Toward a Taxonomy and Attacker Model for Secure Routing Protocols

Matthias Hollick
TU Darmstadt, Germany
mhollick@seemoo.tu-darmstadt.de

Cristina Nita-Rotaru
Northeastern University, USA
c.nitarotaru@neu.edu

Panagiotis Papadimitratos
KTH, Sweden
papadim@kth.se

Adrian Perrig
ETH, Switzerland
adrian.perrig@inf.ethz.ch

Stefan Schmid
Aalborg University, Denmark
schmiste@cs.aau.dk

This article is an editorial note submitted to CCR. It has NOT been peer reviewed.
The authors take full responsibility for this article's technical content. Comments can be posted through CCR Online.

ABSTRACT

A secure routing protocol represents a foundational building block of a dependable communication system. Unfortunately, currently no taxonomy exists to assist in the design and analysis of secure routing protocols. Based on the Dagstuhl Seminar 15102, this paper initiates the study of more structured approaches to describe secure routing protocols and the corresponding attacker models, in an effort to better understand existing secure routing protocols, and to provide a framework for designing new protocols. We decompose the routing system into its key components based on a functional model of routing. This allows us to classify possible attacks on secure routing protocols. Using our taxonomy, we observe that the most effective attacks target the information in the control plane. Accordingly, unlike classic attackers whose capabilities are often described in terms of computation complexity we propose to classify the power of an attacker with respect to the *reach*, that is, the extent to which the attacker can influence the routing information indirectly, beyond the locations under its direct control.

CCS Concepts

•Networks → Routing protocols; •Security and privacy → Security protocols;

Keywords

Taxonomy, Adversarial Models

1. INTRODUCTION

Communication networks have become a critical infrastructure, as other critical infrastructures increasingly rely on them. As routing lies at the heart of any communication network, the security of the underlying routing protocol is crucial to prevent attacks and ensure availability. However, the routing system is not only one of the most complex and fragile components in the global information infrastructure, but also one of the least protected ones [13].

Attackers have repeatedly exhibited their ability to harm and exploit routing systems. Hijacking prefixes [2], compromising routers [11], and exploiting backdoors or vulnerable implementations [1] are some of the preferred intrusions, to mention just a few. The increasing number of wireless and mobile networks has also introduced significant security challenges. Unlike standard Internet routing which is designed for a mostly static topology, where connections between routers are relatively stable, communication is increasingly performed among mobile devices (mobile users, wireless sensors, cars, swarms of tiny robots, etc.). Such environments are often characterized by frequent routing changes, which are further complicated by resource constraints and unpredictable network connectivity.

The goals of an attacker in the context of a distributed routing system can be rich and diverse: the attacker cannot only target the confidentiality, availability, and integrity of information carried in packets directly, but also *indirectly*, that is, in the way the information is forwarded and processed in the network. Specifically, in the context of routing protocols, an adversary may attack the control information to make other entities act in unplanned ways. For example, an insider (an attacker located inside a security-sensitive network) may aim to exfiltrate (or mirror) confidential information, e.g., by violating security policies and logical isolation domains (e.g., by changing the VLAN tag), or by defining a new destination address of packets. Even in a seemingly "secure" environment where an attacker cannot easily inspect or modify information because it is encrypted and signed, a compromised routing protocol might introduce threats: the communication patterns (*who communicates with whom, when, and how frequently?*) may leak sensitive information. An attacker may also aim to detour traffic through a certain geographic region (or country), where traffic patterns are monitored and communications can be blocked at any time, or where more computational resources are available. Moreover, performing cryptographic operations may be too costly in high-performance and latency-critical networks, it is thus important that the routing protocol guarantees the integrity of the paths actually taken.

Despite the efforts to develop and deploy secure routing protocols, there is limited work on the specification of the security requirements [15], including a model of possible attackers, their goals, and finally the attack impact. Quantifying the resilience of a routing protocol as well as the potential impact of different routing attacks simultaneously is a challenging problem. For instance, whether S-BGP is

more effective than origin authentication depends on the specific attack strategy and, ideally, we would like to understand what is the worst possible attack for a given protocol [5, 7].

Well-established routing systems and attack vectors are still poorly specified today, and it is even more notorious in the case of recent networking paradigms such as Software-Defined Networking, Content-Centric Networking, or the Internet-of-Things. We take the advent of these new paradigms as an opportunity to make a first step towards classifying the possible attacks on routing protocols in a structured way.

This paper initiates the development of a structured view and taxonomy of the routing system and possible attacks and vulnerabilities, focusing on routing protocol attackers. In particular, we propose a model and decomposition of the routing system, centered around the fundamental functions/services it provides: forwarding, topology, transport, and identity resolution. Based on this decomposition, we identify possible attacks on the different functions, and derive a classification of attackers accordingly.

A main insight from our analysis is that the information driving the key routing functions requires special protection. Depending on the instantiation of the routing system, this information may stay local or might be shared directly or via multi-hop communication. An attacker targeting the integrity of this information or its availability to the control plane might thus affect the correct working of the entire routing system. This information-centric perspective also leads us to define a measure for the power of an attacker, namely *the reach*: how far beyond its directly controlled components can an attacker influence the routing paths and configurations?

2. A FUNCTIONAL MODEL OF ROUTING

We define routing as a service which allows "routers", i.e., the entities that execute routing protocols and support the relevant functionality, henceforth generally termed *nodes*, to communicate information to other nodes: either directly or indirectly via other nodes in the network.

For the purpose of our taxonomy, we identify the following logical functional components of a routing service: (1) transport service, (2) topology service, and (3) route and data forwarding. Additionally, a routing service usually interacts with external services and resources. Understanding the resources the different components need as well as the interactions and the assumptions (implicit or explicit) they make can help creating a cleaner taxonomy of attacks against routing.

Below we provide more details about the context in which routing resides. We then identify the routing components and describe how they interact with each other.

2.1 Routing Resources and External Services

Before examining the individual functions in more detail, we elaborate on the context in which our routing components are situated.

Hardware. First, a routing system obviously depends on several hardware components (routers, links, SDN controllers, etc.). However, as our focus here is more on the protocols and logic rather than (unintentional or malicious) hardware errors, we treat the hardware as an external entity.

Example. The dependency on the hardware has recently been manifested in various incidents, and (hardware) backdoors have been planted in various products, see the Snowden leaks [19].

Identity resolution. Node identity resolution is the most crucial part of identity management in the context of routing systems. In particular, a routing service usually interacts with an *identity resolution* logic which allows resolving the identity of any node. In the following, we treat identity resolution as an external service, yet we include it in our discussions.

Example. Examples include AS numbers, router identities, MAC addresses, geographical coordinates (physical or logical), DNS or even data.

2.2 Transport Service

The transport service captures the means by which packets are communicated between nodes. These packets can either contain data or control information. Such control information includes, e.g., link status, distance vectors, or network topology. Information can be unicast, multicast, or broadcast. The service depends on the identity resolution service.

Example. Control information such as keep-alive messages or distance vectors are often flooded among neighboring nodes. Unlike other routing protocols, peers in the Border Gateway Protocol (BGP) communicate with neighbors over TCP sessions (port 179). The transport of regular data usually occurs over TCP/IP or UDP/IP unicasts. (Note that our notion of transport is more general than the one used in the context of the OSI stack / Layer-4.) In a software-defined network, control information is also exchanged between the switches/routers and one or multiple controllers.

2.3 Topology Service

The main goal of the topology service is to provide an up-to-date (partial) view on the network topology and notably, connectivity information and descriptions of the communication capabilities (e.g., bandwidth, delay, reliability), captured as metrics. The service is implemented through the use of control messages (such as keep-alive messages), communicated by the transport service. Nodes can modify received control messages (as is the case in path-vector protocols), or can initiate new control messages. Information used to obtain a view of the network can be retrieved either from direct neighbors, or be propagated from other nodes, through multi-hop communication. The service also includes neighbor discovery. The information the topology service uses is stored in a possibly distributed database which maintains information about neighbors, network topology, and path metrics.

The topology service depends on the transport service, and is used in the route computation service described next.

Note that due to the decentralized nature of routing, different nodes might have a different and only partial view of the topology of the network. The topology service depends on the correctness of the neighbor discovery service [18] and the correct propagation of information.

Example. In traditional networks, topology information is often communicated and stored in terms of distance vectors or link states. In software-defined networks, the controller uses OpenFlow and other protocols to build a unified view of network topology and network information base.

2.4 Route Service and Data Forwarding

We define forwarding as the process of selecting the neighboring node (in case of unicast) or neighboring set of nodes (in case of multicast) to which a message should be communicated. As the routing and forwarding tables are a function of the network information base, data forwarding depends on the topology service. Note that the transport service performs the actual forwarding.

The route computation service describes the (centralized or distributed) algorithm by which the actual routes are computed, given the information from the topology service, as well as the inputs from administrator and network policies. The service does not involve any actual communication. The route selection can be done based on metrics such as hop count, link reliability or latency.

Example. Traditional routing services are often based on shortest paths (e.g., ECMP), but more flexible routes can be defined, e.g., using source routing, MPLS or SDN. In the case of source routing protocols, the source alone computes the entire route: the task of the routers along the path boils down to forward the packet to the next hop the source has defined. In case of data centric networks or networks based on geographic routing, routes may also be defined based on local decisions which depend on data or locations.

3. AN OVERVIEW OF ATTACK GOALS AND MODELS

Given the above decomposition, we consider typical security objectives, along with anonymity, and relate those to attacks seeking to violate those for each component.

3.1 High-Level Security and Privacy Attack Goals

The most general classification of attacks can be defined along the security goals that an attacker tries to break. The main security objectives are the canonical ones, availability, integrity, authenticity, confidentiality, to which we add anonymity: many routing protocols promise to provide some form of anonymity (in particular, location anonymity) and unlinkability (e.g., Tor protocols based on onion routers), and accordingly, these properties may also form the target of an attack.

- **Availability:** these attacks include preventing forwarding to one/some/all nodes, attacks which isolate one/some/all nodes, as well as attacks that degrade the performance of the routing service.
- **Authenticity:** these attacks include nodes impersonating other nodes in neighbor discovery and maintenance protocols.
- **Integrity:** attacks that compromise the integrity of the forwarded data (in the data plane) or state information (in the control plane). For example, in today's Internet, messages of the BGP protocol are often propagated in an insecure manner, which attackers might exploit.
- **Confidentiality:** attacks that compromise confidentiality of forwarded data or state information. For instance, an attacker may aim to learn about traffic communicated by other tenants.
- **Anonymity:** attacks that compromise anonymity and location privacy.

3.2 Attacker Goals and Capabilities

We distinguish between a *passive* attacker who can simply read routing related information traversing elements under its control, and an *active* attacker who can modify, delete or generate routing or traffic related information (e.g., packet headers).

The most basic actions an attacker can perform are:

1. *Manipulating information:* an attacker may manipulate control or data information carried in packets. For example, it can announce wrong link metrics or BGP routes.
2. *Eavesdropping communication:* an attacker may eavesdrop or store confidential information carried in packets, or analyze traffic patterns.
3. *Data forwarding attacks:* an attacker can drop, delay, or divert communication.
4. *Identification related attacks:* an attacker can impersonate another entity.

To what extent such attacks can be performed depends clearly on the attacker's capability, including location and visibility.

Issues regarding the classification of attacker capabilities are: the way in which an attacker can influence the target system (i.e., routing or routing functional components), the number of attackers (e.g., in terms of controlled locations), and the resources available (either observable, or direct access). Computational power represents a determining factor.

Inside-Only / Outside-Only / Inside-and-Outside Attackers. One possible classification is to divide attackers into insider vs outsider attackers. Outsider attackers have a more limited interaction with the system: they can observe communication, modify, or inject packets. Inside attackers can observe and interact with the system "from inside", and have access to keys and storage that outside attackers does not have. Designing protocols resilient to insider attackers is more challenging as cryptographic protocols might not be sufficient since attackers have access to cryptographic keys. Note that a set of attackers can include both outside and inside attackers (with respect to the routing system) who can coordinate to further increase their impact.

Number, coordination, attacker placement. For both outside and inside attackers, the number of attackers and the possibility of the attackers to coordinate are important factors for creating stronger attacks. Attacker placements also matter: for example in wireless networks certain positions allow for more exhaustive eavesdropping, and exploiting highly connected adversarial nodes increases the influence of inside attackers over other participants in the network. Moreover, creating the illusion of multiple identities, compromising system components or entire nodes, or physically cloning devices, are all ways in which an attacker can increase its resources.

Global/partial influence. The degree of observability or network resources access can be partial or global. For instance, an outside attacker can have "global" observability (w.r.t. a given domain) or just partial observability of the traffic. Similarly, an inside attacker may control a subset of nodes and thus have access to a partial database. Attackers with global observability can potentially impose higher damage, however the cost of obtaining that global observability can be higher.

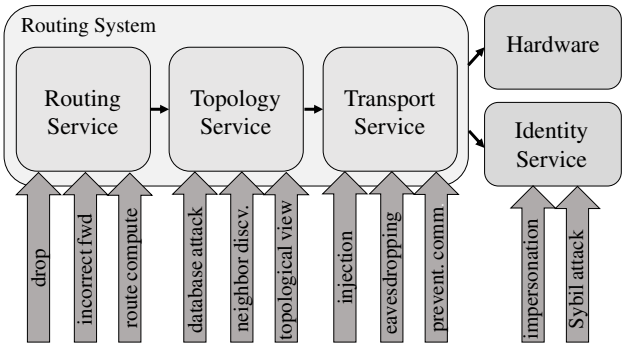

Figure 1: Overview of the taxonomy and attacks.

Entire system or sub-components. Finally, considering the functional model of the routing we presented in the previous section, an attacker of any of the above categories can exert its influence over all of the routing components or over just some particular component. An attacker can also influence or control external components such as the identity resolution service or the hardware.

Computational power. Clearly, the computational power of an attacker also plays a role. In particular, a powerful attacker able to break cryptographic key can more easily eavesdrop and manipulate packet contents, even if encrypted and signed.

To illustrate this point, consider an attacker who has compromised a number of nodes, has partial observability, and tries to break anonymity. The same attacker can try to attack the availability for other nodes. A small network of connected and strategically placed adversarial components may suffice to control an entire network.

4. ROUTING COMPONENT-LEVEL ATTACKS

Given our routing and attacker models, we can now study how different attackers may attack different functions. Clearly, these attacks are usually particularly harmful when conducted by an insider attacker: e.g., if the attacker has also compromised some nodes and controls all the routing components. See Figure 1 for an overview.

4.1 Transport Service

Attacks on the transport service include the following.

- **Injection:** an attacker may inject packets into the communication channels used by the transport service, e.g., for the purpose of covert communication. In our taxonomy, manipulation also falls under this category.[1] An attacker may leverage the transport service and modify control packets to affect the functionality of the routing service (e.g., create black holes) or data packets to corrupt the communicated information (integrity violation). Manipulation is not limited to packet contents (both header and payload), but can also arise in the form of message delays, reordering, omissions, etc., harming performance and integrity. An attack on the identity resolution protocol may also be exploited to inject wrong control information (e.g., for exfiltration purposes) or to launch a man-in-the-middle attack, thus attacking confidentiality.

- **Eavesdropping:** an attacker may sniff transport traffic, e.g., to learn about confidential topological details (weak points for subsequent attacks).

- **Preventing communication**: an attacker can prevent the communication to take place by performing a denial-of-service against the transport protocol itself.

We note that if the transport service provides protection such as authentication, integrity and confidentiality, then several of the aforementioned attacks will not be feasible in the case of an outside attacker. An inside attacker however will have access to the cryptographic keys and thus be able to bypass the cryptographic protection mechanisms.

As the topology service relies on the transport service for its correctness, an attacker can influence the former by attacking the latter.

4.2 Topology Service

The topology service can be attacked along the following dimensions.

- **Database attack:** by directly attacking the topology database (read, add, delete, change), an attacker can divert traffic and harm availability and confidentiality.

- **Neighbor discovery attack:** by attacking the neighbor discovery (remove/mask neighbors), an attacker may, for instance, create wormholes or artificially generate some very highly connected nodes in the network.

- **Correctness of topological views:** by attacking the correctness of distributed topological views, and attacker may introduce, for example, forwarding loops, harming the availability and possibly the correctness.

4.3 Route Computation Service

Attacks on the route computation service include:

- **Drop:** by not forwarding packets, an attacker can harm the availability of the routing system.

- **Incorrect Forwarding:** by forwarding packets to the wrong ports, an attacker can violate the confidentiality of traffic. For example, an attacker can exfiltrate information.

- **Change header fields:** a more sophisticated attacker may also simply change the packet information during forwarding. For example, by changing the VLAN tags, an attacker may be able to exfiltrate information, again violating confidentiality.

- **Route computation**: an attacker which can influence the routing algorithm (e.g., taking control over an SDN controller), can severely violate availability and confidentiality of the routing service.

[1]Injection and manipulation differ in terms of security: e.g., while digital signatures often help to detect modification, they usually do not help against injection.

4.4 Identity Resolution

The identity resolution service can be attacked on the following fronts:

- **Impersonation attack:** an attacker may aim to impersonate other identities. For example, it may aim to compromise the DNS system or spoof IP addresses. Impersonation may be as simple as conducting a replay attack. Besides harming confidentiality (confidential information is communicated to illicit recipients), it can also threaten the network availability (communication between the originally intended destination is no longer possible).
- **Sybil attack:** an attacker may can create a large number of identities, e.g., in an effort to harm the availability of the routing service by consuming excessive resources.

5. QUANTIFYING ATTACK IMPACT

Given our taxonomy, we observe that most security aspects related to our routing functions eventually revolve around the information used and communicated in the control plane: how nodes learn about identities, how control and topology information is propagated, how forwarding tables are defined, etc.

Eventually, the goal of an attack on the routing system is usually to influence paths along which packets are routed. In a basic case, if an attacker controls a router directly, this can be achieved by forwarding the packet to the wrong port. While a single incorrect forwarding decision may already violate logical isolation domains and may be used to exfiltrate confidential information, its range and impact is usually limited. Clearly, the more devices an attacker controls, the more flexibility it has, and the more severe are the possible attacks.

An interesting question hence concerns whether an attacker can influence the path of a packet beyond the components directly under its control. The answer is obviously yes: if no countermeasures are taken, an attacker may change the header fields in the packet when it is passing through the router directly controlled by it. For example, if the router changes the destination IP-address, the packet may be forwarded wrongfully, far beyond the malicious router.

However, an attacker may not only change the fate of individual packets, but even the configuration of other, remote, routers: namely if the attack concerns the information available to the control stack. For example, by attacking the information communicated by the MAC learning protocol, or information related to the link status (availability, weights, etc.), an attacker may trigger wrong forwarding rules in other switches.

To quantify the impact of the attacker, we propose the following notion of *reach*: how far from the devices under direct (partial) control of an attacker, can the routing be manipulated? The reach comes in two flavors: *packet reach* (how far can a packet travel off its intended path?) and *configuration reach* (how far away can the attacker still influence router/switch configurations?).

While a precise definition is beyond the scope of this paper and future work, we provide some intuition. For example, a prefix hijacking attack may have a potentially very high reach: attack packets are rerouted on a global scale. An ARP spoofing attack on the other hand might have a more local reach. Moreover, an attacker who controls a router and which is able to change the IP destination address of a packet, can potentially divert the packet in arbitrary ways. But also a packet drop (e.g., as part of a denial-of-service attack) can, in some sense, entail an unbounded reach.

6. RELATED WORK

Although we are not aware of any prior work that attempted to provide a detailed taxonomy and attacker model for secure routing protocols, we briefly review the most closely related works.

Hu et al. [9] propose to characterize the security of a routing protocol by the strength of the adversary, which is characterized by the number of physical entities the adversary controls, the amount of cryptographic secrets the adversary possesses, and the topological position of the adversary. For instance, an Active-VC adversary controls a vertex cut through the network, or an Active-x-y adversary has compromised the secrets of x legitimate network nodes and controls y physical network nodes. Unfortunately, this approach makes it difficult to compare the relative strength of two routing protocols, if, for example, one protocol can withstand an Active-1-3 adversary and the other an Active-2-1 adversary.

Chan et al. [5] propose to evaluate the adoptability of secure inter-domain routing protocols by simulating how the global adoption of the routing protocol is dependent on the deployment threshold of each individual ISP. In their model, an ISP would deploy the secure routing protocol if the protection offered to their customers surpasses the adoption cost. Goldberg et al. [7] extend their model to more closely model economic aspects.

Several researchers present attack analyses of secure routing protocols. Karlof and Wagner present a list of attacks and countermeasures on sensor network routing protocols [10]. Pei et al. [17] present a fault tree and defense model for routing protocols. Hu and Perrig [8] present a survey of secure ad hoc network routing protocols. Barbir et al. [3] Butler et al. [4] analyze the security of several proposed secure BGP protocols. Lychev et al. [12] analyze the security of BGPsec in a partial deployment.

In terms of specification of secure routing, Papadimitratos et al [15] define correctness properties for secure route discovery, motivated by ad hoc networks. Attacker coordination (collusion) in this context was introduced earlier [14], pointing out unavoidable topology distortion such attackers can achieve at the network layer. Reaction to the adverse effects of routing attacks, with end-to-end [16] or in-netwrok [6] adaptation has been investigated. At the data-link layer, secure neighbor discovery was formally investigated by Poturalski et al. [18], with an impossibility result for a class of wireless protocols and new proven correct ones.

7. CONCLUSION

With this paper, we want to initiate the discussion of a taxonomy for secure routing protocols, a relevant yet underexplored field of research. We believe that a structured approach can help answering important questions such as the following:

- Is there a need to adapt routing to facilitate and take advantage of cloud services? Or can the routing system take care of in-network security aspects of such services?

- Is there a need to fundamentally adjust how routing systems are conceived to the increased threat of Denial-of-Service attacks?
- Can the widespread provision of Quality-of-Service be facilitated simultaneously with introducing secure routing services?
- How can the Software Defined Networking (SDN) paradigm and Network Function Virtualization (NFV) be leveraged to support a secure routing system?
- Is there a need to modify routing and its security mechanisms, as a result of the recent revelations regarding the scope of abuse of routing by powerful nation-state attackers?
- How can attacks such as censorship or protection goals such as anonymity be integrated with secure routing systems?

All these questions pursue to bring attention to address the security issues outlined in this article. However, this requires a constant process: if some modifications were introduced in order to attain these goals, one needs to reassess how the routing system attack surface changes. We encourage both the security as well as the networking community to further this discussion towards a more comprehensive taxonomy on routing security.

Acknowledgments. The discussions leading to this editorial were initiated during Dagstuhl Seminar 15102 on *Secure Routing for Future Communication Networks*, and we thank all participants for their contributions. We would also like to thank Liron Schiff and Kashyap Thimmaraju for fruitful inputs and feedback on this paper. Stefan Schmid is supported by the Danish Villum grant *ReNet*.

8. REFERENCES

[1] Netis routers leave wide open backdoor. http://blog.trendmicro.com/trendlabs-security-intelligence/netis-routers-leave-wide-open-backdoor/, 2014.

[2] H. Ballani, P. Francis, and X. Zhang. A study of prefix hijacking and interception in the internet. In *Proc. ACM SIGCOMM*, pages 265–276, 2007.

[3] A. Barbir, S. Murphy, and Y. Yang. Generic threats to routing protocols. *Request for Comments 4593*, 2006.

[4] K. Butler, T. Farley, P. McDaniel, and J. Rexford. A survey of bgp security issues and solutions. *Proceedings of the IEEE*, 98(1):100–122, 2010.

[5] H. Chan, D. Dash, A. Perrig, and H. Zhang. Modeling adoptability of secure BGP protocols. In *Proc. ACM SIGCOMM*, Sept. 2006.

[6] W. Galuba, P. Papadimitratos, M. Poturalski, K. Aberer, Z. Despotovic, and W. Kellerer. Castor: Scalable Secure Routing for Ad Hoc Networks. In *IEEE INFOCOM*, pages 1–9, San Diego, CA, USA, March 2010.

[7] S. Goldberg, M. Schapira, P. Hummon, and J. Rexford. How secure are secure interdomain routing protocols. In *Proc. ACM SIGCOMM*, 2010.

[8] Y.-C. Hu and A. Perrig. A survey of secure wireless ad hoc routing. *IEEE Security and Privacy*, 2(3):28–39, May 2004.

[9] Y.-C. Hu, A. Perrig, and D. B. Johnson. Ariadne: A secure on-demand routing protocol for ad hoc networks. *Wireless Networks*, 11(1):21–38, 2005.

[10] C. Karlof and D. Wagner. Secure routing in wireless sensor networks: Attacks and countermeasures. *Elsevier's AdHoc Networks Journal, Special Issue on Sensor Network Applications and Protocols*, 1(2–3):293–315, Sept. 2003.

[11] F. Lindner. Cisco ios router exploitation. *Black Hat USA*, 2009.

[12] R. Lychev, S. Goldberg, and M. Schapira. BGP security in partial deployment. is the juice worth the squeeze? In *Proc. ACM SIGCOMM*, 2013.

[13] D. Montgomery and S. Murphy. Toward secure routing infrastructures. *Security Privacy, IEEE*, 4(5):84–87, 2006.

[14] P. Papadimitratos and Z. Haas. Secure Routing for Mobile Ad Hoc Networks. In *SCS CNDS*, pages 193–204, San Antonio, TX, USA, January 2002.

[15] P. Papadimitratos, Z. Haas, and J. Hubaux. How to Specify and How to Prove Correctness of Secure Routing Protocols for MANET. In *IEEE-CS Third International Conference on BroadBand Communcations, Networks, and Systems*, 2006.

[16] P. Papadimitratos and Z. J. Haas. Secure Data Communication in Mobile Ad Hoc Networks. *IEEE Journal on Selected Areas in Communications*, 24(2):343–356, February 2006.

[17] D. Pei, L. Zhang, and D. Massey. A framework for resilient internet routing protocols. *IEEE Network*, 18(2):5–12, Apr. 2004.

[18] M. Poturalski, P. Papadimitratos, and J. P. Hubaux. Formal Analysis of Secure Neighbor Discovery in Wireless Networks. *IEEE Trans. on Dependable and Secure Computing*, 10(6):355–367, Nov 2013.

[19] B. Snyder. Snowden: The nsa planted backdoors in cisco products. *InfoWorld*, 2014.