An Analysis of Routing-Layer Attacks: Wormhole and Sinkhole Exploits

Aditya Prabhu
CIT, Purdue University
CNIT 271

John Mills
CIT, Purdue University
CNIT 271

***Abstract*—This paper will investigate and report on two fundamental types of routing-based network attacks –wormhole attacks and sinkhole attacks–in which threat actors exploit routing protocols to redirect, intercept, or alter data flows. Through analyzing the means and implications of these attacks, this work will exemplify the severity of the threats and introduce potential countermeasures.**

I. Introduction

In today's internet-dependent world, it is incredibly imperative that network routing, the backbone of the internet, is maintained with integrity and reliability. Although the fundamental protocols and frameworks that support the internet have now been around for decades, sophisticated adversaries routinely exploit routing assumptions and trusts to manipulate data flows. This paper examines two such threats under this umbrella. Wormhole attacks often target wireless or ad-hoc networks by creating virtual 'tunnels' that mislead normal network traffic. Sinkhole attacks, particularly BGP hijacking, deceive global internet routing tables to intercept or reroute traffic. By analyzing these attacks in unison, we will illuminate their shared characteristics as trust-exploitation mechanisms within the routing infrastructure and identify common insights that may inform more resilient defense strategies.

II. Background and Motivation

The integrity of network routing depends on a fragile web of trust initially designed in an era when security was not at the forefront of design. Routers and nodes are presumed to advertise accurate and timely route information, and when this inherent trust is subverted, threat actors can gain considerable power. Wormhole attacks, commonly observed in wireless and sensor networks, exploit geographic and timing assumptions, effectively bending the network's topology to route traffic through malicious nodes which appear most efficient (Pawar et al., 2015). Similarly, sinkhole attacks—especially those considered BGP hijacking—misuse the Internet's universal trust in route advertisements, potentially allowing attackers to direct massive portions of global traffic into compromised domains. By examining both attack vectors, we not only obtain insight into the weaknesses of routing architectures but also identify overarching principles of route authentication, path verification, and trust establishment that can inform defense strategies across a range of networking contexts. The motivation for this combined study, therefore, is to forge a more holistic understanding of routing vulnerabilities and to inspire robust, universal countermeasures.

III. Cybersecurity Issues

A. Wormhole Attacks

A wormhole attack occurs when attackers create an illicit shortcut between two distant points in a network. This shortcut allows data packets to be transferred between these points as if they were neighbors, deceiving the network's routing protocols (Hu et al., n.d.). Such attacks are particularly dangerous in wireless ad-hoc networks and can disrupt normal network operations by capturing, rerouting, or dropping packets. There are generally two types of wormhole attacks: in-band attacks and out-of-band attacks. This paper will focus more on in-band attacks. An In-band wormhole (Prajapati & Agrawal, 2014) does not use an external communication medium to develop the link between the colluding nodes. Instead, it

develops a covert overlay tunnel over the existing wireless medium.

Malicious actors generally exploit **vulnerabilities** found in **trust-based systems** to conduct such attacks. These systems essentially use protocols that do not require rigorous verification of routing data such as AODV (Ad Hoc on Demand Distance Vector) and DSR (Dynamic source routing). We shall look into the exploitation of the DSR protocol in order to create vulnerabilities. There are multiple ways this protocol is exploited (Qazi et al., 2013), these include the creation of a wormhole using high-power transmission, or a more common attack called packet relay. In this attack, a malicious node tries to convince two far nodes that they are neighbors by relaying packets between them. A single malicious node can achieve this, and the presence of additional malicious nodes can extend the list of neighboring nodes for the victims across multiple hops. Imagine node X and node Y, which are not direct neighbors, but share a common malicious neighbor, node M1. Node M1 can transfer packets between nodes X and Y, creating the false impression that they are directly connected as neighbors. This can severely disrupt the network and routing calculations.

Not only is the disruption a threat but there are also multiple threats including data interception where the attacker, by positioning themselves on the routing path, intercepts, modifies, or even drops packets passing through. An additional threat, resource depletion, occurs when the wormhole depletes the nodes(in networks with sensors where battery efficiency is important) through inefficient transmission paths.

B. Sinkhole Attacks

BGP Hijacking enables Sinkhole Attacks. Border Gateway Protocol (BGP) hijacking is a critical vulnerability in inter-domain routing that enables attackers to misdirect network traffic. BGP operates on a trust-based model, where Autonomous Systems (ASes) advertise IP prefixes and routing paths without any verification mechanisms inherently built-in (Cho et al., 2019). Malicious actors exploit this inherent trust by announcing IP prefixes they do not own, thus manipulating ASes into directing traffic to malicious systems. This unauthorized attraction of traffic is the essence of a Sinkhole network attack: threat actors intercept traffic intended for legitimate destinations and either discard it or analyze it for malicious purposes.

The vulnerability lies in the susceptibility of BGP to forged AS paths. In this scenario, a threat actor modifies the routing announcements to include their AS as a legitimate intermediary or endpoint, effectively diverting traffic into their systems. These forged paths are often crafted to evade detection by mimicking legitimate configurations (Cho et al., 2019). BGP's lack of an inherent authentication method between ASes is the crux of the vulnerability.

Mechanisms of Exploitation. BGP hijacking attacks exploit misconfigurations and design limitations of the BGP protocol. Hijacking events can generally be grouped into five categories based on attack vector.

- **Typos** are mistakes in AS numbers or prefixes during router configuration which can inadvertently create opportunities for hijacking. For example, an operator may mistype a prefix, resulting in a more specific prefix being announced by a malicious actor and taking precedence over the legitimate traffic (Cho et al., 2019).
- **Prepending** occurs when operators attempt to manipulate traffic flow by adding their AS multiple times to a route's path. Errors in this process can allow attackers to impersonate the intended AS and redirect traffic (Cho et al., 2019).
- **Origin Manipulation** involves attackers announcing IP prefixes they do not own with optimized routing paths to make their announcements preferable to legitimate ones. Thus, the BGP path selection process, which prioritizes shorter paths, is exploited. Traffic destined for the legitimate AS is then diverted to the attacker (Cho et al., 2019).
- Not to be confused with Origin Manipulation, **Forged AS Paths** involve manipulation of the AS path itself to include false information. Attackers may claim proximity to a legitimate AS or forge a connection to a trusted enemy, allowing the malicious system to intercept traffic while appearing as a legitimate route. (Cho et al., 2019).

IV. Possible solutions and Results

A. Wormhole Attack Countermeasures

Multiple countermeasures for Wormhole attacks have been researched and implemented by different researchers and organizations. One of the most common includes the usage of packet leashes, as proposed by Hu et al. This countermeasure introduces the concept of geographical and temporal packet leashes. These leashes are added to the packet and contain each node's own locations and a loosely synchronized clock. The geographical leash ensures that the distance between the sender and the recipient is within certain limits. Additionally, the temporal leash ensures that all packets have an upper bound on their lifetime, restricting the maximum travel distance.

Capkun et al. (2003) developed a method to detect wormhole attacks without needing synchronized clocks. This method, called MAD (Mutual Authentication with Distance Bounding), involves one node sending a quick one-bit challenge to another node, which responds immediately. By measuring the time it takes for the response to come back, the first node can figure out if the second node is actually close by. This technique requires a special hardware module that can quickly manage the radio transceiver to respond instantly, bypassing normal message processing delays.

Khalil et al. (2005) introduced a simple and efficient protocol named LITEWORP, designed to detect and counteract wormhole attacks in static wireless ad hoc and sensor networks. LITEWORP performs secure two-hop neighbor discovery and monitors control traffic locally to spot wormhole nodes. It also effectively isolates these malicious nodes without needing specialized equipment like directional antennas or precise clocks. Importantly, LITEWORP doesn't require nodes to be time-synchronized and doesn't increase packet size, thus causing only minimal impact on bandwidth during the initial setup and wormhole detection phases. Additionally, the system is carefully designed to minimize the risk of mistakenly identifying normal nodes as malicious due to routine network collisions or deliberate interference.

B. Sinkhole Attack Countermeasures

As BGP was not initially designed with a security mindset, potential solutions to its inherent vulnerabilities have been floated for decades. The ARTEMIS system (Automatic and Real-Time Detection and Mitigation System) offers a novel solution to the vulnerabilities inherent in BGP. These vulnerabilities, rooted in the lack of authentication and trust-based architecture, make the protocol susceptible to prefix hijacking. ARTEMIS is an automated system designed to detect and mitigate hijacking events.

ARTEMIS can identify all attack configurations by monitoring BGP updates in real-time through publicly-available monitoring services like RIPE, RIS, and RouteViews. It relies on a local configuration file maintained by the ARTEMIS operator, which includes a list of routing policies, owned prefixes, and AS neighbors. (Sermpezis et al., 2018).

The system can neutralize hijacking events within minutes, significantly reducing the impact of attacks compared to conventional/manual approaches which may take hours or days. By automating the mitigation process, ARTEMIS enables almost-immediate responses.

ARTEMIS can perform Prefix Deaggregation which involves announcing more specific sub-prefixes of the hijacked prefix. For example, if a /23 prefix is hijacked, the system can leverage BGP's longest-prefix match rule by announcing two /24 sub-prefixes. This strategy is particularly effective for prefixes of /23 or less specificity, as routers usually filter more-specific prefixes like /25 (Sermpezis et al., 2018).

ARTEMIS can also outsource mitigation efforts by notifying third-party organizations to announce the hijacked prefix. These organizations, acting as trusted intermediaries, can utilize secure tunneling to direct traffic back to the victim AS. Outsourcing is especially useful for smaller networks or scenarios where the prefix is critical to operations, such as financial services/institutions (Sermpezis et al., 2018).

Conclusions

In this review, the threats posed by wormhole and sinkhole attacks to network routing systems have been examined. Dangerous vulnerabilities which arise from inherent trust/assumptions within routing protocols have been presented. Wormhole attacks manipulate network topology to mislead routing paths, while Sinkhole attacks, particularly BGP hijacking, exploit global internet routing to intercept and reroute traffic. Both Sinkhole and Wormhole attacks showcase how trust-based protocols can be exploited to cause disruptions, security breaches, and depletion/dropping of resources.

By exploring various countermeasures such as ARTEMIS and advanced techniques like packet leashes or MAD, this review underscores the feasibility of vulnerability-tailored defense mechanisms. The solutions identified and vulnerabilities exposed emphasize the importance of implementing authentication, real-time monitoring, and efficient detection mechanisms in order to safeguard network integrity.

As routing infrastructures continue to serve as the foundation of the global internet, their security must evolve to withstand increasingly sophisticated threats. Future research should centralize on enhancing protocol resilience, minimizing response times, and the deployment of scalable, proactive defense solutions. The authors of this review hope to inspire continued innovation in the fortification of networks against the growing pool of potential threat actors.

References

[1] Cho, S., Fontugne, R., Cho, K., Dainotti, A., & Gill, P. (2019, June). BGP hijacking classification. In 2019 Network Traffic Measurement and Analysis Conference (TMA) (pp. 25-32). IEEE.

[2] Hu, Y.-C. ., Perrig, A., & Johnson, D. B. (n.d.). Packet leashes: a defense against wormhole attacks in wireless networks. IEEE INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies (IEEE Cat. No.03CH37428).

[3] Khalil, I., Bagchi, S., & Shroff, N. B. (2005). LITEWORP: A Lightweight Countermeasure for the Wormhole Attack in Multihop Wireless Networks. https://doi.org/10.1109/dsn.2005.58

[4] Pawar, M. V., & Anuradha, J. (2015). Network security and types of attacks in network. Procedia Computer Science, 48, 503-506.

[5] Prajapati, H., & Agrawal, R. (2014). Techniques for Detection & Avoidance of Wormhole Attack in Wireless Ad Hoc Networks. International Journal of Enhanced Research in Management & Computer Applications, 3, 21–27

[6] Qazi, S., Raad, R., Mu, Y., & Susilo, W. (2013). Securing DSR against wormhole attacks in multirate ad hoc networks. Journal of Network and Computer Applications, 36(2), 582–592. https://doi.org/10.1016/j.jnca.2012.12.019

[7] Sermpezis, P., Kotronis, V., Gigis, P., Dimitropoulos, X., Cicalese, D., King, A., & Dainotti, A. (2018). ARTEMIS: Neutralizing BGP hijacking within a minute. IEEE/ACM transactions on networking, 26(6), 2471-2486.

[8] Srdjan Capkun, Levente Buttyán, & Jean-Pierre Hubaux. (2003). SECTOR. Security of Ad Hoc and Sensor Networks. https://doi.org/10.1145/986858.986862