Wormholes in Space: Unveiling Wormhole Attack in Low Earth Orbit Satellite Networks

Xiaojian Wang
University of Colorado Denver
Denver, CO, USA
xiaojian.wang@ucdenver.edu

Ruozhou Yu
North Carolina State University
Raleigh, NC, USA
ryu5@ncsu.edu

Dejun Yang
Colorado School of Mines
Golden, CO, USA
djyang@mines.edu

***Abstract*—With the development of Low Earth Orbit (LEO) satellite networks (LSNs) and the decreasing costs of satellite manufacturing and deployment, an increasing number of satellites are being placed in low Earth orbit to provide global, low-latency internet services. However, current satellite communications are characterized by high dynamism, unstable connections, routine configurations, and overall higher latency compared to terrestrial networks, making them inherently less stable. This creates new opportunities for attackers, who can establish a fast and stable tunnel through terrestrial networks to redirect messages or traffic within the satellite network, thereby enabling a specific form of attack. In this paper, we present a novel attack in which an adversary deploys wormholes on satellites in an LSN to mislead routing and aggressively attract traffic from target areas, thereby enabling large-scale eavesdropping and severely compromising network security. We formally formulate the objectives and constraints of the attack, taking into account the wormhole's unique space-ground coupling in the LSN, its predictable dynamics, coverage limitations, and resource constraints. Additionally, we propose an algorithm to derive the optimal attack strategy. We demonstrate that strategically placed wormholes can intercept a significant portion of traffic across target areas, with the extent of impact varying based on the available budget and temporal variation in traffic demand. Finally, we propose countermeasures of wormhole attack, and highlight the potential of enhancing the attack in future work.**

***Index Terms*—Satellite network, low earth orbit, security, attack, routing disruption, traffic attraction**

I. Introduction

With the decreasing costs of satellite manufacturing and deployment, companies such as SpaceX [1], Amazon [2], and OneWeb [3] are actively developing large-scale Low Earth Orbit (LEO) satellite constellations to build LEO satellite networks (LSNs). These networks are designed to provide low-latency communication, high bandwidth, and seamless global Internet coverage. LSNs enable a broad range of applications, including remote communication, disaster management, maritime and aviation connectivity, and supporting IoT infrastructure in regions where terrestrial networks are unavailable.

Despite the potential benefits of LSNs, recent measurements of LEO satellite constellations [4]–[6] indicate that their actual performance often falls short of expectations. The high dynamism of satellite movement, unstable connections, frequent handovers, routine configurations, environmental factors, and limited ground infrastructure result in end-to-end delays for users in many regions that can be several times higher than those of terrestrial networks. The excessive delay not only degrades user experience but also opens the door for attackers to exploit latency asymmetries for strategic attacks.

A wormhole is a hypothetical spacetime tunnel predicted by Einstein's theory, providing a shortcut between distant points [7]. Wormhole attacks [8] exploit low-latency tunnels to manipulate network topology, enabling routing manipulation, communication disruption, and man-in-the-middle attacks [9], [10]. Their covert nature and ability to bypass cryptographic protections [11] make them highly dangerous. However, wormhole attacks should no longer be viewed as a purely terrestrial threat, as the increasing deployment of satellites in large-scale networks introduces new opportunities to exploit their communication architecture and the latency asymmetries between space and ground networks.

In contested military or high-security regions, critical operations often rely on LSNs, making them appealing targets for attackers. By strategically deploying wormholes, an adversary can intercept traffic, extract sensitive data, and disrupt key communications, thereby undermining network reliability.

Unlike terrestrial wormholes, which are typically static once established, allowing continuous exploitation as long as traffic in a given region passes through a fixed endpoint, wormholes in space are inherently dynamic due to satellite mobility. In such networks, the satellites relaying regional traffic change over time, complicating the establishment and persistence of wormholes. Successful attacks must therefore adapt to this mobility through precise spatiotemporal coordination between space and ground segments. Beyond mobility, effective attack deployment must also operate under strict budget constraints, adding another layer of difficulty.

We adopt the perspective of an attacker to investigate the strategic deployment of wormholes in LSNs: How can an attacker determine the optimal spatiotemporal placement of wormholes under budget constraints to maximize effectiveness and impact? To the best of our knowledge, this is the first formal study to model and analyze wormhole attacks in LSNs. We propose a wormhole placement optimization problem with both wormhole endpoints located in space, aiming to maximize intercepted traffic while accounting for coverage constraints, budget limitations, and satellite mobility. To address this problem, we develop an optimization algorithm that determines effective wormhole placements over time. Our results show that effective wormhole placement, determined by

This research was supported in part by NSF grants 2045539, 2414523, 2433966 and 2414522. The information reported here does not reflect the position or the policy of the federal government.

both the timing and the choice of the compromised satellite, can compromise a substantial share of traffic in the target areas, with the impact further shaped by budget constraints and temporal factors.

The contribution of this paper is listed as follows:

- We introduce a novel wormhole attack that exploits the unique properties of LSNs to intercept and/or disrupt space-based communications.
- We formulate and solve an optimization problem for the spatiotemporal placement of wormholes under budget constraints to maximize intercepted traffic while accounting for coverage limitations and satellite dynamics.
- We evaluate the proposed attack using real-world satellite dynamics and time-varying user traffic distributions. Experimental results demonstrate its effectiveness in compromising targeted communications.

Organization. The rest of the paper is organized as follows. §II reviews the background and related work. §III formalizes the system model. §IV presents the wormhole attack. §V presents the evaluation results. §VI describes some countermeasures against the proposed attack. §VII presents the discussion and future work. §VIII concludes the paper.

II. Background and Related Work

A. Dynamic Routing in Low Earth Orbit Satellite Networks

LSNs operate in low Earth orbit, typically within 2,000 km of the Earth's surface, providing global coverage and high-speed internet access, especially in remote or underserved regions. An LSN constellation consists of numerous small satellites deployed across multiple orbital planes to ensure continuous coverage. These constellations follow specific topologies, such as Walker-Delta which used by SpaceX [1] and Walker-Star which used by Oneweb [3], to optimize coverage and efficiency. Satellites in the same or nearby orbits communicate, route, and forward data via inter-satellite links.

Dynamic distributed routing has been widely explored in LSNs to address the challenges posed by their constantly changing topology. By enabling real-time sensing of network states, such as traffic load variations and link congestion, dynamic distributed routing enhances adaptability, optimizes resource utilization, and ensures efficient and reliable data transmission [12], [13]. A distributed datagram routing approach minimizes propagation delay by dynamically selecting the next hop based on real-time delay and congestion status is proposed in [14]. LCPR improves load balancing by dynamically selecting the next hop through congestion state exchanges with neighboring satellites [15]. DODR, an on-demand distance vector protocol, efficiently chooses the next hop to bypass failed links, reducing end-to-end delay with minimal overhead [16]. A routing broadcast strategy optimizes next-hop selection by updating the route table to mitigate packet loss and balance traffic load from users within the same geographical subnet is proposed in [17]. Queue state-based dynamic routing can optimize next-hop selection by detecting queuing delays and predicting congestion. Examples include QSDR, which dynamically balances traffic load, and CEMR, which periodically exchanges expected queuing delays to improve routing efficiency [18], [19].

Although extensive research has focused on dynamic routing in LSNs, the notorious wormhole attack has not yet been studied in this context. Addressing this gap is critical for ensuring secure and reliable LSN network operation.

B. Related Work

1) Attacks in LSNs: Given the unique characteristics of LSNs, such as dynamic topology, high mobility, and limited resources, various attacks have been explored in the literature.

Existing research on security threats in LSNs can be categorized into several areas. Some works focus on compromising the location privacy of terminal users [20], [21], while others address software and protocol security vulnerabilities in satellite systems [22]–[24]. Several studies have explored the Link Flooding Attack (LFA), a denial-of-service attack that targets ISLs by overwhelming the network with excessive traffic, leading to congestion and service disruptions [25], [26]. The energy drain attack exploits botnets to inject malicious traffic, depleting satellite energy reserves and disrupting operations [27]. The StarMaze attack, a ring-based strategy, manipulates a set of ISLs to either degrade network service or force routing detours [28]. However, these attacks either fail to consider how different routing protocols influence their effectiveness or overlook the possibility of coordinated space-terrestrial attacks. To the best of our knowledge, we are the first to investigate the impact of attacks on dynamic routing protocols, addressing both space and terrestrial dimensions.

2) Wormhole Attacks in Wireless Sensor Networks: The wormhole attack [8] is one of the most severe threats to wireless sensor networks (WSNs) and has been successfully implemented in real-world scenarios [9], [10]. In this kind of attack, an adversary controls one or more pairs of nodes across different locations in the network, intercepts packets at one location, and forwards them through an out-of-band low-latency tunnel to a distant location, where they are replayed as if they originated locally. This manipulation distorts the network's topology, misleading legitimate nodes and enabling further exploitation, such as routing manipulation, communication disruption, man-in-the-middle attacks and network partitioning. Wormhole attacks are particularly dangerous due to their covert nature, making detection extremely challenging, while their ability to bypass cryptographic protections and operate on encrypted traffic [11] further amplifies their impact on overall network functionality. Some works focus on maximizing the effectiveness of wormhole attacks by leveraging edge betweenness centrality [29]. Others are more related to countermeasures, aiming to detect and mitigate wormhole attacks through various techniques [11], [30].

Wormhole attacks should no longer be seen as exclusive to terrestrial networks. In space, attackers can exploit latency asymmetries together with the predictable nature of satellite coverage and orbits, creating new vulnerabilities in LSNs. We are the first to formally model and optimize such attacks.

III. System Model

A. LSNs Model

Network Model. We consider an LSN composed of a set of satellites interconnected through Inter-Satellite Links (ISLs). The network is modeled as a time-slotted graph, where the set of discrete time steps is given by $\mathcal{T} = \{1, 2, \ldots, T_{\max}\}$. At each time step $t \in \mathcal{T}$, the network is represented by a time-varying graph $\mathcal{G}_t = (\mathcal{V}, \mathcal{E}_t)$, where $\mathcal{V}$ denotes the set of satellites, and $\mathcal{E}_t$ represents the set of active ISLs at time t. Motivated by recent advances in dynamic routing for satellite networks [12], [31], we model LSNs as employing protocols where satellites broadcast local congestion, delay, and load metrics to optimize next-hop selection and improve overall performance.

Traffic Model. We consider users on the ground who utilize the LSNs to communicate with each other. A request is represented by a tuple $r = (s_r, d_r, t_r, f_r)$, where s_r and d_r denote the source and destination ground users, t_r is the request time, and f_r is the flow amount. The set of all requests is denoted by $\mathcal{R}$. Traffic in LSNs is routed through ISLs using dynamic routing, with the gateway satellite selected deterministically according to predefined criteria, such as minimizing latency or maximizing connectivity stability.

B. Threat Model

Attacker's Goal. The attacker aims to exploit the LSN to intercept critical communications within a target area Ω, such as a military zone or other strategically significant region. Over a designated time period $\mathbb{T} \subseteq \mathcal{T}$, the attacker seeks to attract and intercept as much traffic through Ω as possible.

Attacker's Capabilities. Suppose the attacker can either take control of an existing ground station or establish a new one. In practice, this is feasible because community ground station networks such as SatNOGS [32], a global open-source participatory project, allow users to deploy their own ground stations and integrate them into the broader network. The attacker-controlled ground stations can establish a fast tunnel via the terrestrial network, enabling low-latency communication between them and functioning as tunnel endpoints. We consider a scenario where the attacker controls two such ground stations, G_A and G_B, with one located in the target area Ω. Without loss of generality, we assume that G_A is within Ω.

An attacker-controlled ground station can issue commands to a satellite, causing it to broadcast false load or congestion data and manipulate next-hop selection. This manipulation redirects surrounding traffic to the compromised satellite, which bypasses normal ISL routing and sends it directly to the tunnel endpoint G_A. The traffic then passes through the tunnel between G_A and G_B, where it is forwarded to another attacker-controlled satellite connected to G_B, which receives the traffic and reinjects it into the LSN. Considering factors such as antenna alignment and operational constraints, we assume that an attacker-controlled ground station can control only one satellite at a time.

Coverage and Wormhole Indicators. We define binary coverage indicators $\Lambda_v^A(t)$ and $\Lambda_v^B(t)$, where $\Lambda_v^A(t) = 1$ if satellite v can connect to G_A at time t, and 0 otherwise. $\Lambda_v^B(t)$ is defined analogously for G_B. We also define wormhole indicators $w_A^v(t)$ and $w_B^v(t)$. $w_A^v(t) = 1$ indicates that satellite v is selected as a wormhole connected to G_A at time t, meaning it is compromised and can receive commands to alter its behavior. The definition of $w_B^v(t)$ for G_B is analogous. A satellite can be selected as a wormhole endpoint only when its coverage indicator equals 1, indicating that it is within the attacker's control range.

Cost and Budget. Controlling a satellite by sending commands and altering its behavior incurs costs, such as energy consumption and operational expenses. For example, transmitting and maintaining control signals require energy and communication resources, especially in long-distance and spectrum-constrained environments. Additionally, forging legitimate instructions may require bypassing authentication mechanisms, which consumes computational resources. We define c_A^v as the cost of using satellite v as a wormhole endpoint for G_A for a time, including sending malicious messages and altering its behavior. Similarly, c_B^v represents the corresponding cost for G_B. These costs are considered separately, as they may depend on the geographical location of the ground station or other factors. The attacker operates under a total budget constraint denoted by Π.

IV. Wormhole Attack in LSNs

Given a target area of interest, such as a military zone or a region of strategic importance, the attacker seeks to maximize the interception and analysis of traffic from this area to gather intelligence. To achieve this under limited budget constraints, coverage limitations, dynamic satellite movement, and attacker capabilities, the attacker strategically optimizes wormhole deployment to maximize valuable traffic capture.

This is accomplished by sending commands to satellites from an attacker-controlled ground station, turning satellites into wormhole points. The compromised satellites then broadcast deceptive information, such as artificially low queue occupancy, minimal load, and reduced delay, to mislead neighboring satellites into selecting them as the next hop. Even if target area users do not directly choose a compromised satellite as a gateway, their traffic can still be redirected to the wormhole if it is forwarded to a neighboring satellite, which may then relay it to the wormhole.

After being trapped by the wormhole endpoint, the traffic is forwarded to the terrestrial tunnel endpoint, G_A, and then relayed through a low-latency terrestrial tunnel to another tunnel endpoint, G_B. To remain undetected during the reconnaissance phase, the attacker must ensure that the traffic ultimately returns to the LSN. To achieve this, G_B compromises another satellite to serve as a wormhole endpoint, allowing it to forward the intercepted traffic back into the network. By this point, by manipulating dynamic routing and leveraging the terrestrial tunnel, the attacker has attracted traffic from the

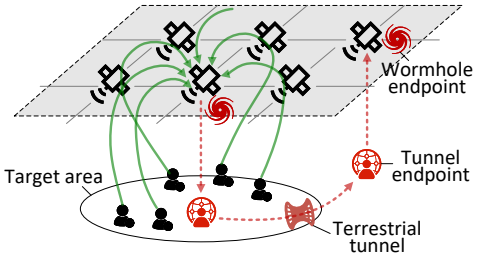


Fig. 1. Wormhole attack in LSN.

coverage area of the wormhole satellite connected to G_A during each active attack time slot.

The overall process of wormhole attack is illustrated in Fig. 1. Given the constrained budget Π and the dynamic movement of satellites, which causes time-varying coverage and thus changes the set of attackable satellites, the attacker must adopt an effective strategy for selecting wormhole endpoints in each time slot to maximize intercepted traffic throughput during the attack period $\mathbb{T}$.

In the following two subsections, the wormhole attack is formulated as an optimization problem, followed by the design of an efficient algorithm to solve it.

A. Traffic Attraction Problem

To systematically capture the attacker's objective and operational constraints, we introduce the *Traffic Attraction Problem*, which formalizes the attacker's goal, decision variables, and resource limitations. We define a binary variable $x_{r,v,u}(t)$ to indicate whether wormhole satellites v and u intercept request r at time t, with $x_{r,v,u}(t) = 1$ if intercepted and 0 otherwise.

There are two types of intercepted requests: those that originally use the wormhole as their gateway, and those initially routed through neighboring satellites but diverted to the wormhole due to its presence. For a given request $r \in \mathcal{R}$, if its original gateway is not a wormhole, interception depends on whether the presence of the wormhole alters its routing. If the wormhole does not affect the next-hop decision, the request is not intercepted; otherwise, it is. For example, if the request's gateway is a neighbor of the wormhole and next-hop selection favors the wormhole, the request can be intercepted. We define an indicator $\phi^r_{v,A}(t)$, where $\phi^r_{v,A}(t) = 1$ if the outflow of request r at time t is either attracted to or originally routed through wormhole satellite v connected to G_A; otherwise, $\phi^r_{v,A}(t) = 0$. We also define a binary variable $a_r \in \{0, 1\}$, where $a_r = 1$ if request r is intercepted, and $a_r = 0$ otherwise.

The attacker's objective is to maximize the intercepted traffic from the target area. The final attack strategy should include two key aspects: when to attack, which depends on the traffic pattern of the satellite network, and which satellite to function as the endpoint of the wormhole. This strategy is represented as a set containing the vectors $w_A(t)$, which consists of all wormhole indicators $w^v_A(t)$ connecting to G_A, and $w_B(t)$, which consists of all wormhole indicators $w^v_B(t)$ connecting to G_B, for each time slot t. We formally represent the attack strategy as $\Theta_I = \{(w_A(t), w_B(t)) \mid t \in \mathbb{T}\}$.

Next, we formalize the *Traffic Attraction Problem* as an optimization problem, considering the time-varying topology of the satellite network, the wormhole coupling characteristics, budget constraints, interception conditions, and other relevant factors. The problem is formulated as follows:

$$\max \quad \sum_{t\in\mathbb{T}}\sum_{r\in\mathcal{R}} f_r\, a_r \tag{1}$$

$$\text{s.t.} \quad \sum\nolimits_{v\in\mathcal{V}} w^v_A(t) \le 1, \quad \sum\nolimits_{v\in\mathcal{V}} w^v_B(t) \le 1, \quad \forall t \in \mathbb{T}, \tag{1a}$$

$$\sum_{v\in\mathcal{V}} w^v_A(t) = \sum_{v\in\mathcal{V}} w^v_B(t), w^v_A(t) + w^v_B(t) \le 1, \forall t \in \mathbb{T}, \tag{1b}$$

$$w^v_A(t) \le \Lambda^A_v(t), \quad w^v_B(t) \le \Lambda^B_v(t), \quad \forall v \in \mathcal{V},\ \forall t \in \mathbb{T}, \tag{1c}$$

$$\sum\nolimits_{t\in\mathbb{T}}\sum\nolimits_{v\in\mathcal{V}} \left(c^v_A\, w^v_A(t) + c^v_B\, w^v_B(t)\right) \le \Pi, \tag{1d}$$

$$x_{r,v,u}(t) \le w^v_A(t), x_{r,v,u}(t) \le w^u_B(t), x_{r,v,u}(t) \le \phi^r_{v,A}, \quad \forall r \in \mathcal{R}, \forall v, u \in \mathcal{V}, \forall t \in \mathbb{T}, \tag{1e}$$

$$a_r = \sum\nolimits_{t\in T}\sum\nolimits_{v\in\mathcal{V}}\sum\nolimits_{u\in\mathcal{V}} x_{r,v,u}(t), \quad \forall r \in \mathcal{R}, \tag{1f}$$

$$w^v_A(t) \in \{0, 1\}, w^v_B(t) \in \{0, 1\}, x_{r,v,u}(t) \in \{0, 1\}, \quad \forall r \in \mathcal{R}, \forall v, u \in \mathcal{V}, \forall t \in \mathbb{T}. \tag{1g}$$

The objective (1) seeks to maximize the amount of intercepted traffic from the target area. Constraint (1a) regulates the selection of wormhole endpoints by allowing at most one satellite to be attacked by each compromised ground station in each time slot. Constraint (1b) ensures a balanced number of selected endpoints between G_A and G_B, prevents assigning both wormhole endpoints to the same satellite. Constraint (1c) ensures that the satellite to be attacked is reachable by the attacker. The budget constraint (1d) limits the overall cost of wormhole deployment across all time slots, ensuring that the attack remains within its resource constraints. Constraints (1e) and (1f) dictates that a request is only intercepted if its traffic is influenced by the presence of a wormhole, either by passing through a wormhole satellite or being redirected due to it. Lastly, constraint (1g) enforces the binary nature of decision variables, defining whether a satellite functions as a wormhole endpoint and whether a request is successfully intercepted.

B. Wormhole Attack Algorithm

As the *Traffic Attraction Problem* is a mixed-integer linear programming (MILP) problem, standard MILP solvers such as Gurobi [33] and CPLEX [34] can, in principle, be applied. However, in the context of LSNs, this approach faces a fundamental challenge. LEO satellites move extremely fast, requiring an orbital speed of approximately 7.8 kilometers per second to maintain their orbit around Earth [35]. This high mobility causes the network topology to change rapidly, resulting in a large number of time-varying connectivity possibilities that must be captured as decision variables across the attack period. This scale renders direct MILP solving either computationally infeasible or prohibitively slow.

Our key insight is that, although satellites move quickly, their trajectories are deterministic and predictable. This leads

Algorithm 1: Wormhole Attack Algorithm

Input: Network $\mathcal{G}_t = (\mathcal{V}, \mathcal{E}_t)$ for all $t \in \mathbb{T}$, cost c_A^v and c_B^v, request set R, attack budget Π, target area Ω, G_A and G_B locations

Output: Attack strategy $\{(w_A(t), w_B(t)) \mid t \in \mathbb{T}\}$

1 **for** $t \in \mathbb{T}$ **do** calculate coverage $\Lambda_v^A(t)$ and $\Lambda_v^B(t)$;
// Consider only satellites connected to G_A and G_B throughout $\mathbb{T}$ to reduce the search space.
2 $V' \leftarrow \emptyset$;
3 **for** $v \in \mathcal{V}$, $t \in \mathbb{T}$ **do**
4 **if** $\Lambda_v^A(t) = 1$ *or* $\Lambda_v^B(t) = 1$ **then**
5 $V' \leftarrow V' \cup v$;
6 $\mathcal{V} \leftarrow V'$;
7 **for** $r \in \mathcal{R}$ **do** calculate interception indicator $\phi_{v,A}^r(t)$;
8 Attacker solves optimization problem (1);
9 Output attack strategy $\{(w_A(t), w_B(t)) \mid t \in \mathbb{T}\}$.

to predictable coverage patterns between satellites and ground stations over time. Leveraging this predictability, we can precompute the set of satellites that are within communication range of G_A or G_B at each time slot. Only these satellites can possibly serve as wormhole endpoints; all others are guaranteed to be unreachable and can be safely excluded from the optimization. This targeted reduction in the variable space significantly shrinks the problem size, enabling efficient solution by MILP solvers.

The wormhole attack algorithm is presented in Algorithm 1. It begins by computing the coverage indicators $\Lambda_v^A(t)$ and $\Lambda_v^B(t)$ for all satellites v at each time slot t, identifying which satellites are capable of connecting to G_A or G_B. To reduce the search space, the algorithm restricts attention to the subset of satellites that maintain connectivity to either ground station throughout the entire time period $\mathbb{T}$ (lines 2-6). Next, for each request $r \in \mathcal{R}$, the algorithm calculates the interception indicators $\phi_{v,A}^r(t)$, which determine whether the request can be intercepted via a candidate wormhole at time t (line 7). Given these inputs, the attacker solves the *Traffic Attraction Problem* (Equation (1)), to determine when and where to place wormholes in order to maximize the total intercepted traffic while respecting the budget Π (line 8). The final output is the attack strategy $\{(w_A(t), w_B(t)) \mid t \in \mathbb{T}\}$ (line 9).

V. Performance Evaluation

A. Experiment Settings

We evaluate the effectiveness of the proposed wormhole attack under realistic settings, incorporating a real-world satellite constellation, geospatial user distribution, and real-world traffic dynamics observed over time.

To model the satellite network, we adopted the Starlink Shell I configuration [1], which comprised 1,584 satellites distributed across 72 orbital planes, with 22 satellites per orbit. Connectivity was determined using an angle-based coverage model, where a minimum elevation angle of 40 degrees was applied to simulate practical line-of-sight constraints between satellites and ground nodes.

User distribution was generated using a Geodesic Grid Strategy combined with triangular meshing to ensure uniform spatial coverage [25]. To improve realism, we filtered the grid using a global GDP dataset to exclude regions unlikely to generate meaningful traffic. This process yielded a set of 15,070 valid user locations, with each tile representing an area of approximately 51.01 km^2.

The target area was defined by selecting a center point and identifying the k nearest user tiles to form the region of interest. We vary k in the range $\{2, 3, \ldots, 20\}$ to represent different levels of spatial granularity and to systematically evaluate the attack's effectiveness under varying target area configurations. To assess the performance and robustness of the wormhole attack across geographic regions, we randomly selected 100 different target area centers.

Traffic was simulated using the Milan Dataset [36], a real-world urban mobility trace. Requests were sampled every 10 minutes, with each representing 1MB of data. We assumed that 80% of sources were active at any given time slot, and individual flow sizes varied by ±2% to reflect realistic fluctuations in traffic load. For routing, each user selected the nearest satellite as its gateway. A request was considered intercepted if it was routed through either a wormhole-controlled satellite or one of its immediate neighbors—reflecting the influence a compromised node could exert on nearby routing decisions.

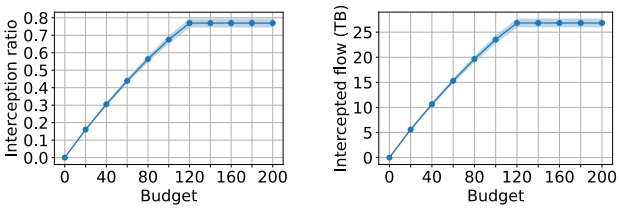
Finally, we imposed an hourly budget constraint to reflect the attacker's resource limitations. The budget ranged from 0 to 200 in increments of 20, where each satellite connected to either G_A or G_B incurred a cost of 10 units. Unless otherwise specified, the default budget was set to 200. The default attack period spans one day (1440 minutes), with a time step of 10 minutes. Evaluations were conducted by default at 15:00, corresponding to mid-day traffic conditions.

B. Evaluation Results

We used two metrics to evaluate attack effectiveness: the *interception ratio*, defined as the total intercepted throughput divided by the total traffic to or from the target area, and the *intercepted flow*, which measures the absolute amount of data captured by the wormhole attack.

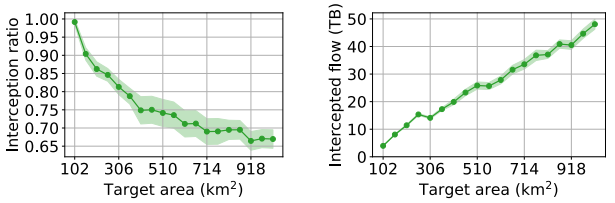
Vary budget. Fig. 2 illustrates how interception performance changes with increasing budget. Both interception ratio and intercepted flow grew steadily as more satellites were used as wormhole endpoints. The curves began to plateau around a budget of 120, not due to insufficient resources, but because some traffic paths naturally avoided wormhole satellites and their neighbors due to the network's routing behavior. In this section, the shaded regions in the figures represent the 95% confidence intervals over 100 randomly selected target areas.

Vary target area size. Fig. 3 shows how interception performance changes with the size of the target area. As the area increased, the interception ratio gradually decreased. This is because a larger target region results in more dispersed traffic, making it harder for wormhole satellites and their neighbors



(a) Interception ratio vs. budget (b) Intercepted flow vs. budget

Fig. 2. Interception performance under different budget constraints.



(a) Interception ratio vs. area size (b) Intercepted flow vs. area size

Fig. 3. Interception performance under different target area sizes.

to cover all flows. At the same time, the intercepted flow increased with area size, as larger regions generate more traffic overall, resulting in greater volumes of intercepted data.

Attack across time. Fig. 4 shows how the intercepted flow varied over the course of a day. The intercepted traffic volume was lowest during early morning hours (around 6am), gradually increased as user activity rose, and peaked between 5PM and 7PM, corresponding to evening traffic surges. This trend reflects the temporal dynamics of real-world network usage, indicating that the effectiveness of the wormhole attack closely follows daily traffic patterns of LSN.

VI. Countermeasures

In this section, we propose potential detection and defense strategies against our proposed attack.

Delay-based detection. Fine-grained dynamic measurements in LSNs monitor hop counts and packet delays to detect anomalies indicative of wormhole disruptions. By analyzing propagation delays, the system can identify inconsistencies in expected latency, which may signal malicious tunneling.

Geographical boundary enforcement. Geo-fencing techniques [37] restrict packet flow to predefined geographical boundaries, preventing unauthorized rerouting through wormholes. By leveraging satellite location awareness and orbital information, the system can ensure that packets do not reach unauthorized regions or traverse prohibited paths.

Path validation. Path validation mechanisms enforce legitimate packet traversal through designated routers, preventing adversaries from redirecting traffic through unauthorized links. For example, integrating cryptographic verification with delay-based metrics enhances route authenticity [38].

Doppler shift analysis. Checking the Doppler shift of broadcast messages serves as a physical-layer fingerprint to verify their legitimacy. By analyzing the expected frequency shifts caused by satellite motion, the system ensures that received messages are real-time transmissions rather than tampered or

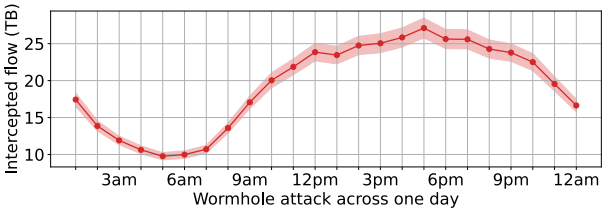


Fig. 4. Intercepted flow over a 24-hour period.

replayed signals. Any deviation from the expected Doppler pattern can indicate an attack, helping to detect and mitigate wormhole-based manipulation.

VII. Discussion and Future Work

Limitations. Our attack assumes that LSNs employ dynamic distributed routing. While current LSNs predominantly rely on source routing, dynamic distributed routing represents a natural evolution as networks scale and demand greater adaptability. As future satellite networks move toward more autonomous and resilient architectures, proactively evaluating their security vulnerabilities becomes essential.

Our attacker model assumes that an attacker must establish a direct connection with a satellite to issue malicious commands, which limits the attack surface and increases the difficulty of attack execution. In practice, however, broader attack capabilities may involve indirect methods such as pre-planted malware, command relays, hijacking legitimate communication links, or exploiting vulnerabilities in satellite firmware updates, all of which could expand the attack's reach and impact.

While executing an attack over a period and compromising a large number of satellites may appear challenging, adversaries could adopt a strategic, long-term approach. Techniques such as gradual infiltration, pre-positioning of compromised nodes, or leveraging supply chain vulnerabilities could make large-scale attacks more practical than they initially seem.

Future Work. Our attack targets dynamic routing by primarily focusing on traffic attraction near the gateway. However, a wormhole endpoint can influence routing on a much larger scale, intercepting traffic beyond its immediate vicinity. As long as traffic flows through the endpoint or its neighboring nodes, the attack remains effective. While our evaluation considers traffic redirection within a single hop, the actual impact could be significantly greater, potentially disrupting routing across multiple hops and amplifying the attack's overall effectiveness.

This work primarily focuses on the logical-level strategy of the wormhole attack. Incorporating a physical-layer delay model would improve accuracy and practicality. In addition, the tunnel is not necessarily restricted to terrestrial links. Furthermore, optimizing the selection of G_A and G_B based on delay modeling could enhance the attack's efficiency and effectiveness. With the advancement of SDN, G_A and G_B may no longer be limited to ground stations but could instead be low-cost, deployable ground-based relay devices. Another key aspect for future investigation is stealthiness, specifically the development of strategies to minimize the risk of detection and ensure covert attack execution.

Our current model assumes an offline request pattern, where the attacker has prior knowledge of network requests. However, in real-world scenarios, requests are often dynamic and continuous. Future research could explore machine learning-based approaches, such as time-series forecasting models trained on historical data, to predict request patterns in real time. Additionally, statistical traffic analysis could help infer request distributions and detect recurring access patterns. Game-theoretic models could also be employed to simulate adversarial interactions between the attacker and the network, optimizing attack strategies based on expected system responses. Furthermore, incorporating probabilistic models for gateway selection could better reflect real-world decision-making processes, while reinforcement learning techniques could enable adaptive attack strategies that adjust dynamically to observed network behavior.

VIII. Conclusion

As LSNs expand, their dynamic topology and latency asymmetries create new security vulnerabilities. This paper presents a novel wormhole attack that exploits space-ground communication properties to manipulate routing and intercept traffic from target areas. We formulate the wormhole attack under real-world constraints and evaluate its impact using real satellite and user data. Results show the severity of such attack and highlight the need for tailored countermeasures.

References

[1] "Starlink: High-speed internet around the world," accessed 2025-09-12. [Online]. Available: https://www.starlink.com/us

[2] "Project kuiper," accessed 2025-09-12. [Online]. Available: https://www.aboutamazon.com/what-we-do/devices-services/project-kuiper

[3] "Oneweb," accessed 2025-09-12. [Online]. Available: https://oneweb.net/

[4] L. Izhikevich, M. Tran, K. Izhikevich, G. Akiwate, and Z. Durumeric, "Democratizing leo satellite network measurement," *Proceedings of the ACM on Measurement and Analysis of Computing Systems*, vol. 8, no. 1, pp. 1–26, 2024.

[5] S. Ma, Y. C. Chou, H. Zhao, L. Chen, X. Ma, and J. Liu, "Network characteristics of leo satellite constellations: A starlink-based measurement from end users," in *IEEE INFOCOM*, 2023, pp. 1–10.

[6] N. Mohan, A. E. Ferguson, H. Cech, R. Bose, P. R. Renatin, M. K. Marina, and J. Ott, "A multifaceted look at starlink performance," in *ACM WWW*, 2024, pp. 2723–2734.

[7] A. Einstein and N. Rosen, "The particle problem in the general theory of relativity," *Physical Review*, vol. 48, no. 1, p. 73, 1935.

[8] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Packet leashes: a defense against wormhole attacks in wireless networks," in *IEEE INFOCOM*, vol. 3, 2003, pp. 1976–1986.

[9] J. R. Gómez, H. F. V. Montoya, and Á. L. Henao, "Implementing a wormhole attack on wireless sensor networks with xbee s2c devices," *Revista Colombiana de Computación*, vol. 20, no. 1, pp. 41–58, 2019.

[10] P. Perazzo, C. Vallati, D. Varano, G. Anastasi, and G. Dini, "Implementation of a wormhole attack against a rpl network: Challenges and effects," in *IEEE WONS*, 2018, pp. 95–102.

[11] M. Khabbazian, H. Mercier, and V. K. Bhargava, "Severity analysis and countermeasure for the wormhole attack in wireless ad hoc networks," *IEEE Transactions on Wireless Communications*, vol. 8, no. 2, pp. 736–745, 2009.

[12] X. Cao, Y. Li, X. Xiong, and J. Wang, "Dynamic routings in satellite networks: An overview," *Sensors*, vol. 22, no. 12, p. 4552, 2022.

[13] H. S. Chang, B. W. Kim, C. G. Lee, S. L. Min, Y. Choi, H. S. Yang, D. N. Kim, and C. S. Kim, "Fsa-based link assignment and routing in low-earth orbit satellite networks," *IEEE transactions on vehicular technology*, vol. 47, no. 3, pp. 1037–1048, 1998.

[14] E. Ekici, I. F. Akyildiz, and M. D. Bender, "A distributed routing algorithm for datagram traffic in leo satellite networks," *IEEE/ACM Transactions on networking*, vol. 9, no. 2, pp. 137–147, 2001.

[15] X. Liu, X. Yan, Z. Jiang, C. Li, and Y. Yang, "A low-complexity routing algorithm based on load balancing for leo satellite networks," in *IEEE VTC2015-Fall*, 2015, pp. 1–5.

[16] X. Ji, L. Liu, P. Zhao, and D. Wang, "A destruction-resistant on-demand routing protocol for leo satellite network based on local repair," in *IEEE FSKD*, 2015, pp. 2013–2018.

[17] Y. Xiao, T. Zhang, and M. Sun, "Geographical addressing strategy for space-ground integrated network," *International Journal of Satellite Communications and Networking*, vol. 39, no. 2, pp. 178–192, 2021.

[18] H. Li, H. Zhang, L. Qiao, F. Tang, W. Xu, L. Chen, and J. Li, "Queue state based dynamical routing for non-geostationary satellite networks," in *IEEE AINA*, 2018, pp. 1–8.

[19] B. Jianjun, L. Xicheng, L. Zexin, and P. Wei, "Compact explicit multi-path routing for leo satellite networks," in *IEEE HPSR*, 2005, pp. 386–390.

[20] E. Jedermann, M. Strohmeier, V. Lenders, and J. Schmitt, "Record: A reception-only region determination attack on leo satellite users," in *USENIX Security*, 2024, pp. 6113–6130.

[21] D. Koisser, R. Mitev, N. Yadav, F. Vollmer, and A.-R. Sadeghi, "Orbital trust and privacy:{SoK} on {PKI} and location privacy challenges in space networks," in *USENIX Security*, 2024, pp. 6093–6111.

[22] L. Yu, J. Hao, J. Ma, Y. Sun, Y. Zhao, and B. Luo, "A comprehensive analysis of security vulnerabilities and attacks in satellite modems," in *ACM SIGSAC*, 2024, pp. 3287–3301.

[23] J. Willbold, M. Schloegel, M. Vögele, M. Gerhardt, T. Holz, and A. Abbasi, "Space odyssey: An experimental software security analysis of satellites," in *IEEE SP*, 2023, pp. 1–19.

[24] W. Liu, Y. Li, H. Li, Y. Chen, Y. Wang, J. Lan, J. Wu, Q. Wu, J. Liu, and Z. Lai, "The dark side of scale: Insecurity of direct-to-cell satellite mega-constellations," in *IEEE SP*, 2024, pp. 445–464.

[25] G. Giuliari, T. Ciussani, A. Perrig, and A. Singla, "{ICARUS}: Attacking low earth orbit satellite networks," in *USENIX ATC*, 2021, pp. 317–331.

[26] Y. Zhang, Q. Wu, Z. Lai, Y. Deng, H. Li, Y. Li, and J. Liu, "Time-varying bottleneck links in leo satellite networks: Identification, exploits, and countermeasures," in *NDSS*, 2025.

[27] ——, "Energy drain attack in satellite internet constellations," in *IEEE IWQoS*, 2023, pp. 1–10.

[28] Y. Wang, H. Li, Z. Lai, and J. Li, "Starmaze: Ring-based attack in satellite internet constellations," in *IEEE IWQoS*, 2024, pp. 1–10.

[29] N. Schweitzer, A. Dvir, and A. Stulman, "Network wormhole attacks without a traditional wormhole," *Ad Hoc Networks*, vol. 151, p. 103286, 2023.

[30] T.-H. Chu, S.-Y. Kuo, and Y.-H. Chou, "Using quantum-inspired tabu search algorithm with logic operation and moving average indicator for wormhole attack detection in a wsn," *Journal of Internet Technology*, vol. 20, no. 1, pp. 167–176, 2019.

[31] Z. Han, C. Xu, G. Zhao, S. Wang, K. Cheng, and S. Yu, "Time-varying topology model for dynamic routing in leo satellite constellation networks," *IEEE Transactions on Vehicular Technology*, vol. 72, no. 3, pp. 3440–3454, 2022.

[32] "Satnogs – open source global network of satellite ground-stations," accessed 2025-09-12. [Online]. Available: https://satnogs.org/

[33] "The leader in decision intelligence technology - gurobi optimization," accessed 2025-09-12. [Online]. Available: https://www.gurobi.com/

[34] "Ibm ilog cplex optimization studio," accessed 2025-09-12. [Online]. Available: https://www.ibm.com/products/ilog-cplex-optimization-studio

[35] "Types of orbits," accessed 2025-09-12. [Online]. Available: https://www.esa.int/Enabling_Support/Space_Transportation/Types_of_orbits

[36] G. Barlacchi, M. De Nadai, R. Larcher, A. Casella, C. Chitic, G. Torrisi, F. Antonelli, A. Vespignani, A. Pentland, and B. Lepri, "A multi-source dataset of urban life in the city of milan and the province of trentino," *Scientific data*, vol. 2, no. 1, pp. 1–15, 2015.

[37] S. T. Ahmed, A. A. Ahmed, A. Annamalai, and M. F. Chouikha, "A scalable and energy-efficient lorawan-based geofencing system for remote monitoring of vulnerable communities," *IEEE Access*, vol. 12, pp. 48 540–48 554, 2024.

[38] C. Gu, Q. Wu, Z. Lai, H. Li, J. Li, W. Liu, Q. Zhang, J. Liu, and Y. Li, "Starveri: Efficient and accurate verification for risk-avoidance routing in leo satellite networks," in *IEEE ICNP*, 2024, pp. 1–11.