DRAFT: Robust Communication in Structured Networks

Edward L. Platt
elplatt@umich.edu

Daniel M. Romero
drom@umich.edu

December 2015

1 Introduction

2 Trust Model

We assume that a sender A (or Alice) wants to send sensitive information to a receiver B (or Bob). Alice and Bob are both nodes on a communication network represented by a graph $G = (V, E)$. Two nodes are connected when they are able to communicate directly with each other. We also assume the presence of an adversary C (or Eve) who wishes to disrupt that communication by altering or delaying the transmission. Eve has compromised a subset of nodes and has full control over their behavior. Any transmission routed through a compromised node is considered faulty. Alice and Bob do not know which nodes have been compromised.

In our model, links also represent trust. Specifically, two nodes are connected if each node believes that the other has not been compromised by its adversary. In other words, a communication link is severed if one node believes the other to be compromised. If trust were transitive, a connected path from Alice to Bob, would guarantee a trusted channel, but trust is not transitive [1]. Rather than entirely abandoning transisitivy, we assume that trust is partially transitive. Specifically each node has a *trusted neighborhood* of nodes up to h hops away, which we assume have not been compromised by that node's adversaries. Our objective is now to construct a robust communication channel from Alice's trusted neighborhood to Bob's.

3 Multipath Fault Tolerance

We achieve robust communication between trusted neighborhoods through Concurrent Multipath Routing (CMR) []. If there are multiple *redundant paths* (i.e., paths sharing no nodes or links) between Alice and Bob's trusted neighborhoods, multiple copies of a message can be sent along different paths, enabling standard error detection and error correction techniques to be applied at the destination. If Alice randomly selects k of n total redundant paths, Eve's best strategy is to compromise at least one node on as many of the paths as possible. Because an error can be detected if even a single copy has been tampered with, Eve must compromise all k paths in order to convince Bob to accept a compromised message. If Eve has the resources to compromise l total nodes, the probability that Bob receives an undetectable error is:

$$p_e = \frac{l!\,(n-k)!}{n!\,(l-k)!}. \tag{1}$$

Letting $k = \alpha n$ and $l = \beta n$, then applying Stirling's approximation gives:

$$\begin{aligned} p_e \approx & \frac{\sqrt{\beta(1-\alpha)}}{\sqrt{\beta-\alpha}} \\ & \times \left[\left(\frac{\beta-\alpha}{1-\alpha}\right)^{\alpha} \left(\frac{\beta}{\beta-\alpha}\right)^{\beta} (1-\alpha) \right]^{n} \end{aligned} \tag{2}$$

Note that Eq. (2) is exponential in the number of redundant paths n, which depends only on the network structure, and not on the resources available to individual nodes. If a network has a large num-

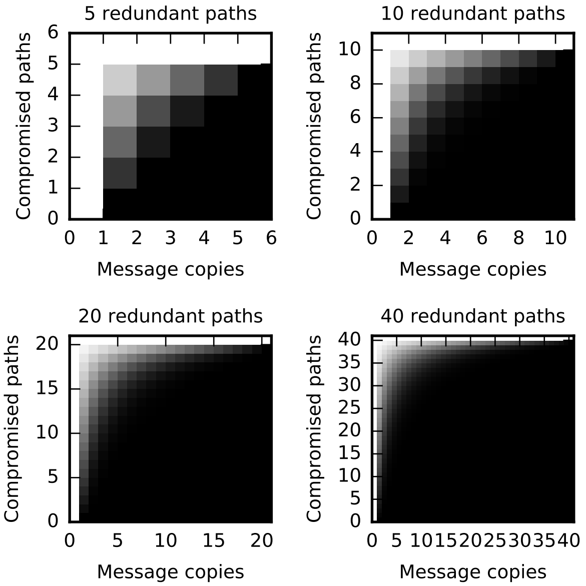

Figure 1: Probability p_e of an undetected error as a function of the number of message copies k and compromised paths l.

ber of redundant paths between trusted neighborhoods, a very low probability of undetected errors can be achieved, even if an adversary has the resources to compromise a very large fraction of the avialable paths. The value of p_e for various k, l, and n is shown in Figure 1.

4 Butterfly Network

5 Discussion

6 Conclusion

References

[1] Bruce Christianson and William S Harbison. Why isn't trust transitive? In *Security protocols*, pages 171–176. Springer, 1997.

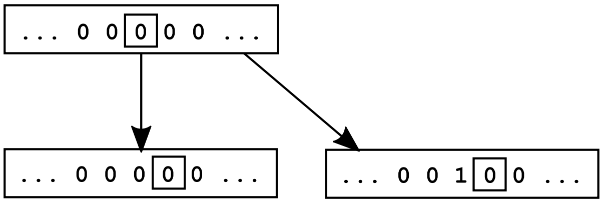

Figure 2: