Towards Attack-Tolerant Networks: Concurrent mutlipath routing and the butterfly network

Anonymous
For Blind Review

Abstract

It is crucial for large-scale communication networks such as the internet to be resilient against attacks [41] such as censorship and surveillance, which pose a threat to free expression and free association. Self-organized networks such as the internets router network typically have heavy-tailed degree distributions [5], making them highly vulnerable to targeted attacks against central nodes [1]. While cryptographic solutions exist, they fail to address the underlying topological problem, and remain vulnerable to man-in-the-middle attacks [34] and coercion [17]. Coercion-resistant, topological approaches to attack tolerance are needed to address the current vulnerability of communications infrastructure to censorship and surveillance. We present a novel concurrent multipath routing (CMR) algorithm for the wraparound butterfly network topology, as well as a highly attack-tolerant Structured Multipath Fault Tolerance (SMFT) architecture which incorporates the butterfly CMR algorithm. Our work is the first theoretical demonstration of a point-to-point communication network architecture that can resist coercion and other non-technical attacks, without requiring transitive trust. To address cases where the network structure cannot be fully controlled, we demonstrate how a snapshot of the internet's router network can be partially rewired for greater attack-tolerance.

1 Introduction

> The Net interprets censorship as damage and routes around it.
>
> –*John Gilmore* [15]

Is it possible for any large-scale communication network to resist targeted attacks? The internet was originally designed to withstand targeted (nuclear) attacks [6], and the resilience of the internet has long been part of common wisdom [15]. But 18 years after Albert et al. [1] showed the internet's router network is vulnerable to targeted attacks, the fundamental problem of attack-tolerant network topology remains unsolved. Attack-tolerant topologies are desirable for any physical or virtual network where a compromised node puts communication at risk. For example, the network of verified keys in the public key infrastructure underlying secure http [14], or the network of DNS nameservers. The ongoing vulnerability of the internet is evidenced by a long history of censorship and surveillance incidents achieved by means of targeted attacks [11]. In this paper, we present the first theoretical network topology supporting attack-toloerant, point-to-point networked communication, without relying on transitive trust [9].

Methods for tolerating various kind of faults within networks are an important and ongoing area of research [47, 1, 41]. *Adversarial faults*, those in which an adversary can target attacks strategically, deserve special attention. Such attacks are both extremely difficult to guard against and often have important social implications. In particular, censorship and surveillance are often achieved by targeting central network locations and either blocking or capturing the information flowing through them. While cryptograpy can provide some protection against surveillance, it is vulnerable to *man-in-the-middle* attacks [34], and cannot overcome censorship when communication is blocked. In this paper, we instead consider a topological approach. The Internet's decentralized design was motivated by the need to withstand targeted attacks, such as nuclear strikes [6]. But despite longstanding common wisdom [15], both theoretical results and recent events have demonstrated that the internet is surprisingly vulnerable to attack.

Analysis of the internet's router network has shown that while it is remarkably resilient against random faults, it is highly susceptible to adversarial faults [1]. These results have been attributed to the heavy-tailed degree distribution of the Internet's router network [4, 5]. Random failures are highly likely to affect only low-

degree nodes, thus having little effect. However, adversarial faults target the few high-degree nodes, and therefore remove a large number of edges with each fault. So while the *protocols* of the Internet are decentralized, the *network structure* is somewhat centralized. In other words, the protocols of the Internet do not *require* centralization, but centralization may still emerge from the sociotechnical processes that create its network structure.

The internet's vulnerability to censorship and other targeted attacks has been demonstrated by several recent events. In 2008, YouTube suffered a worldwide outage for several hours when a service provider in Pakistan advertised false routing information [18]. The action (known as a *black hole attack*) was intended to censor YouTube within Pakistan only, but resulted in a worldwide cascading failure when a router misconfiguration allowed the false routing information to propagate outside of Pakistan. This incident exemplifies the type of attack requiring a topological approach. First, the attack was *non-technological* (a government order), allowing the attacker to bypass any cryptographic or technology-based defenses. Second, the attack originated at a *single point of failure* (a misconfigured router). Third, the behavior of the compromised component (the router) cascaded through a *network* (the network of internet routers) because the correct behavior of other components depended on the correct behavior of the single point of failure. And while the action was not an intentional attack against the global internet, the ability of an attacker to succeed without even trying only highlights the internet's vulnerability to adversarial faults.

Similarly, in 2013, the Texas-based email provider Lavabit was ordered to disclose their private SSL keys to the FBI [36]. Lavabit instead chose to cease operations in order to protect their users from surveillance. Once again, the attack was non-technical. And again, the attack was on a single point of failure: Lavabit's web server and that server's SSL keys. In this case, the affected network was the internet's public key infrastructure. With the private keys, an attacker would be able to intercept and surveil traffic because the users would incorrectly trust that they were communicating with Lavabit. So we see that such vulnerabilities are not limited to any one system, but result from centralized structure itself.

This paper addresses the need for a theoretial understanding of network and redundancy-based approaches to attack tolerance. Our primary result is theoretical: an algorithm for constructing highly redundant paths in a particular network topology, suggesting the importance of further theoretical and applied work.

We make two main contributions. We prove that the number of h-internally vertex disjoint paths between two nodes in a wrap-around butterfly network is at least 2^h, and present a scalable and efficient concurrent multipath routing (CMR) algorithm to find these paths. This result is combined with structured multipath fault-tolerance (SMFT) to achieve a high level of attack-tolerance. We also show that rewiring a the edges of the internet's router network to resemble a butterfly network allows it to tolerate a higher number of failures without fragmenting, and increases the effective redundancy in the presence of a large number of adversarial faults.

2 Background and Related Work

Centralized approaches to attack-tolerance such as *public key infrastructure* (PKI) suffer from a number of vulnerabilities [14], including vulnerability to coercion, which stems largely from the single points of failure inherent to centralization. The *web of trust* is a decentralized alternative [46, 39] but depends on the unrealistic assumption of trust transitivity [9].

Many distributed consensus protocols (e.g., cryptocurrencies) are designed to tolerate arbitrary or adversarial faults. Byzantine agreement protocols [25, 8] provide tolerance against arbitrary faults (including attacks) under some circumstances, but are limited to small networks due to poor scalability. Proof-of-work [13, 33] (blockchain) systems provide better scalability, but are wasteful of computational and energy resources, and do not take advantage of trusted relationships. Federated Byzantine Agreement (FBA) [31] is scalable, allows for flexible trust, and is highly fault-tolerant on networks meeting specific requirements. However, FBA does not provide a method for constructing networks to meet those requirements.

All existing attack-tolerant networks we are aware of are content-addressable networks (CANs) in which data is stored and retrieved based on key values, rather than point-to-point networks, in which data is communicated between two parties. Fiat and Saia described a scheme that combines the butterfly topology with expander graphs to create a highly censorship-resistant, content-addressable network [16], although this scheme requires high levels of data replication and indefinite storage. Perhaps the most mature structural solution is the Freenet collaboration [10]. Freenet uses secret sharing [40, 7] and small-world routing [45, 21] to create a content-addressable network with a high level of both confidentiality and censorship resistance. Freenet guarantees that data is stored redundantly, but still allows for centralized network structure, and thus single points of failure, as data travels from its origin to the redundant storage locations. Unlike the above content-addressable networks, our architecture is purely network based and does not require nodes to store data indefinitely.

Multipath routing protocols identify multiple paths between source and destination in contrast to traditional

unipath routing, which uses a single path. The special case of *concurrent* multipath routing uses multiple paths simultaneously. Multipath routing has many applications, including reduced congestion, increased throughput, and more reliability [37]. Many of these routing protocols offer increased confidentiality [47]. Some approaches utilize redundant paths as backups for increased fault tolerance [2], and some specifically protect against adversarial faults [22, 19, 29]. Most work on multipath routing has been motivated by applications related to wireless sensor networks (WSNs), and have thus focused on ad-hoc, unstructured networks, often having a central base station. The method of Liu et al. [28] routes multiple messages first to random peers and then to a central base station, with the network edges constrained by sensors' physical location. We have found very few examples of CMR applied to *adversarial* fault tolerance in the existing literature, and all have focused on ad-hoc wireless sensor networks, without attention to the role of network structure.

Our proposed routing algorithm makes use of a *structured network*, in which link structure is predetermined. Structured networks have been a popular tool in parallel processing architectures [24]. 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 [30, 23]. Such networks can be designed to have favorable structural and routing properties, which can be used to to improve attack-tolerance.

Our proposed architecture is differentiated from existing systems by several properties. Decentralized architectures are more resistant to coercion [17] and man-in-the-middle attacks [34]. Topological approaches address the root cause of vulnerability in heavy-tail networks, rather than relying on technology that can be side-stepped through coercion. The topological approach is also more sustainable than proof-of-work systems. Point-to-point communication allows two individuals to exchange messages without requiring large amounts of indefinite data storage on intermediate nodes.

3 Networks and Fault Tolerance

3.1 Multipath Fault Tolerance

Standard fault tolerance methods [3, 42] use redundancy to detect and correct statistically independent faults. In complex networks however, faults can be correlated when, for example, two messages pass through the same faulty node. For now, let us assume our sender (Alice) and receiver (Bob) are connected by δ *independent paths* such that no two paths contain the same faulty node. Let $k = \alpha\delta$ be the number of messages Alice can send and $l = \beta\delta$ be the number of nodes Mal can compromise. If Alice choses paths at random and Mal compromises paths at random, the probability of blocking or altering all of Alice's messages can be shown to be approximately:

$$p_f \approx \frac{\sqrt{\beta(1-\alpha)}}{\sqrt{\beta-\alpha}}\left[\left(\frac{\beta-\alpha}{1-\alpha}\right)^{\alpha}\left(\frac{\beta}{\beta-\alpha}\right)^{\beta}(1-\alpha)\right]^{\delta} \quad (1)$$

Fig. 1 shows the value of p_f as a function of k and l. Eq. (1) shows that while p_f depends on the fractions of paths actually utilized α and compromised β, it decreases exponentially with δ. This result is significant because δ depends only on the network structure. *Thus, the scheme can be effective, even when the number of paths used k is a small fraction of the channels available*. In other words, this scheme exhibits a *stabilizing asymmetry:* senders can tolerate attacks from significantly more powerful adversaries. Furthermore, this scheme requires only a small increase in network traffic as long as the network provides a large number of independent paths δ.

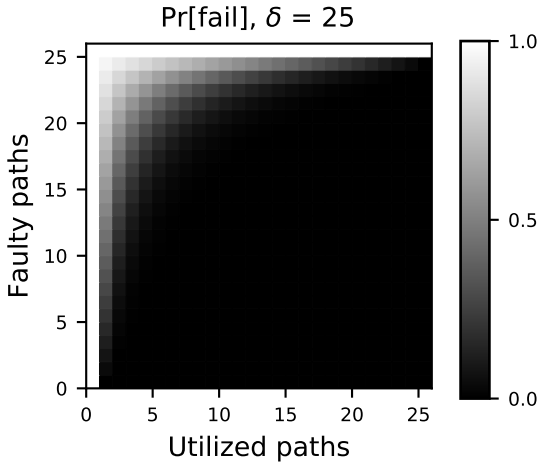

Figure 1: The probability of an undetectable error as a function of the number of redundant channels and the number of adversarial faults. A small increase in the number of utilized paths (network traffic) can compensate for a large increase in attacker power.

3.2 Effective Redundancy

The effect of an attack on communication between two nodes depends on how many of the paths between those nodes pass through the a compromised node. The number of such compromised paths depends on both the network topology and the position of the endpoint nodes relative to the compromised node. If the compromised node

is one of the endpoints, then all paths from that node are compromised. When the endpoints are farther from the compromised node, the paths from the endpoints branch out into many paths before one of those passes through the compromised node.

The network topology determines how many redundant paths exist less than a given distance h away from each node. With more paths, any single compromised node has a smaller effect. For a given node pair (s,t), We call this number of paths $\delta_{h,s,t}$ the *pairwise effective redundancy*. For the entire network, the *effective redundancy* is the minimum over all vertex pairs:

$$\delta_h(G) \equiv \min_{s,t \in V} \delta_{s,t,h}. \quad (2)$$

In graph theoretical terms, the effective redundancy at distance h is the minimum number of *h-internally vertex-disjoint* paths between any node pair. A higher effective redudncancy means that, for a given distance h between an endpoint and a compromised node, the more redundant paths are available to route around that attack. In the absence of centralized bottlenecks, the effective redundancy is limited by the endpoint closest to an attack.

3.3 Structured Multipath Fault Tolerance

Finding a maximal set of independent paths for an arbitrary network is NP hard [38], posing a challenge for multipath fault tolerance. We propose side-stepping this problem by using structured networks, for which independent paths can be generated efficiently. We call this approach *structured multipath fault tolerance* (SMFT), and now proceed to show how it is implemented on the butterfly network topology.

4 The Butterfly Network Topology

In order to implement structured multipath fault tolerance, we need a structured network topology with high effective redundancy. In this paper, we apply SMFT to the butterfly network topology [24]. The butterfly network is recursive, with larger versions composed out of multiple smaller versions, suggesting large attack-tolerant networks could be constructed by merging smaller ones. To address the case when the network cannot be fully controlled, we show how partially rewiring a snapshot of the internet's router network can greatly increase it's effective redundancy and attack-tolerance properties, without requiring additional edges.

4.1 Butterfly Network Topology

We choose the butterfly topology [24] because of several desirable properties (described below) and because its structure allows for relatively straightforward design and analysis of routing algorithms. While several variations on the butterfly network exist, we utilize the m-dimensional, directed wrap-around butterfly, denoted wBF(m):

$$\begin{aligned} \text{wBF}(m) &= (V, E_{\downarrow} \cup E_{\rightarrow}) && (3)\\ V &= \mathbb{Z}_m \times \mathbb{Z}_2^m && (4)\\ E_{\downarrow} &= \{((l,z),(l+1 \pmod m, z)\} && (5)\\ E_{\rightarrow} &= \{(l,z),(l+1 \pmod m, z \oplus 1_l\}, && (6) \end{aligned}$$

where $\mathbb{Z}_m$ is the set of integers modulo m, $\oplus$ represents component-wise addition modulo 2, and 1_l is a vector with a 1 in index l and 0 elsewhere. Each node is associated with a level l and an m-bit string z known as *the place-within-level*. There are two types of edges: down, and down-right. 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 place-within-level equal to z with the lth bit inverted.

The wrap-around butterfly network is known to have several of the properties we desire for scalable, decentralized communication networks:

Vertex-transitivity: Because the wrap-around butterfly is vertex transitive, it is maximally decentralized;

Small-diameter: For any two nodes, the length of the shortest path between them is $O(\log N)$, where N is the number of nodes in the network (corresponding to low-latency in real-world terms);

Sparsity: With a constant degree of 4, the wrap-around butterfly is extremely sparse, and can scale indefinitely without node degree becoming a limitation;

Redundancy: Multiple paths exist between any two nodes. Specifically, we will prove below that the number of h-internally vertex-disjoint paths between two nodes increases exponentially with h.

The structure of the butterfly network lends itself to a well-known (unipath) routing algorithm, which we later extend to the multipath case. The unipath algorithm first follows a down or down-right edge at every step, increasing the level l by 1 and cycling through the indices of the place-within-level. If the current node's place-within-level matches the destination node's at index l, a down edge is chosen and the place-within-level does not change. Otherwise, a down-right edge is chosen and the lth component of the place-within-level is flipped, after which it matches the destination. After m iterations of this, all levels have been visited and the place-within-level matches that of the destination. Simply following down (or up) edges will then increment (decrement) the level until the destination node is reached.

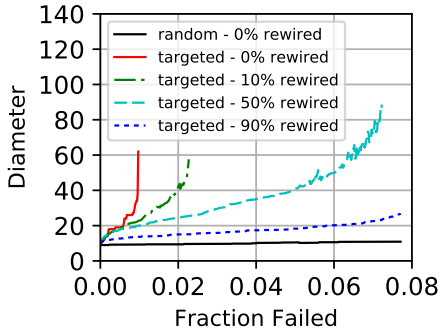

Figure 2: Simulation of targeted attacks against a snapshot of the internet's router network with a fraction of the edges rewired into a partial butterfly configuration. The original network fragments when the top 1% of nodes are removed. With only 10% of the butterfly edges present, this value doubles to 2%.

4.2 Butterfly Rewiring

Even when a butterfly topology cannot be implemented perfectly, it can still increase the attack tolerance properties of a network. Here, we simulate targeted attacks against a snapshot of the internet's router network on January 2, 2000 [26], having 6493 nodes and 13914 edges. At each step of the simulation, betweenness centrality is recalculated and the most central node is removed. We also simulate attack on several rewired networks. The rewiring process alters the network structure to resemble a butterfly topology, without adding any additional edges. We 1. generate edges corresponding to a 9-dimensional butterfly network between the 4608 highest-degree router nodes, 2. choose a fraction f of those edges at random, 3. add those edges to the router network, and 4. remove an equal number of the original edges at random.

Our simulations show improved resistance to fragmentation and higher effective redundancy when even a fraction of edges have been rewired to match the butterfly topology. While the original router network fragments when about 1% of the nodes have been removed (Fig. 4.2), this number increases to 2% with only 10% of the butterfly edges present. With 90% of the butterfly edges present the network remains unfragmented beyond the failure of the 8% most central nodes.

5 Multipath Butterfly Routing

We now present a routing algorithm to construct 2^h *h-internally vertex-disjoint* paths between two nodes in a butterfly network, where h is minimum distance from an endpoint to a compromised node. Informally, Alice sends each message h hops, then to a distinct intermediate node, then to a node h hops from Bob, and finally to Bob. The intermediate nodes are in a sense "far" from each other and ensure that no two paths overlap. Each path can be parameterized by a single integer s.

5.1 Algorithm Specification

We now begin the formal specification of our multipath routing scheme for the wrap-around butterfly network. Utilizing vertex transitivity, we label the source node as $(l^{(0)}, z^{(0)}) = (0,0)$ and denote the destination node as $w = (l_w, z_w)$, without loss of generality.

Let s be an h-bit binary string with s_i denoting the bit at index i. There are 2^h such strings. Let $v_s^{(t)} = (l^{(t)}, z^{(t)})$ be the node at position t in the path parameterized by s. For convenience, we will omit the subscript s when it is obvious from context. We define three distinct partitions of m-bit binary strings. Let $Q_{v^{(0)}}$ be the set of m-bit strings in which the bits at all indices $h \le i < l_w - h$ match those of $z^{(0)}$, and let $\overline{Q_{v^{(0)}}}$ be its complement. Note that $Q_{v^{(0)}}$ is trivially all m-bit strings if $l_w < 2h$. Let R_s be the set of m-bit strings with the lowest h bits all matching the bits of s, and let $\overline{R_s}$ be its complement. Let S_s be the set of m-bit strings with the h bits preceding index l_w all matching the bits of $\tilde{s}$, where $\tilde{s}$ is a cyclic permutation of s:

$$\tilde{s}_i \quad = \quad s_{(i+l_w) \bmod h}, \tag{7}$$

and let $\overline{S_s}$ be its complement. We will make use of the fact that:

$$s \neq s' \quad \Longrightarrow \quad S_s \cap S_{s'} = R_s \cap R_{s'} = \emptyset. \tag{8}$$

Routes are constructed in 7 stages. The network topology dictates that $l^{(t+1)} = l^{(t)} + 1 \pmod m$, so we let $l = t \pmod m$. and that $z^{(t+1)}$ is equal to $z^{(t)}$ with or without the bit in index $l^{(t)}$ inverted, depending on whether the down or down-right edge was taken at step t.

Stage 1: $(0 \le t < h)$ Down or down-right edges are chosen such that 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. Throughout Stage 1, $z^{(t)} \in Q_{v^{(0)}}$. At the end of Stage 1, $z^{(h)} \in S_s$, and $z^{(t)}$ will remain so until the level cycles to 0 at $t = m$.

Stage 2: $(h \le t < l_w - h)$ Edges are chosen to make the tth bit of $z^{(t+1)}$ the inverse of the tth bit of $z^{(0)}$. Note that this stage does not occur when $l_w < 2h$. If this stage occurs, then $z^{(t)} \in \overline{Q_{v^{(0)}}}$ until these levels are reached again in stage 6.

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

Stage 4: ($l_w \leq t < m$) Paths are chosen such that the tth bit of $z^{(t+1)}$ matches that of the destination node z_w. This stage will not occur if $l_w > m-h$.

Stage 5: ($m \leq t < m+h$) There are two cases. If $2h < l_w < m-h$, then there is no overlap between the indices defining R_s and S_s. In this case, the first h bits of $z^{(t)}$ are set to match z_w. Otherwise there is some overlap between the indices defining R_s and S_s. In this case, the each of the first h bits of $z^{(t)}$ is either kept the same if $l_w - h \leq l < l_w$, or set to the corresponding bit of z_w otherwise. In this stage and after, $z^{(t)}$ is no longer guaranteed to be in R_s. However, $z^{(t)}$ remains in S_s during and after this stage.

Stage 6: ($m+h \leq t < m+l_w-h$) In this stage, edges are chosen to set the bits of $z^{(t)}$ to their corresponding value in z_w. $z^{(t)} \in \overline{Q_{v^{(0)}}}$ throughout this stage, but not afterwards.

Stage 7: ($m+l_w-h \leq t < m+l_w$) The h bits of $z^{(t)}$ preceding index l_w are set to match z_w. All nodes in this stage are within h hops of w and thus in its trusted neighborhood. After this stage, $v^{(m+l_w)} = w$ and routing is complete.

5.2 Proof of Path Independence

Theorem 1. *Given an m-bit wrap-around butterfly network ($m > 1$), and an integer h ($1 \leq h \leq \left\lfloor \frac{m}{2} \right\rfloor$), for all node pairs (v,w) such that $d(v,w) \geq 2h$, there exist at least 2^h h-internally vertex disjoint paths v_s ($0 \leq s < 2^h$) from v to w such that $s \neq s' \implies v_s \cap v_{s'} \subset T_h(u) \cup T_h(v)$.*

Proof. Nodes from two paths can only coincide if their levels are the same. Nodes which share a level must either be in the same stage, or 4 stages apart. Let (a,a') denote a pair of sub-paths corresponding to stage a of one path and stage a' of another. Excluding paths that intersect in their trusted neighborhoods, (1,1) and (7,7), we have reduced the list of possible intersections to the following cases: (2,2), (3,3), (4,4), (5,5), (6,6), (1,5), (2,6), and (3,7). Nodes in stages 2–4 belong to R_s so cannot overlap with any stage 2–4 nodes from another path, eliminating (2,2), (3,3), and (4,4). Similarly, nodes in stages 4–6 belong to a unique S_s, eliminating (5,5) and (6,6). Nodes in stage 1 belong to $Q_{v^{(0)}}$ while those in stage 5 belong in its complement, eliminating (1,5). Similarly, for all l in stage 2, $z^{(l)}$ is equal to $z^{(0)}$, while in stage 6, $z^{(l)}$ is the inverse, eliminating (2,6) This leaves only (3,7), a collision which can occur only for only one path (with s matching the first h bits of z_w), and which enters the trusted neighborhood in stage 3. For this single path, we can proceed directly from stage 2 to stage 7, eliminating the last possible collision. □

6 Discussion

In its current form, our work has several limitations. Most obviously, it requires control over the network structure. However, we have shown that even partial control over network structure can improve attack tolerance properties. There is also the question of how to construct such a network without a central authority. We conjecture that smaller independently-formed networks could be merged into a single larger network without central coordination. When nodes are tied to geographic locations, the butterfly topology would require connections between very distant locations. Such connections are extremely expensive to construct and maintain, although they do exist in the form of internet backbones. An alternative solution might involve satellite links, which connect distant geographic points much more easily. While turning our network theoretical results into practical applications will require considerable additional work, we believe that work is inevitably necessary in order to create attack-tolerant networks.

7 Conclusion

Coercion-resistant, topological approaches to attack tolerance are needed to address the current vulnerability of communications infrastructure to censorship and surveillance. We have presented a novel concurrent multipath routing (CMR) algorithm for the butterfly network, as well as a structured multipath fault tolerance (SMFT) scheme, which can be combined to create a coercion-resistant, attack-tolerant point-to-point communication architecture. Even when network structure cannot be perfectly controlled, we have shown that partially rewiring a snapshot of the internet's router network can greatly increase its attack-tolerance properties. We believe that this work provides a foundation for the development of topology-based architectures to guard against adversarial attacks, including censorship and surveillance.

8 Acknowledgments

Anonymized for blind review.

References

[1] ALBERT, R., JEONG, H., AND BARABSI, A.-L. Error and attack tolerance of complex networks. *Nature 406*, 6794 (2000), 378–382.

[2] ALRAJEH, N. A., ALABED, M. S., AND ELWAHIBY, M. S. Secure ant-based routing protocol for wireless sensor network. *Int J Distrib Sens N 2013* (2013).

[3] AVIZIENIS, A., LAPRIE, J.-C., RANDELL, B., AND LANDWEHR, C. Basic concepts and taxonomy of dependable

and secure computing. *IEEE T Depend Secure 1*, 1 (2004), 11–33.

[4] BARABSI, A.-L., AND ALBERT, R. Emergence of scaling in random networks. *Science 286*, 5439 (1999), 509–512.

[5] BARABSI, A.-L., AND OTHERS. Scale-free networks: a decade and beyond. *Science 325*, 5939 (2009), 412.

[6] BARAN, P., AND OTHERS. On distributed communications. *Volumes I-XI, RAND Corporation Research Documents, August* (1964), 637–648.

[7] BLAKLEY, G. R. Safeguarding cryptographic keys. *P Natl Comp Conf 48* (1979), 313–317.

[8] CASTRO, M., LISKOV, B., AND OTHERS. Practical Byzantine fault tolerance. In *OSDI* (1999), vol. 99, pp. 173–186.

[9] CHRISTIANSON, B., AND HARBISON, W. S. Why isn't trust transitive? In *Security protocols* (1997), Springer, pp. 171–176.

[10] CLARKE, I., SANDBERG, O., WILEY, B., AND HONG, T. W. Freenet: A distributed anonymous information storage and retrieval system. In *Designing Privacy Enhancing Technologies* (2001), Springer, pp. 46–66.

[11] DAINOTTI, A., SQUARCELLA, C., ABEN, E., CLAFFY, K. C., CHIESA, M., RUSSO, M., AND PESCAP, A. Analysis of country-wide internet outages caused by censorship. In *Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference* (2011), ACM, pp. 1–18.

[12] DINGLEDINE, R., MATHEWSON, N., AND SYVERSON, P. Tor: The second-generation onion router. Tech. rep., DTIC Document, 2004.

[13] DWORK, C., AND NAOR, M. Pricing via processing or combatting junk mail. In *Advances in Cryptology* (1993), Springer, pp. 139–147.

[14] ELLISON, C., AND SCHNEIER, B. Ten risks of PKI: What you're not being told about public key infrastructure. *Comput Secur J 16*, 1 (2000), 1–7.

[15] ELMER-DEWITT, P., AND JACKSON, D. First nation in cyberspace. *Time 6* (1993), 62–64.

[16] FIAT, A., AND SAIA, J. Censorship resistant peer-to-peer content addressable networks. In *SIAM SODA* (2002), ACM, pp. 94–103.

[17] GREWAL, G. S., RYAN, M. D., BURSUC, S., AND RYAN, P. Y. Caveat coercitor: Coercion-evidence in electronic voting. In *Security and Privacy (SP), 2013 IEEE Symposium on* (2013), IEEE, pp. 367–381.

[18] HUNTER, P. 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.

[19] KHALIL, I., BAGCHI, S., ROTARU, C. N., AND SHROFF, N. B. UnMask: Utilizing neighbor monitoring for attack mitigation in multihop wireless sensor networks. *Ad Hoc Networks 8*, 2 (2010), 148–164.

[20] KHIANI, S. R., DETHE, C., AND THAKARE, V. Comparative Analysis of Multipath Routing Techniques and Design of Secure Energy Aware Routing Algorithm for Wireless Sensor Network. *IJACR 3*, 3 (2013), 374.

[21] KLEINBERG, J. The small-world phenomenon: An algorithmic perspective. In *STOC* (2000), ACM, pp. 163–170.

[22] KOHNO, E., OKAZAKI, T., TAKEUCHI, M., OHTA, T., KAKUDA, Y., AND AIDA, M. Improvement of assurance including security for wireless sensor networks using dispersed data transmission. *J Comp Sys Sci 78*, 6 (2012), 1703–1715.

[23] KORZUN, D., AND GURTOV, A. *Structured peer-to-peer systems: fundamentals of hierarchical organization, routing, scaling, and security*. Springer, New York, NY, 2013.

[24] KSHEMKALYANI, A. D., AND SINGHAL, M. *Distributed computing: principles, algorithms, and systems*. Cambridge University Press, 2008.

[25] LAMPORT, L., SHOSTAK, R., AND PEASE, M. The Byzantine generals problem. *TOPLAS 4*, 3 (1982), 382–401.

[26] LESKOVEC, J., KLEINBERG, J., AND FALOUTSOS, C. Graphs over time: densification laws, shrinking diameters and possible explanations. In *Proceedings of the eleventh ACM SIGKDD international conference on Knowledge discovery in data mining* (2005), ACM, pp. 177–187.

[27] LEVIEN, R. Attack-resistant trust metrics. In *Computing with Social Trust*. Springer, 2009, pp. 121–132.

[28] LIU, A., ZHENG, Z., ZHANG, C., CHEN, Z., AND SHEN, X. Secure and energy-efficient disjoint multipath routing for WSNs. *IEEE T Veh Technol 61*, 7 (2012), 3255–3265.

[29] LOU, W., AND KWON, Y. H-SPREAD: a hybrid multipath scheme for secure and reliable data collection in wireless sensor networks. *IEEE T Veh Technol 55*, 4 (2006), 1320–1330.

[30] LUA, E. K., CROWCROFT, J., PIAS, M., SHARMA, R., AND LIM, S. A survey and comparison of peer-to-peer overlay network schemes. *IEEE Commun Surv Tut 7*, 2 (2005), 72–93.

[31] MAZIRES, D. *Stellar Consensus Protocol: A Federated Model for Internet-level Consensus*. 2015.

[32] MOHR, L. B. *Explaining organizational behavior*. Jossey-Bass, 1982.

[33] NAKAMOTO, S. Bitcoin: A peer-to-peer electronic cash system. *bitcoin.org* (2008), 28.

[34] NAYAK, G. N., AND SAMADDAR, S. G. Different flavours of man-in-the-middle attack, consequences and feasible solutions. In *Computer Science and Information Technology (ICCSIT), 2010 3rd IEEE International Conference on* (2010), vol. 5, IEEE, pp. 491–495.

[35] NICKERSON, J. V., TVERSKY, B., CORTER, J. E., YU, L., AND MASON, D. Thinking with networks. In *CogSci* (2010), vol. 36.

[36] POULSEN, K. Edward Snowdens e-mail provider defied FBI demands to turn over crypto keys, documents show. *WIRED* (2013).

[37] QADIR, J., ALI, A., YAU, K.-L. A., SATHIASEELAN, A., AND CROWCROFT, J. Exploiting the power of multiplicity: a holistic survey of network-layer multipath. *IEEE Comm Surv Tut 17*, 4 (2015), 2176–2213.

[38] REITER, M. K., AND STUBBLEBINE, S. G. Resilient authentication using path independence. *IEEE T Comput 47*, 12 (1998), 1351–1362.

[39] RICHTERS, O., AND PEIXOTO, T. P. Trust transitivity in social networks. *PloS one 6*, 4 (2011), e18384.

[40] SHAMIR, A. How to share a secret. *Communications of the ACM 22*, 11 (1979), 612–613.

[41] STERBENZ, J. P., HUTCHISON, D., ETINKAYA, E. K., JABBAR, A., ROHRER, J. P., SCHLLER, M., AND SMITH, P. Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines. *Computer Networks 54*, 8 (2010), 1245–1265.

[42] VON NEUMANN, J. Probabilistic logics and the synthesis of reliable organisms from unreliable components. *Automata studies 34* (1956), 43–98.

[43] WALKER, D. C. *Mass notification and crisis communications: Planning, preparedness, and systems*. CRC Press, 2012.

[44] XU, X., MAO, Z. M., AND HALDERMAN, J. A. Internet censorship in China: Where does the filtering occur? In *International Conference on Passive and Active Network Measurement* (2011), Springer, pp. 133–142.

[45] ZHANG, H., GOEL, A., AND GOVINDAN, R. Using the small-world model to improve freenet performance. In *INFOCOM* (2002), vol. 3, IEEE, pp. 1228–1237.

[46] ZIMMERMANN, P. R. *The official PGP user's guide*. MIT press, 1995.

[47] ZIN, S. M., ANUAR, N. B., KIAH, M. L. M. M., AND AHMEDY, I. Survey of secure multipath routing protocols for WSNs. *J Netw Comput Appl 55* (2015), 123–153.