Attack-Tolerance in Structured Networks via Multipath Routing Draft: 2016-02-16

EDWARD L. PLATT, University of Michigan
DANIEL M. ROMERO, University of Michigan

TODO

CCS Concepts: •**TODO**→ **TODO;**

Additional Key Words and Phrases: censorship, decentralization, fault tolerance, multipath, networks, peer-to-peer, trust

TODO: Fix bibtex encoding.

1. INTRODUCTION

Communication networks, expemplified by the Internet, have become ubiquitous and critical infrastructural for communities, organizations, and markets. As with any critical infrastructure, the cost of a failure can be immense, so methods for tolerating various kind of faults are an important and ongoing area of research. The key question is: what are the techniques and network structures that can be used to create robust, fault-tolerant systems?

Many complex networks, including the Internet and World-Wide Web, exhibit scale-free structure [Barabsi and Albert 1999; Barabsi and others 2009]. While scale-free networks tolerate random faults well, they are highly susceptible to adversarial faults, i.e. attacks [Albert et al. 2000]. For example, in 2008, YouTube suffered a worldwide outage for several hours when a service provider in Pakistan advertised false routing information [Hunter 2008]. The action (known as a *black hole attack*) was intended to censor YouTube within Pakistan only, but resulted in a worldwide cascading failure. Such vulnerabilities are not limited to any one system or protocol, but an attribute of complex communication networks themselves. General techniques for understanding and mitigating these vulnerabilities are needed.

In this paper, we formally evaluate the effects of network structure on attack-resistance. We also propose an efficient, fault-tolerant network architecture. Our analysis focuses on *structured networks*, in which links between nodes are constrained to a particular architecture. The proposed fault-tolerant architecture utilizes *multipath routing*, in which many possible paths exist betweeen two nodes on a communication network. In our case, multiple paths allow multiple copies of a message to be sent, which can be used for error-detection and error-correction by the receiver.

Our main contributions are:

— We present a formal *partial trust model*, which makes weaker transitivity assumptions than previous web-of-trust models, and use this model to quantify the effects of network structure on fault tolerance;

This work is supported by TODO.
Authors addresses: E.L. Platt and D.M. Romero, School of Information; email: {elplatt,drom}@umich.edu.

EC'16, July 24–28, 2016, Maastricht, The Netherlands. ACM 978-1-4503-3936-0/16/07.
http://dx.doi.org/10.1145/XXXXXXX.XXXXXXX

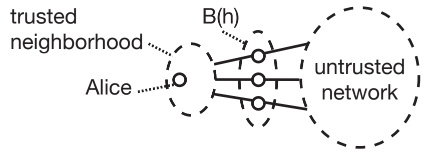

Fig. 1. TODO

— We show that the probability of successfully detecting an adversarial fault increases exponentially with the number of disjoint untrusted paths between the neighborhoods of the sender and receiver, and that this value depends on network structure;
— We present a scalable, efficient and attack-tolerant multipath routing algorithm on the butterfly network topology.

Paper organization. TODO

2. BACKGROUND AND RELATED WORK

Within *structured networks*, link structure is predetermined. Such networks can be designed to have favorable structural properties, at the expense of complicating the addition or removal of nodes. Structured networks have been a popular tool in distributed and parallel processing architectures [Kshemkalyani and Singhal 2008]. More recently, peer-to-peer systems based on distributed hash tables have used structured "overlay" networks to map table keys to local TCP/IP routes [Lua et al. 2005].

Distributed fault tolerance.

Multipath routing [Qadir et al. 2015]

Secure multipath routing [Zin et al. 2015]

Redundancy for fault tolerance [Alrajeh et al. 2013]

Multipath for increased security [Khalil et al. 2010; Kohno et al. 2012; Lou and Kwon 2006]

Randomized paths [Liu et al. 2012]

3. ADVERSARY-RESISTANT COMMUNICATION NETWORKS

3.1. Goals

Scalability Decentralization Secrecy Stabilizing asymmetry

3.2. Network Properties

Sparse

Low-diameter

Vertex-transitivity

Redundancy [Baran and others 1964]

Routing

3.3. Trust

Scale and indirect communication

Source-to-network

Source-to-destination

4. MULTIPATH FAULT TOLERANCE

Fault tolerance with partial trust and redundancy.

4.1. Fault Tolerance

Results

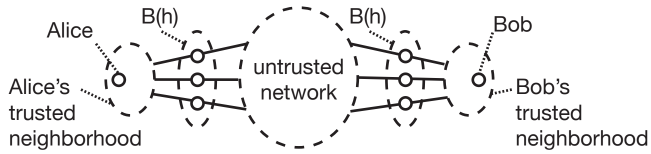

Fig. 2. TODO

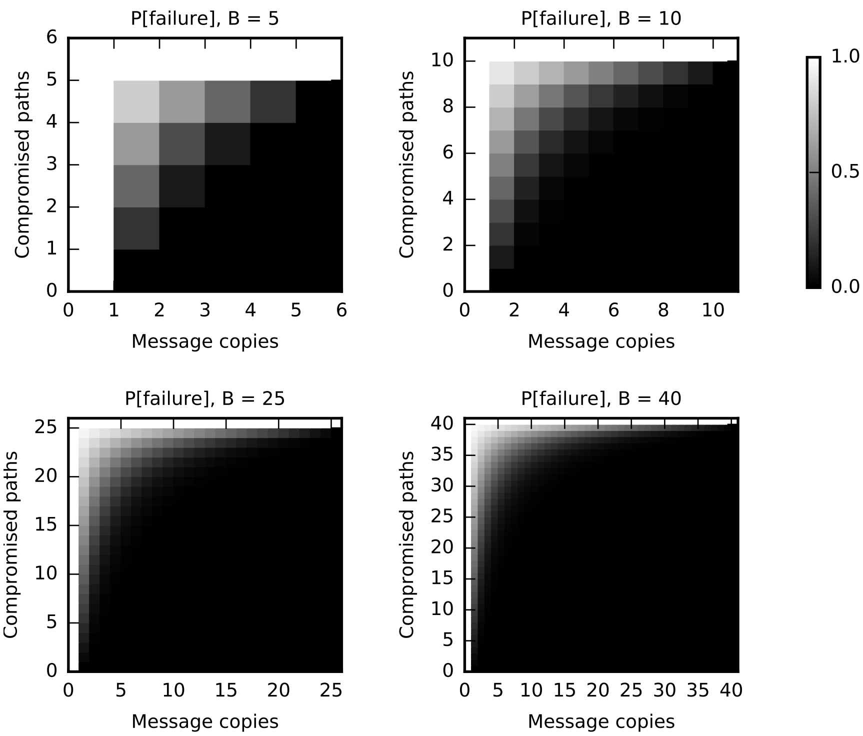

Fig. 3. TODO

5. MULTIPATH ROUTING ON THE BUTTERFLY TOPOLOGY

We now describe a Concurrent Multipath Routing scheme on a specific family of networks: the butterfly network []. Several variations on the butterfly network exist. Specifically, we utilize the wrap-around butterfly. We denote the m-dimensional directed wrap-around butterfly as $\mathrm{wBF}(m)$:

$$\begin{aligned}
\mathrm{wBF}(m) &= (V, E_{\downarrow} \cup E_{\rightarrow}) && (1)\\
V &= \mathbb{Z}_m \times \mathbb{Z}_{2^m} && (2)\\
E_{\downarrow} &= \{((l,z),(l+1 (\bmod m), z) \\
&\quad \mid l \in \mathbb{Z}_d, z \in \mathbb{Z}_{2^m}\} && (3)\\
E_{\rightarrow} &= \{(l,z),(l+1 (\bmod m), z \oplus 2^l) \\
&\quad \mid l \in \mathbb{Z}_d, z \in \mathbb{Z}_{2^m}\}, && (4)
\end{aligned}$$

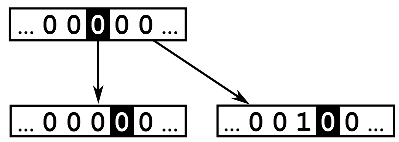

Fig. 4. Schematic illustration of the two types of edges in a directed butterfly network. The node (l, z) is shown as the bit string z with a square around the lth bit.

where $\oplus$ represents the bitwise XOR operator. Each node is associated with a level l and an m-bit integer z. There are two types of edges, shown in Figure 4. Down edges ($E_{\downarrow}$) connect nodes sharing the same z value in a cycle of increasing level l. Down-right edges ($E_{\rightarrow}$) also link to a node of level $l+1$, but one having the bitstring equal to z with the lth bit flipped.

The wrap-around butterfly network has a number of properties making it useful for multipath routing:

Vertex transitivity. The problem of finding a route between arbitrary nodes v and w can be reduced to finding a route from node $(0, 0)$ to some $\tilde{w}$.

Logarithmic diameter. For any two nodes, the length of the shortest path between them is logorithmic in the size of the network.

Constant degree. In practical applications, each communication link requires additional resources, such as physical infrastructure or entries in a routing table. A constant degree limits the number of such resources needed as the network grows in size.

We now describe a routing scheme that provides 2^h redundant paths between the h-hop trusted neighborhoods of any two nodes in an m-bit wrap-around butterfly network. Utilizing vertex transitivity, we label the source node as $(0, 0)$ and denote the destination node as $w = (l_w, z_w)$.

Let s be an integer such that $0 \leq s < 2^h$. Let $v_s^{(t)} = (l^{(t)}, z^{(t)})$ be the tth node in the path labeled by s. For convenience, we will omit the subscript s. We define two partitionings of the integers in $\mathbb{Z}_{2^m}$: one having the lowest h bits matching the bits of s, and one having the h bits preceeding the destination level l_w matching s:

$$S_s = \{z \in \mathbb{Z}_{2^m} | \forall i \in \mathbb{Z}_h z_i = s_i\} \tag{5}$$

$$R_s = \{z \in \mathbb{Z}_{2^m} | \forall i \in \mathbb{Z}_h z_{(l_w - h + i)} = s_i\}. \tag{6}$$

Note that if $r \neq s$, then $S_s \cap S_r = R_s \cap R_r = \emptyset$.

We now construct a path such that between trusted neighborhoods $z^{(t)}$ is always in S_s, R_s, or both, guaranteeing that the path does not overlap with the other paths $v_r^{(t)}$. Routing proceeds in stages, with the level l increasing by 1 at each hop. In Stage 1 ($0 \leq t < h$), down or down-right edges are chosen such that the the tth bit of $z^{(t+1)}$ is equal to the tth bit of s. Throughout Stage 1, all nodes are within the sender's trusted neighborhood. At the end of Stage 1, $z^{(h)} \in S_s$, and $z^{(t)}$ will remain so until the level loops back to 0 at $t = m$.

In Stage 2 ($h \leq t < l_w - h$), edges are chosen to make the tth bit of $z^{(t+1)}$ match the tth bit of z_w.

In Stage 3 ($l_w - h \leq t < l_w$), the bits of $z^{(t)}$ are chosen to match s, such that after the stage is complete, $z^{(l_w)} \in R_s$.

In Stage 4 ($l_w \leq t < m$), as in stage 2, paths are chosen such that the tth bit of $z^{(t+1)}$ matches z_w. After Stage 4, all bits of $z^{(m)}$ are equal to those of z_w except for the first h and the h preceeding index l_w. $z^{(m)}$ is also in both S_s and R_s.

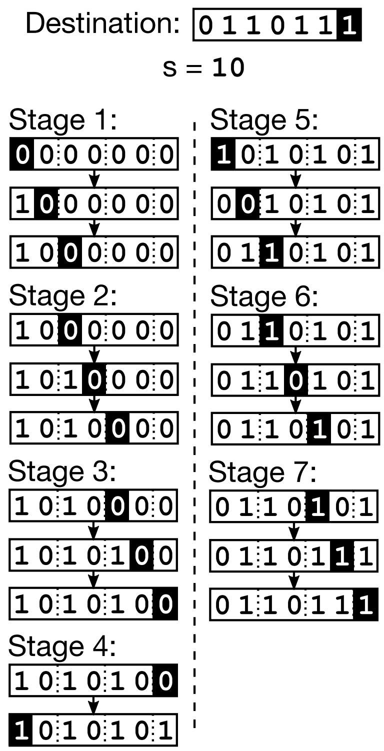

Fig. 5.

At this point, we define $\tau = t - m$. In Stage 5 ($0 \leq \tau < h$), the first h bits of $z^{(t)}$ are set to match z_w, potentially removing $z^{(t)}$ from S_s.

In Stage 6 ($h \leq \tau < l_w - h$), all down edges are chosen, incrementing the level without any effect on $z^{(t)}$. At the end of Stage 6, $z^{(m+l_w-h)}$ is still in R_s and $v^{(m+l_w-h)}$ is now within the trusted neighborhood of w.

In the seventh, and final stage ($l_w - h \leq \tau < l_w$), the h bits of $z^{(t)}$ preceeding index l_w are set to match z_w. After this stage, $v^{(m+l_w)} = w$ and routing is complete.

6. DISCUSSION

Secrecy

Creation of the network. Improves on web of trust. Gives framework for determining where to build trust.

Applications Distributed apps: storage, email, cryptocurrency, secure multiparty computation. Wireless Sensor Networks

7. CONCLUSION

ACKNOWLEDGMENTS

The authors would like to thank TODO

REFERENCES

Rka Albert, Hawoong Jeong, and Albert-Lszl Barabsi. 2000. Error and attack tolerance of complex networks. *nature* 406, 6794 (2000), 378–382.

Nabil Ali Alrajeh, Mohamad Souheil Alabed, and Mohamed Shaaban Elwahiby. 2013. Secure ant-based routing protocol for wireless sensor network. *International Journal of Distributed Sensor Networks* 2013 (2013).

Albert-Lszl Barabsi and Rka Albert. 1999. Emergence of scaling in random networks. *science* 286, 5439 (1999), 509–512.

Albert-Lszl Barabsi and others. 2009. Scale-free networks: a decade and beyond. *science* 325, 5939 (2009), 412.

Paul Baran and others. 1964. On distributed communications. *Volumes I-XI, RAND Corporation Research Documents, August* (1964), 637–648.

Philip Hunter. 2008. Pakistan YouTube block exposes fundamental internet security weakness: Concern that pakistani action affected youtube access elsewhere in world. *Computer Fraud & Security* 2008, 4 (2008), 10–11.

Issa Khalil, Saurabh Bagchi, Cristina N Rotaru, and Ness B Shroff. 2010. UnMask: Utilizing neighbor monitoring for attack mitigation in multihop wireless sensor networks. *Ad Hoc Networks* 8, 2 (2010), 148–164.

Eitaro Kohno, Tomoya Okazaki, Mario Takeuchi, Tomoyuki Ohta, Yoshiaki Kakuda, and Masaki Aida. 2012. Improvement of assurance including security for wireless sensor networks using dispersed data transmission. *J. Comput. System Sci.* 78, 6 (2012), 1703–1715.

Ajay D Kshemkalyani and Mukesh Singhal. 2008. *Distributed computing: principles, algorithms, and systems*. Cambridge University Press.

Anfeng Liu, Zhongming Zheng, Chao Zhang, Zhigang Chen, and Xuemin Shen. 2012. Secure and energy-efficient disjoint multipath routing for WSNs. *Vehicular Technology, IEEE Transactions on* 61, 7 (2012), 3255–3265.

Wenjing Lou and Younggoo Kwon. 2006. H-SPREAD: a hybrid multipath scheme for secure and reliable data collection in wireless sensor networks. *Vehicular Technology, IEEE Transactions on* 55, 4 (2006), 1320–1330.

Eng Keong Lua, Jon Crowcroft, Marcelo Pias, Ritu Sharma, and Sharon Lim. 2005. A survey and comparison of peer-to-peer overlay network schemes. *Communications Surveys & Tutorials, IEEE* 7, 2 (2005), 72–93.

Junaid Qadir, Anwaar Ali, Kok-Lim Alvin Yau, Arjuna Sathiaseelan, and Jon Crowcroft. 2015. Exploiting the power of multiplicity: a holistic survey of network-layer multipath. *Communications Surveys & Tutorials, IEEE* 17, 4 (2015), 2176–2213.

Shazana Md Zin, Nor Badrul Anuar, Miss Laiha Mat Mat Kiah, and Ismail Ahmedy. 2015. Survey of secure multipath routing protocols for WSNs. *Journal of Network and Computer Applications* 55 (2015), 123–153.