarding, which is one particular type of linear network codes, as a linear optimization problem. To the end of the paper, we conjectured that only $N(s)$, the neighbors of the source, need to perform coding to achieve the maximum throughput with linear codes and single node failures:

*Conjecture 1:* The error-detection capacity of the network is achieved with all nodes in $V\backslash\{s, N(s)\}$ only forwarding a replica of the information packets.

It turns out that this conjecture is not true. The network in Fig.1 is a counter example. In this network, the source has infinite broadcast capacity, each of nodes in $N(s)$ has broadcast capacity 1, and each of the neighbors of the destination has capacity 2. Solving the optimization problem in [2] for this network will give the maximum error detection rate with duplication and forwarding equals to $3\frac{2}{3}$. But in fact, with linear network coding in the neighbors of the destination can achieve a rate of 4. A scheme to achieve rate of 4 is as follows:

$s$ broadcast packet $a, b, c, d$, and $a+b+c+d$. $r_1$ to $r_5$ each forward one of the five packets from $s$. Then $r_6$ forwards $a$ and $b$, $r_7$ forwards $c$ and $d$, and $r_8$ will forward $a+b+c+d$. In addition, $r_8$ will also generate a new packet $a+c$ from packet $a$ and $c$.

We can see that none of $r_1$ to $r_5$ can tamper the packets without being detected because they are protected by the $(5, 4)$ code $(a, b, c, d, a+b+c+d)$. So the adversary can only attack $r_6$ to $r_8$. If the adversary attacks $r_6$, it cannot tamper packet $a$ without being detected since it is protected by the $(3, 2)$ code $(a, c, a+c)$. $r_6$ cannot tamper packet $b$ without being detected either, since the destination can derive $b+d$ from $a+b+c+d$ and $a+c$ it receives from $r_8$, and $b$ is protected by the code $(b, d, b+d)$. Similarly, neither $r_7$ nor $r_8$ can tamper the packets they transmit without being detected.

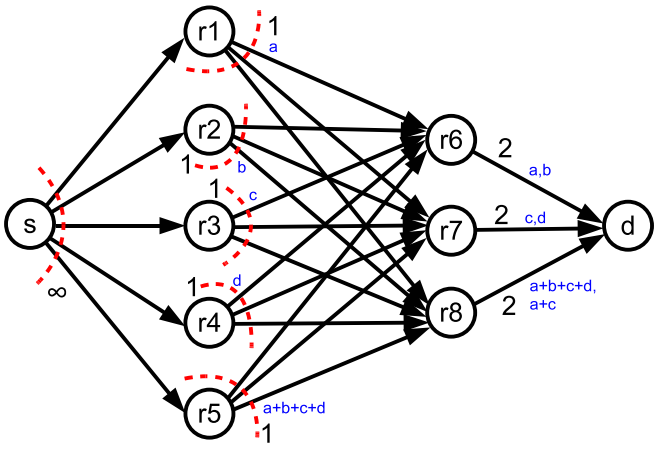


Fig. 1. Counter example for previous conjecture

This research was supported in part by Army Research Office grant W-911-NF-0710287

## References

[1] G. Liang and N. Vaidya, "When watchdog meets coding," *Technical Report, CSL, UIUC,* May 2009.
[2] G. Liang, R. Agarwal, and N. Vaidya, "Secure capacity of wireless broadcast networks," *Technical Report, CSL, UIUC,* September 2009.
[3] O. Kosut and L. Tong, "Nonlinear network coding is necessary to combat general byzantine attacks," in *47th Annual Allerton Conference on Communication, Control, and Computing,* October 2009.
[4] S. Kim, T. Ho, M. Effros, and A. Salman, "Network error correction with unequal link capacities," in *47th Annual Allerton Conference on Communication, Control, and Computing,* October 2009.