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 Fault Tolerance

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.