Journal of Cybersecurity Education, Research and Practice

Volume 2024 | Number 1 Article 26

9-26-2024

Leveraging Propagation Delay for Wormhole Detection in Wireless Networks

Harry May
Louisiana Tech University, hlm012@latech.edu

Travis Atkison
University of Alabama, atkison@cs.ua.edu

Recommended Citation
May, Harry and Atkison, Travis (2024) "Leveraging Propagation Delay for Wormhole Detection in Wireless Networks," *Journal of Cybersecurity Education, Research and Practice*: Vol. 2024: No. 1, Article 26.
DOI: https://doi.org/10.62915/2472-2707.1193
Available at: https://digitalcommons.kennesaw.edu/jcerp/vol2024/iss1/26

Leveraging Propagation Delay for Wormhole Detection in Wireless Networks

Abstract

Detecting and mitigating wormhole attacks in wireless networks remains a critical challenge due to their deceptive nature and potential to compromise network integrity. This paper proposes a novel approach to wormhole detection by leveraging propagation delay analysis between network nodes. Unlike traditional methods that rely on signature-based detection or specialized hardware, our method focuses on analyzing propagation delay timings to identify anomalous behavior indicative of wormhole attacks. The proposed methodology involves collecting propagation delay data in both normal network scenarios and scenarios with inserted malicious wormhole nodes. By comparing these delay timings, our approach aims to differentiate between legitimate network paths and potential wormhole shortcuts. Utilizing the NS-3 network simulator, we validate the effectiveness of our method in accurately detecting and mitigating wormhole attacks. The key advantage of our approach lies in its proactive nature and ability to detect wormholes without relying on specific attack signatures or additional hardware. Using the consistency of propagation delay data, our method offers a promising avenue for early detection and prevention of wormhole attacks, thereby enhancing network security and reliability. The results and insights presented in this paper contribute to the ongoing efforts in developing defense mechanisms against sophisticated network attacks, emphasizing the potential of propagation delay analysis in addressing the challenges posed by wormhole threats in wireless networks.

Keywords

Wireless network attacks, wormhole, simulation, detection, mitigation

Leveraging Propagation Delay for Wormhole Detection in Wireless Networks

Harry May
Department of Computer Science
Louisiana Tech University
Ruston, Louisiana USA
email: hlm012@latech.edu
ORCID: 0000-0002-0571-1392

Travis Atkison
Department of Computer Science
University of Alabama
Tuscaloosa, Alabama USA
email: atkison@cs.ua.edu
ORCID: 0000-0001-7258-7355

***Abstract*—Detecting and mitigating wormhole attacks in wireless networks remains a critical challenge due to their deceptive nature and potential to compromise network integrity. This paper proposes a novel approach to wormhole detection by leveraging propagation delay analysis between network nodes. Unlike traditional methods that rely on signature-based detection or specialized hardware, our method focuses on analyzing propagation delay timings to identify anomalous behavior indicative of wormhole attacks. The proposed methodology involves collecting propagation delay data in both normal network scenarios and scenarios with inserted malicious wormhole nodes. By comparing these delay timings, our approach aims to differentiate between legitimate network paths and potential wormhole shortcuts. Utilizing the NS-3 network simulator, we validate the effectiveness of our method in accurately detecting and mitigating wormhole attacks. The key advantage of our approach lies in its proactive nature and ability to detect wormholes without relying on specific attack signatures or additional hardware. Using the consistency of propagation delay data, our method offers a promising avenue for early detection and prevention of wormhole attacks, thereby enhancing network security and reliability. The results and insights presented in this paper contribute to the ongoing efforts in developing defense mechanisms against sophisticated network attacks, emphasizing the potential of propagation delay analysis in addressing the challenges posed by wormhole threats in wireless networks.**

***Index Terms*—Wireless network attacks, wormhole, simulation, detection, mitigation**

I. Introduction

Wireless networks have become a central part of modern communication systems, enabling communication without physical cables. These networks offer flexibility and convenience for exchanging information between devices across various applications. However, like any technology, wireless networks are susceptible to many security vulnerabilities, including wormhole attacks. A wormhole attack occurs when malicious devices create a direct, high-speed tunnel between distant devices or nodes in a network, bypassing regular routes and shortening the communication distance. This manipulation of the network topology allows attackers to launch multiple harmful activities, including eavesdropping, data alteration, and denial of service, posing a significant threat to the confidentiality, integrity, and availability of the network. As the wireless landscape continues to expand, it is crucial to understand the implications of these vulnerabilities and the importance of detecting and mitigating wormhole attacks to ensure network security and reliability. This paper aims to address this gap by proposing a novel approach for wormhole attack detection by analyzing propagation delay values between nodes. By leveraging the physical properties of wireless signal propagation, we aim to provide an efficient mechanism to safeguard wireless networks against wormhole attacks. Our research contributes to the broader goal of enhancing the security and reliability of wireless networks, which are critical for a wide range of applications in today's interconnected world.

The remainder of the paper is organized as follows: Section 2 provides a brief overview of the physical layout of a wormhole in the network and reviews some previous detection strategies. Section 3 explains the setup for data collection, modifications to the communication protocol, box plot statistics, and the proposed detection technique. Section 4 examines the results collected from the experimental setup, including a potential digital signature for a wormhole. A strategy for detecting a wormhole attack and triggering the mitigation procedure is in Section 5. Finally, Section 6 summarizes the results and outlines future research directions.

II. Related Work

Among the many security threats in wireless network infrastructures, including Blackhole, Sybil, selective forwarding, rushing, spoofed, sinkhole, Hello flood, and others, threatening wormhole attacks stand out as a formidable adversary, relentlessly compromising integrity and performance. Each attack possesses individual characteristics in its attack method, with the wormhole attack being unique in structure and possible objectives. Consequently, researchers have directed their efforts toward painstakingly understanding wormhole attacks and devising effective defense mechanisms. Detecting these stealthy attacks has emerged as a focal point, leading to an intensive exploration of detection techniques that can identify their presence with precision. However, it's important to note that the proposed AODV-PD protocol may not be suitable for countering these other attacks due to their distinct characteristics and objectives. The significance of reliable detection techniques cannot be overstated, as they form the foundation for implementing effective mitigation strategies. This section describes a sample wormhole environment and an overview of related works in this field, covering the investigation of wormhole attacks, the advancement of detection techniques, and the deployment of measures to identify malicious nodes. Emphasizing the inseparability of detection and mitigation, this discussion highlights the integral role of an integrated approach in safeguarding wireless networks from the vulnerabilities posed by wormhole attacks. Without robust detection, the pursuit of mitigation remains a vague goal.

A. Wormhole Attack

A wormhole attack in a wireless network is a severe security threat that exploits the characteristics of these networks to create a shortcut between two distant nodes, enabling the attacker to bypass normal routing paths. The objective of the attack may be to modify, analyze, decrypt, drop, or delay communication data, depending on the attacker's objectives, motivation, and resources. In this attack, malicious nodes collude to create a direct, high-speed communication link, allowing them to forward packets between each other without undergoing the usual routing checks.

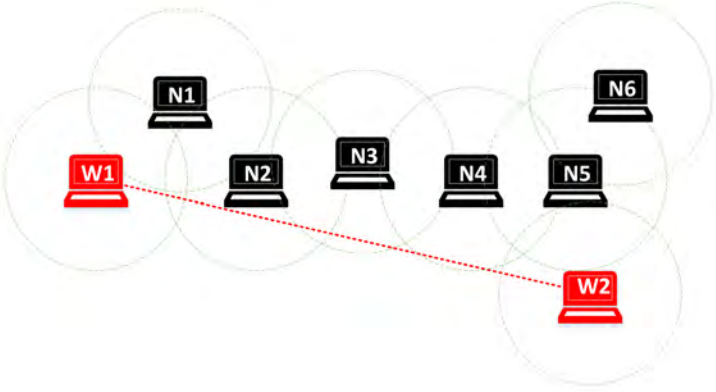

Fig. 1. Simple network with wormhole.

Wormholes may be classified using different criteria such as implementation methods, the medium used, the attackers involved, and the location of the victim nodes [1]–[3]. The implementation of the wormhole may be defined as encapsulated, out-of-band, high power, packet relay, or protocol deviation [4], [5]. The out-of-band wormhole was chosen for this research because of the different construction options available to an attacker, dependent on their resources. The out-of-band wormhole attack has several objectives, including stealth and acceptance as part of the preferred route in a network. An example of a simple network with a wormhole can be seen in Figure 1, with nodes W1 and W2 as the wormhole nodes. As shown, the attacker creates the wormhole by placing two or more malicious nodes, W1 and W2, within communication distance of existing nodes so that the selected route has the shortest hop count. The first route follows N1-N2-N3-N4-N5-N6, totaling 5 hops. The malicious nodes, connected by a high-speed link, must insert themselves into the network such that the hop count is preferably four or less. After insertion, the preferred path is N1-W1-W2-N5-N6, due to the shorter hop count of 4.

B. Detection Strategies

A node is considered malicious when it falsifies or alters the transfer of information within the network. Detecting the presence of wormhole attacks in wireless networks is a critical step in mitigating their impact. Various detection techniques are proposed in the literature to identify and differentiate legitimate communication paths from malicious wormhole tunnels. The methods explored by other authors include:

- Anomaly detection: Based on various metrics, such as network traffic, resource consumption, and abnormal device behavior [6]. The strength of anomaly detection is its flexibility and adaptability, coupled with a low false positive rate. Choosing the appropriate metric, like propagation delay between nodes, improves detection capabilities. This approach, along with the timing method, is selected for this research.
- Intrusion detection system (IDS): Normally, a physical setup to monitor network traffic, utilizing signature-based or behavior-based practices to identify malicious nodes [7]–[10]. IDS offers real-time monitoring of network systems and is scalable and customizable. However, challenges include potential false positives, complex configurations, and maintenance requirements.
- Reputation-based detection: This involves assigning a score to each node based on previous behavior [11]–[15]. This method provides real-time responses to potential threats with reduced false positive feedback and minimal impact on network performance. However, it relies on historical behavior, which can lead to a misinterpretation of incoming data.
- Cooperation-based detection: Relies on collaboration between known good nodes, sharing information to identify suspicious behavior [16]–[20]. This method improves threat visibility and detection accuracy but encounters challenges related to trust, privacy, data sharing, and coordination among participants.
- Cryptographic techniques: Creates digital signatures for each node, uniquely identifying known nodes and quickly detecting impersonating nodes [21]–[23]. Cryptographic techniques maintain confidentiality, integrity, and authentication in the network, enabling secure communication. However, they can be complex to implement, and manage, and may introduce performance overhead.
- Statistics: Utilizes calculations such as relative frequency or usage density to identify possible malicious nodes [24]–[27]. Statistical techniques provide advantages such as anomaly detection, scalability, flexibility, and data-driven insights. Challenges include false negatives, model complexity, threshold settings, and correct interpretability. The effectiveness of statistical detection depends on appropriate models and results validation.

DOI: 10.62915/2472-2707.1193

- Timing: Involves various forms, including synchronization by a central node, timing between nodes, round trip timing (RTT), end-to-end timing, and shortest path timing [28]–[31]. This technique benefits from sensitivity to hidden behavior, low false positives, and early warning signs. Limitations include noise and environmental variables, false negatives, and network complexity. The effectiveness of timing-based detection heavily depends on the accurate calibration of detection mechanisms.

The variety of detection methods suggests that a standardized procedure for identifying wormholes is lacking, primarily due to the absence of a digital signature specific to this type of attack. For this same reason, a method of mitigation is not clearly defined. The proposed method for this research uses a form of timing called propagation delay between nodes.

C. Real-World Events

Although there are no documented real-world instances of wormhole attacks, they are likely employed alongside other types of attacks, particularly man-in-the-middle (MITM) attacks. Wormhole attacks create a covert and low-latency link between two distant points in a network, enabling attackers to relay messages undetected. This stealth capability makes wormhole attacks an ideal precursor to MITM attacks, allowing the attacker to intercept, modify, and monitor network traffic undetected. By establishing a hidden channel in the network, wormhole attacks facilitate more complex and damaging attacks, underscoring the need for effective detection and mitigation strategies. Wormhole attacks are designed to be as stealthy as possible to avoid detection, allowing attackers to intercept and relay messages without significantly altering the traffic's appearance. This stealth allows the wormhole to embed itself in the network, bypassing traditional security measures and becoming a hidden conduit for malicious activities. Once embedded, the wormhole can monitor traffic, modify packets, drop packets, or execute any other actions aligned with the attacker's motives.

A well-known example of such an attack is Stuxnet (2010) [32], [33], a sophisticated malware that targeted the Natanz uranium enrichment facility in Iran. Stuxnet aimed to disrupt the centrifuges by manipulating the industrial control systems without detection. To achieve this, the malware had to insert itself into the network's operations stealthily, avoiding detection by both human operators and automated security systems. This scenario is an ideal candidate for a wormhole attack, as the wormhole could facilitate the MITM attack needed for Stuxnet to monitor and alter communications within the network, ensuring the malware could execute its payload without raising alarms.

Another real-world example is the DigiNotar attack in 2011 [34], where attackers intercepted digital certificates used for message encryption. By compromising DigiNotar, a Dutch certificate authority, the attackers could issue fraudulent certificates, effectively enabling MITM attacks on a broad scale. These fraudulent certificates allowed attackers to decrypt, modify, and re-encrypt messages, making it possible to intercept secure communications across various platforms. The stealth and precision required to intercept and manipulate digital certificates highlight the potential role of wormhole attacks in setting up the conditions for MITM attacks, as they provide a covert channel for intercepting and redirecting traffic.

Furthermore, the 2017 KRACK [35] attack exploited vulnerabilities in the WPA2 protocol, using MITM tactics to intercept and decrypt Wi-Fi traffic, underscoring the critical need to secure network communications against advanced MITM attacks. These real-world examples underscore the critical need for robust detection mechanisms like the AODV-PD protocol to safeguard wireless networks against such security threats. By focusing on simplicity of implementation, computational efficiency, scalability, detection accuracy, and adaptability to real-world networks, the AODV-PD protocol offers a practical and efficient solution for detecting and mitigating wormhole attacks, thereby preventing the subsequent MITM attacks that can cause significant damage to network operations and security.

III. Methodology

As shown in the list above, the detection of malicious nodes in a wireless network varies widely in the procedures. The method proposed by this paper uses the basic concept of timing as presented by other authors but the detection condition is different. Application of the proposed method for wormhole detection utilizes several areas including propagation delay, protocol modification using link accumulation, and outlier detection in timing collection data. In wireless communication, propagation delay is considered as the amount of time it takes the beginning of a signal to travel from a sender node to a receiver node. The proposed scheme would measure the propagation delay metric for each link in the preferred path using the RREQ message of the AODV communication protocol. Similar research on round trip timing may be found by Papadimitratos, et al. [19], Van Tran, et al. [30], Korkmaz, et al. [28], Zhen, et al. [31], and Ling, et al. [36]. The main difference is that their research does not use a combination of delay timing and outlier data in identifying possible malicious nodes. Modification of the AODV protocol allows the forwarding of the propagation delay timing data for each link to the destination node similar to the path accumulation by Gwalani, et al. [37]. The format for the link and propagation delay will be in a *'link-link, time'* format. The greatest overhead change will occur at the destination node because it now has the task of extracting the propagation delay timing from the RREQ message, calculating box plot data, identifying any outlier delay data, and updating the weighting factor of any outlier links for mitigation purposes. Similar to other protocol modification schemes [37]–[39], this method would be called AODV-PD or Ad-hoc On-demand Distance Vector Propagation Delay.

Wormhole attacks pose a significant threat to the integrity and security of wireless networks, particularly in scenarios where traditional security measures fall short. This paper presents a methodology for detecting wormhole attacks through the integration of an experimental setup, data collection procedures, a modified Ad hoc On-Demand Distance Vector (AODV) protocol, and an innovative detection technique using propagation delay values.

A. Experimental Setup

The experimental setup, shown in Figure 1, involves creating a simulated wireless network using the NS-3 network simulator software to investigate the detection of wormhole attacks. This setup comprises six standard wireless nodes and two malicious wormhole nodes, all operating in a controlled environment. Table I provides the objectives along with associated tutorials to achieve the steps required to configure and finalize the wireless network, including node placement, network configuration parameters, and the inclusion of malicious wormhole nodes.

- Wireless Nodes (6 Standard Nodes): Six standard wireless nodes are configured to simulate legitimate network participants. These nodes communicate with each other using wireless communication protocols and adhere to standard routing mechanisms. They generate and exchange data packets within the network, creating a realistic communication environment.
- Malicious Wormhole Nodes (2 Nodes): Two malicious wormhole nodes are strategically placed within the network to simulate the presence of a wormhole attack. These nodes attempt to deceive the network by establishing a shortcut between distant locations, potentially disrupting communication and compromising data integrity. A characteristic of a wormhole node is the communication link includes both wireless and wired connections.
- Wireless Channel and Propagation Model: The wireless channel characteristics, including signal propagation, interference, and attenuation, are simulated using appropriate models within NS-3. These models replicate the real-world wireless environment, influencing the quality of signal transmission and the effectiveness of communication between nodes.
- Traffic Generation and Data Exchange: The standard nodes generate data traffic by exchanging packets among themselves using the AODV protocol. These data packets traverse the simulated wireless channel, experiencing signal strength variations and potential interference as they move through the environment. This traffic generation reflects real-world scenarios and forms the basis for the analysis of network behavior.

B. Data Collection Procedures

The experimental evaluation of the network's design, with and without a wormhole, entailed a series of experiments focusing on standard data metrics. The NS-3 simulator's automated scripting tools facilitated the generation of routing tables for each node and the computation of propagation delays between nodes. To validate the usefulness of the detection technique, a comparative analysis was conducted using the propagation delays along the preferred route selected by the AODV protocol, both with and without the injected wormhole.

TABLE I
NS-3 REFERENCES

Objective	*Reference Tutorial Script*
Building Point To Point	5.2 A First Tutorial Script
Building LAN Network	7.1 Building A Bus Network Topology
Building Wireless Network	7.3 Building a Wireless Network Topology
Setting Mobility	7.1 Building A Bus Network Topology
Setting Radio Propagation	Propagation Module
Setting Routing Protocol	7.1 Building A Bus Network Topology
Extracting Metric Data	8.0 Tracing

Given the absence of a definitive digital signature for identifying a set of nodes as a wormhole, the primary objective was to detect link values that deviate significantly from standard propagation values. Upon identifying outlier values, additional measures were implemented to isolate the problematic link. The AODV-PD algorithm, designed for efficient wormhole attack detection and mitigation in wireless networks, comprises three key stages.

The first stage, see Algorithm 1, involves the initial collection of propagation delay information between nodes. During this step, the algorithm associates the extracted propagation delay values with Route Request (RREQ) messages, which are then forwarded to the destination node along with the appended propagation values.

Upon reaching the destination node, the second stage of the algorithm begins. Here, all received propagation delay values are aggregated, and a statistical analysis, specifically a box plot, is computed to identify any outliers among these delay values. Outliers indicate propagation delays that significantly deviate from the norm, serving as reliable indicators of potential wormhole presence.

The third stage of the AODV-PD algorithm is activated if outliers are detected in the second stage. In this scenario, the algorithm checks the weighting factor associated with the link exhibiting the outlier delay. This dynamic parameter reflects the link's reliability and trustworthiness. If the calculated factor exceeds a predetermined threshold, signifying a substantial deviation from normal behavior, the algorithm takes corrective action by adjusting the weighting factor. If the adjusted factor exceeds a defined limit, the link is isolated from future preferred paths. This responsive approach ensures that links displaying suspicious behaviors are promptly and effectively mitigated, thereby enhancing the overall security and reliability of the wireless network.

C. AODV Modification

The Ad hoc On-Demand Distance Vector (AODV) routing protocol [40], a popular choice for wireless networks, is tailored to incorporate enhanced security features. This modification enables nodes to collaborate and exchange additional information, such as signal strength and hop count, while establishing routes. By enriching the protocol with these metrics, nodes become capable of identifying inconsistencies

Algorithm 1 Proposed algorithm pseudocode

```
FUNCTION: collect-PD-values()
for all wireless nodes do {collect propagation delay value}
    start-node = get-start-node-name()
    end-node = get-end-node-name()
    PD = get-PD-value()
    append-to-RREQ-message(PD, start-node, end-node)
end for=0

FUNCTION: create box plot
for all RREQ Messages do {extract links and PD values}
    generate-boxplot-from-PD-values
    if $outliers > 0$ then
        modify-weighting-factor {change WF of link}
    end if
    if $WF > setpoint$ then
        exclude-link-from-path-selection {quarantine-link}
    end if
    append-to-RREQ-message(PD, start-node, end-node)
end for=0
```

in communication patterns that may signify the presence of a wormhole attack. Implementation of the proposed detection scheme requires modification of the AODV protocol to transfer propagation delay timing extracted from each link in the selected path. Modification of the AODV communication protocol is similar to the link accumulation protocol proposed by Gwalani, et al. [35] and Seada, et al. [38]. The unmodified AODV protocol uses RREQ and RREP messages to establish a path from a source to a destination. One of the modifications needed for this research uses link accumulation information containing the linked nodes and the propagation delay timing associated with this link. Each node would append the beginning node label, ending node label, and the propagation delay time to the RREQ message as it progresses from source node to destination node. The destination node, receiving all RREQ messages, is able to extract all links and propagation delay values. Note that the normal operation of the RREQ and RREP has not changed so it is able to identify the shortest path from source to destination using the routing table.

D. Box Plot and Outliers

A box plot, also known as a box-and-whisker plot, is a method used in statistical analysis to graphically display the distribution of a set of values. Included in the display as shown in Figure 2, is the minimum, maximum, median, and quartiles for the set. The display typically displays a rectangular box representing the middle 50% of the data with a line inside the box that represents the median value. The ends of the box represent the lower (Q1) and upper quartiles (Q3). The whiskers, shown as 1 and 5 in Figure 2, represents the minimum value and maximum value in the set.

In statistics, an outlier would be a data point that is very different from other values in the dataset. Since the value would be much larger or smaller than expected, it might be a measurement error, data entry error, or a true value that is significantly different than the other values. Outliers can have a significant impact on statistical calculations because they can skew the results which could change the interpretation of the results. Because of this, it is very important to correctly identify and handle any outliers accordingly. In the case of the box plot, any data point that falls outside the whiskers is considered an outlier. It is important to note that all outliers are not necessarily bad, in that they may represent rare or extreme events in whatever dataset is observed.

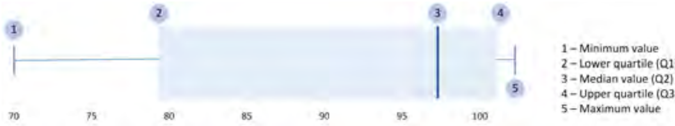

Fig. 2. Box plot structure.

E. Detection Technique

The detection technique employed for identifying a wormhole in a wireless network relies on the analysis of propagation delay timing between nodes. This method involves the aggregation of timing values at the destination node, utilizing the box plot format for data representation and analysis. The primary objective of this technique is to detect outlier values within the box plots, which may indicate the presence of a wormhole in the network.

At first, propagation delay values are collected between pairs of nodes in the network. These values indicate the duration required for signals to travel between nodes. The collected timing data is then appended to the RREQ message and sent to the destination node, where it is organized into a box plot. The box plot provides a graphical representation of the timing data, including key statistical metrics such as the median, quartiles, and potential outliers.

During the analysis phase, the destination node closely monitors the box plot for any deviation from the expected timing patterns. Outlier values, characterized by their significant deviation from the median and quartiles, are flagged as potential indicators of a wormhole. The detection algorithm is designed to trigger an alert or initiate mitigation measures upon detecting such outlier values, indicating a suspicious communication path that may be associated with a wormhole.

During the analysis phase, the destination node closely monitors the box plot for any deviations from expected timing patterns. Outlier values, characterized by their significant deviation from the median and quartiles, are flagged as potential indicators of a wormhole. The detection algorithm triggers an alert or initiates mitigation measures upon detecting such outlier values, indicating a suspicious communication path that may be associated with a wormhole.

The comparison of a box plot without an outlier is shown in Figure 2, while a box plot with an outlier is shown in Figure 3. The difference highlights the deviations in propagation delay patterns caused by the introduction of a wormhole, showcasing

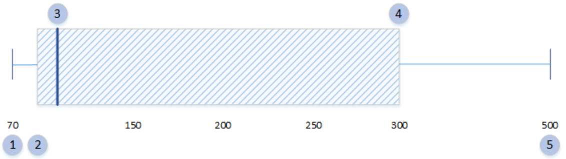

Fig. 3. Box plot with outlier.

the usefulness of box plots in detecting and visualizing such anomalies in wireless network communication. Figure 3 serves as the digital signature of a wormhole presence in a wireless network, reflecting the characteristic traits associated with such a malicious entity. A fundamental objective of a wormhole is to project itself in the network as the optimal pathway from a source to a designated destination node.

This objective is achieved by strategically bypassing a sufficient number of normal nodes, thereby reducing the overall path length to the shortest possible route. The minimum requirement for this bypassing operation is the circumvention of at least two normal nodes. In the depicted scenario illustrated in Figure 4, wormhole nodes W1 and W2 effectively bypass three normal nodes, namely N2, N3, and N4. As a result, the hop count diminishes from 5 to 4, thereby prompting the network to reevaluate and select a new optimal path. This transition is visually represented in the box plot in Figure 3 as a change in the maximum value.

Specifically, the propagation delay associated with the N1-W1 and W2-N5 links is expected to align with the values depicted in Table II. However, the propagation delay for the W1-W2 link significantly exceeds the previously observed maximum value. Upon reception of the RREQ message at the destination node, comprehensive information regarding the network links and their corresponding timing metrics becomes available, enabling the destination node to make an informed decision in selecting the new preferred route.

IV. Results

This section presents the research findings on detecting wormholes in a wireless network. The analysis of the experimental data has yielded promising results. An example of a simple wireless network with a wormhole implant is presented in Figure 4, including the associated propagation timing shown in Table II. Using values from this table, a box plot is created, indicating outlier data as possible wormhole links.

A. Example Network and Associated Data

The NS-3 network simulator serves as a testbed due to its ability to extract propagation delay metrics between network nodes, making it an ideal tool for experimental analysis. Several example networks, with and without wormholes, were created using standard wireless network configurations. The routing table produced by the NS-3 network simulator shows the preferred route selected by the destination node. The selected route for Figure 4 without the wormhole is N1-N2-N3-N4-N5-N6, so the propagation delay for this route is 97.25 + 101.45 + 101.45 + 100.12 + 95.58 = 495.85(ns). After the insertion of the wormhole, the routing table shows the preferred path is now N1-W1-W2-N5-N6. Values for this path are 83.39 + 502.84 + 73.16 + 95.58 = 754.97ns.

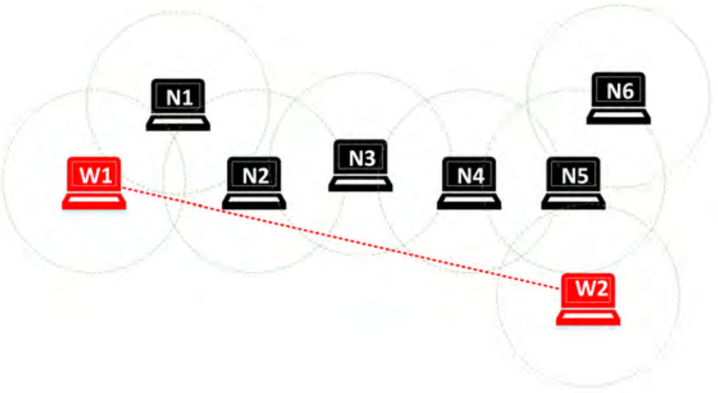

Fig. 4. Simple network with wormhole.

TABLE II
PROPAGATION DELAYS FOR ALL NETWORK LINKS

Link	*Propagation Delay(ns)*	*Distance(m)*
n1-n2	97.25	29.15
n2-n3	101.45	30.41
n3-n4	101.45	30.41
n4-n5	100.12	30.02
n5-n6	95.58	28.65
n1-w1	83.39	25.00
n5-w2	73.16	21.93
w1-w2	502.84	150.75

B. Creating the Box Plots

The box plot example without the wormhole was created using seven values: 97.25, 101.45, 101.45, 100.12, 95.58, 83.39, and 73.16 which are the propagation values from Table II. The first step in creating a box plot is to sort the values in ascending order or 73.16, 83.39, 95.58, 97.25, 100.12, 101.45, and 101.45. Next, the five summary statistics are:

- Minimum value: 73.16
- Lower quartile (Q1): 89.48 (the median of the lower half of the data: 73.16, 83.39, 95.58, 97.25)
- Median (Q2): 97.25 (the middle value of the dataset)
- Upper quartile (Q3): 100.78 (the median of the upper half of the data)
- Maximum value: 101.45.

Outliers on box plots are defined by a value that is 1.5 times bigger or smaller than the expected value. It is defined by the 1.5 IQR Rule. The Inter Quartile Range, IQR, is shown in Figure 2 as $IQR = Q3 - Q1$. In this case, the $IQR = 100.78 - 89.48 = 11.30$. To identify outliers, the range would be:

- Lower outlier value: $Q1 - 1.5 * IQR = 89.48 - (1.5 * 11.30) = 72.53$
- Upper outlier value: $Q3 + 1.5 * IQR = 100.78 + (1.5 * 11.30) = 117.73$

DOI: 10.62915/2472-2707.1193

Values are considered outliers if they were less than the lower outlier value or greater than the upper outlier value. Notice that the above values did not include the propagation delay by the wormhole which is shown in Table II as link w1-w2.

TABLE III
BOX PLOT VALUES

Measurement	*Without Wormhole*	*With Wormhole*
Population size	7	8
Minimum	73.16	73.16
Maximum	101.45	502.84
First Quartile	89.48	89.48
Third Quartile	100.78	101.45
Quartile Range	11.30	11.97
Median	97.25	98.68
Outlier	None	502.84
IQR	11.30	11.97
Outlier Upper	117.73	119.40

It can be seen as shown in Table III, the comparison of the values with and without a wormhole. The maximum value of 502.84 is clearly much greater than the outlier limit of 119.40. In this case, the outlier is tagged as the link with the propagation delay of 502.84ns.

C. Wormhole Detection: AODV-PD in Comparison to Existing Methods

Numerous detection methods, detailed in the Detection Strategies section, each have unique approaches and techniques. Complex methods for detecting wormhole attacks include IDS [10], Cryptographic [41], and Statistical [25] methods. Lesser complex methods include anomaly-based [6], reputation-based [14], timing-based [29], and cooperation-based [17] detection. One of the features of the AODV-PD protocol is its simplicity of implementation. The AODV-PD protocol incorporates statistical and timing methods but with some differences. Statistical analysis methods from other authors [24], [25], [27], [42] vary from hypothesis-based detection [24] to multi-path routing statistics [42]. Correspondingly, timing methods range from precision instrument measurements [29] to complex round-trip timing (RTT) measurements [28].

The proposed AODV-PD protocol offers significant advantages over the methodologies proposed by Qian, et al. [25], Zhao, et al. [27], and Hurley, et al. [24] in terms of simplicity and efficiency. While Qian's approach utilizes multi-path selection and statistical analysis for measurement, it can introduce complexity and computational overhead in large-scale networks. In contrast, the AODV-PD protocol leverages propagation delay analysis, a straightforward and effective method that does not require intricate multi-path selection algorithms. Additionally, Zhao's method combines graph theory and statistics for wormhole detection, relies on extensive neighbor information storage at each node, potentially leading to increased memory usage and management overhead. In contrast, the AODV-PD protocol maintains a lightweight overhead by focusing on propagation delay data without necessitating extensive neighbor information storage. Furthermore, Hurley's method emphasizes hypothesis-based decision-making for push attacks, and may lack robustness in detecting diverse wormhole attack scenarios. The AODV-PD protocol's proactive and adaptive approach, coupled with its efficient propagation delay analysis, ensures reliable wormhole detection and mitigation without compromising network performance or introducing unnecessary complexities.

Timing is a major concern of this research, making comparisons with the work of Bahillo, et al. [29] and Van Tran, et al. [30] particularly relevant as both researchers use timing in their methodologies. Bahillo's approach incorporates round trip timing (RTT) measurements, while Van Tran focuses on propagation delay. Evaluation of these methods is based on their ease of implementation, computational overhead, scalability and efficiency, detection accuracy and robustness, and adaptability to real-world networks. The comparative analysis is presented in Table IV, highlighting the advantages and limitations of each approach compared with the AODV-PD protocol.

TABLE IV
COMPARISON WITH OTHER TIMING METHODS

Criteria	*Bahilllo's RTT Method*	*Van Tran's Method*	*AODV-PD Protocol*
Simplicity of Implementation	Requires external timing measurements and protocol modifications	Utilizes complex algorithms and multiple detection strategies	Uses inherent propagation delay values; no additional hardware or protocol changes
Computational Overhead	High, due to intricate timing mechanisms and hardware modifications	High, due to complex and resource-intensive detection strategies	Low, with lightweight computational load focused on propagation delay analysis
Scalability and Efficiency	Limited scalability, as complex methods can hinder performance	Struggles with scalability due to extensive data processing	Designed for scalability, efficiently handles large and dynamic networks
Detection Accuracy and Robustness	Accurate, but potentially over-reliant on precise timing measurements	Accurate, but computationally expensive	High accuracy with efficient and simple detection mechanisms
Adaptability to Real-World Networks	May face challenges in real-world applications due to complexity	Challenges due to resource requirements and complexity	Proven adaptable to various network conditions, practical for real-world deployment

While future evaluations could consider a broader range of metrics such as throughput, end-to-end delay, and network overhead, examining trade-offs among these metrics will be crucial for a comprehensive understanding of performance distinctions. The AODV-PD protocol's attributes include simplified and efficient wormhole detection mechanisms, scalability, adaptability to diverse network environments, and maintaining a satisfactory Packet Delivery Ratio (PDR) even under wormhole attacks. Integrating these attributes into performance evaluations will provide valuable insights into the protocol's overall effectiveness and suitability for real-world deployment in wireless networks.

V. Discussion

In this paper, we proposed the AODV-PD protocol for detecting wormhole attacks in wireless networks. We compared the performance of our protocol with other presented methods in terms of simplicity, scalability, and packet delivery ratio. The implementation of the proposed method yielded several key findings that underscore its ability in addressing wormhole attacks in wireless networks.

A. Simplified Wormhole Detection with AODV-PD

The AODV-PD protocol distinguishes itself through its simplicity and efficiency in both implementation and identification and mitigation of wormhole attacks, especially when contrasted with more complicated protocols such as the neighbor discovery or Split Multi-path Routing (SMR) techniques advocated by Khalil, et al. [5] and Lee, et al. [4]. These methods often introduce unnecessary complexity and computational burdens, making them less practical and effective compared to the streamlined approach offered by the AODV-PD protocol. Various methods proposed for detecting wormholes in wireless networks emphasize the importance of timing as a critical factor. Typically, this timing is based on the distance between neighboring nodes, although the calculation methods can vary significantly. For instance, Bahillo et al. [29] introduce a sophisticated timing method that necessitates external timing measurements and modifications to the routing protocol. Similarly, Korkmaz et al. [28] propose Round Trip Timing (RTT), which adds complexity by integrating power readings with RTT measurements to assess the presence of malicious nodes. In contrast, the AODV-PD protocol simplifies the timing process by leveraging built-in propagation delay values, consolidating all calculations at the destination node without introducing additional complexities. By associating propagation delay values with Route Request (RREQ) messages and conducting statistical outlier detection at the destination node, the AODV-PD protocol achieves robust wormhole detection without imposing significant computational overhead or requiring specialized hardware. This streamlined approach enhances the protocol's scalability, real-time responsiveness, and applicability to diverse network environments, making it a practical and efficient solution for defending against wormhole attacks in wireless networks.

B. Scalability and Adaptability

The scalability of a new method for detecting and mitigating wormholes in wireless networks is critical to its viability and practicality. Research by Li et al. [43] illustrates the influence of scalability on network throughput, demonstrating how changes in network size, coverage area, and packet complexity can impact performance.

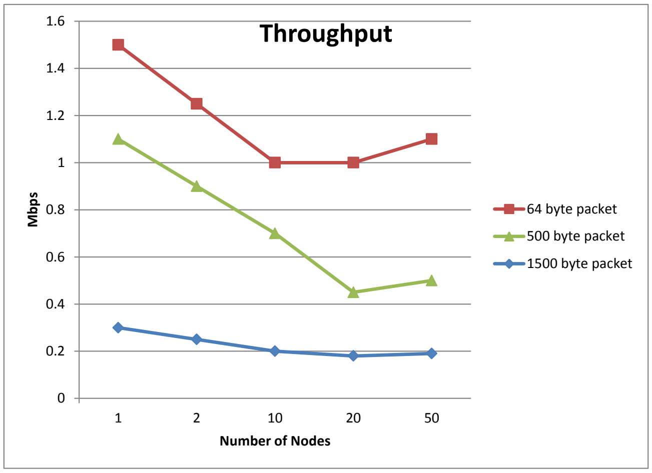

Fig. 5. Throughput scalability

This issue is evident in Figure 5 depicting throughput variations with varying packet sizes and numbers of nodes. Hu et al. [44] highlight scalability challenges in ad hoc network routing, a sentiment supported by the work of Gupta et al. [45]. The AODV-PD protocol aligns with similar scalability patterns. By leveraging built-in propagation delay values and aggregating calculations at the destination node, the AODV-PD protocol streamlines the detection and mitigation process without introducing unnecessary complexity that could hinder scalability. This approach ensures the protocol can effectively adapt to changes in network size, node density, and communication complexity, maintaining reliable performance across diverse wireless network environments.

C. Packet Delivery Ratio

The normal AODV protocol typically exhibits a Packet Delivery Ratio (PDR) ranging between 95% to 100% in networks with fewer than 20 nodes. Network results by Mistry, et al. [46] and Singh, et al. [47] show in Figure 6 the PDR approaches 100% out to 80 nodes. The AODV-PD protocol only accumulated data for 20 nodes but demonstrates a comparable PDR performance, primarily due to the possibility that a wormhole may refrain from triggering network malfunction notifications.

This similarity is crucial as maintaining a high PDR is essential for efficient communication and network reliability. The AODV-PD protocol's innovative approach to wormhole detection and mitigation has been rigorously evaluated through experimentation and simulation using the NS-3 network simulator. The results show that the AODV-PD protocol effectively detects and mitigates wormhole attacks without significantly impacting the overall packet delivery efficiency of the network. This finding underscores the protocol's practicality and suitability for deployment in real-world wireless network environments.

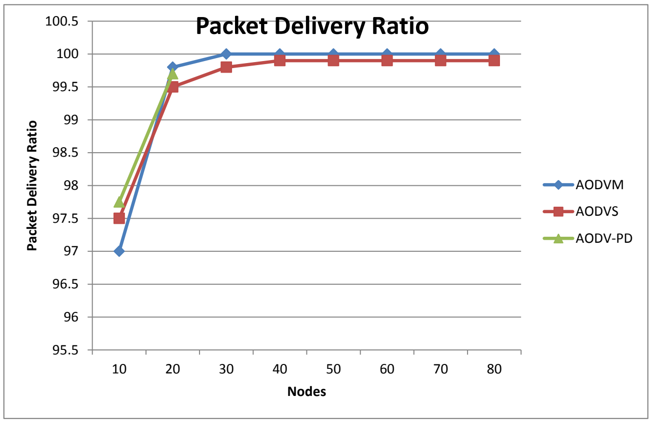

Fig. 6. Packet Delivery Ratio

D. Practical Deployment Challenges

Scalability and Adaptability: The section on Scalability and Adaptability examines the performance of the AODV-PD protocol across various network sizes and densities. This section references the findings of Li, et al. [43], Hu, et al. [44], and Gupta, et al. [45] as to scalability, demonstrating the effectiveness and adaptability of the AODV-PD protocol in diverse network environments.

Anomaly Detection Techniques: This research is concerned with both timing and anomaly detection, recognizing the importance of these areas in the detection of wormhole attacks. Future comparison studies will cover not only timing but also more in-depth anomaly detection techniques. Anomaly detection involves identifying deviations from normal network behavior, which is crucial for early and accurate detection of wormhole attacks. Comparisons in future research will include anomaly detection methods alongside statistical techniques as proposed by Nakayama, Hurley, Qian, Song, and Zhao [6], [24], [25], [27], [48]. These studies will help highlight the strengths and weaknesses of the AODV-PD protocol in various detection scenarios, ensuring a thorough evaluation of its performance in real-world applications.

Integration with IDS Systems: Integrating the AODV-PD method with existing Intrusion Detection Systems (IDS) represents a significant research effort. For the AODV-PD protocol to be useful, it must seamlessly integrate with other systems. This integration requires careful consideration of compatibility, communication protocols, and system interoperability, each of which could form the basis of dedicated research projects. Beyond that, exploring hybrid systems, which combine multiple detection methods for enhanced security, is an unfamiliar yet promising area. The development and testing of such hybrid systems will require significant research to understand how different detection mechanisms can effectively work together. This exploration will help to add to the strengths of each method while mitigating their weaknesses.

E. Summary

To get accurate and meaningful results, it's important to choose the right performance measures. Common ones include packet delivery ratio (PDR), average end-to-end delay, throughput, and the number of control messages. In wireless networks, it is vital to compare networks without wormholes (control groups) to networks with wormholes (treatment groups) to see how well wormhole detection methods work. When comparing these measures, researchers often use statistical tests like the Mann-Whitney U test, two-sample t-test, and Levene's test. The Mann-Whitney U test is useful when the data doesn't follow a normal distribution because it compares the order of the values rather than their averages, which makes it less sensitive to outliers. The two-sample t-test assumes that the data is normally distributed and checks if there is a significant difference between the averages of the two groups. Levene's test checks if the variances between the groups are equal, ensuring that the assumptions for the t-test are correct. By using these tests, researchers can see how wormholes affect network performance, giving them a better understanding of how well the detection methods work under different conditions.

The proposed wormhole attack detection method offers simplicity, scalability, and efficiency, making it easily integrated into existing wireless networks. Its simplicity stems from minimal hardware requirements and straightforward modifications to the AODV protocol, facilitating widespread adoption across diverse environments. The scalable nature of the detection criteria ensures effective deployment across networks of varying sizes and complexities, accommodating dynamic wireless network structures. Despite comprehensive detection capabilities, the method has negligible impact on packet delivery ratio and communication delays, seamlessly integrating with existing routing protocols. This adaptability underscores its suitability for real-world scenarios, where swift and accurate detection of wormholes is vital. The box plot results hint at future developments, potentially incorporating digital signatures for enhanced network security.

Despite positive outcomes, certain limitations in the study must be acknowledged. The method may not be effective against sophisticated wormhole attacks using multiple tunnels or hop counts, requiring further investigation and refinement. The study primarily focused on simulated environments, and real-world deployments may present unforeseeable challenges warranting exploration in future research.

To build on these findings, future research should explore the practical deployment of the proposed method in diverse real-world scenarios. Investigating its adaptability to varying network dynamics, understanding the potential impact of network size, and validating its effectiveness against growing attack strategies are avenues worth exploring. Furthermore, exploring potential optimizations and enhancements, such as incorporating machine learning algorithms for adaptive threat detection, could further advance the state-of-the-art in wireless network security.

VI. Conclusion

Detecting wormhole attacks in wireless networks remains highly challenging, particularly in the absence of a definitive digital signature for such attacks. Our study has demonstrated the limitations of existing detection methods, highlighting the need for innovative solutions. While our proposed method is a step forward, further refinement and exploration of alternative solutions are imperative. Future research should prioritize developing advanced simulation software for detection and mitigation, along with potential revisions to communication protocols in wireless networks. Additionally, integrating IoT and MANET networks into these research efforts is crucial. Investigating the feasibility of using box plot information as a dependable digital signature for wormhole attacks requires thorough research to validate its effectiveness. Advancing these research avenues can significantly enhance the security posture of wireless networks and fortify them against malicious threats.

References

[1] Viren Mahajan, Maitreya Natu, and Adarshpal Sethi. Analysis of wormhole intrusion attacks in manets. In *Military Communications Conference, 2008. MILCOM 2008. IEEE*, pages 1–7. IEEE, 2008.

[2] Hon Sun Chiu and King-Shan Lui. Delphi: wormhole detection mechanism for ad hoc wireless networks. In *Wireless pervasive computing, 2006 1st international symposium on*, pages 6 pp.–6. IEEE.

[3] Reshmi Maulik and Nabendu Chaki. A comprehensive review on wormhole attacks in manet. In *Computer Information Systems and Industrial Management Applications (CISIM), 2010 International Conference on*, pages 233–238. IEEE, 2010.

[4] Gunhee Lee, Jungtaek Seo, and Dong-kyoo Kim. An approach to mitigate wormhole attack in wireless ad hoc networks, 2008.

[5] Issa Khalil, Saurabh Bagchi, and Ness B Shroff. Mobiworp: Mitigation of the wormhole attack in mobile multihop wireless networks. *Ad Hoc Networks*, 6(3):344–362, 2008.

[6] Hidehisa Nakayama, Satoshi Kurosawa, Abbas Jamalipour, Yoshiaki Nemoto, and Nei Kato. A dynamic anomaly detection scheme for aodv-based mobile ad hoc networks. *IEEE transactions on vehicular technology*, 58(5):2471–2481, 2008.

[7] Ju Long, Li Hongjuan, Liu Yaqiong, Xue Weilian, Li Keqiu, and Chi Zhongxian. An improved intrusion detection scheme based on weighted trust evaluation for wireless sensor networks. In *Ubiquitous Information Technologies and Applications (CUTE), 2010 Proceedings of the 5th International Conference on*, pages 1–6, 2010.

[8] Pavan Pongle and Gurunath Chavan. Real time intrusion and wormhole attack detection in internet of things. *International Journal of Computer Applications*, 121(9), 2015.

[9] Khaled Mohammed Saifuddin, Abu Jobayer Bin Ali, Abu Shakil Ahmed, Sk Shariful Alam, and Abu Saleh Ahmad. Watchdog and pathrater based intrusion detection system for manet. In *2018 4th International Conference on Electrical Engineering and Information and Communication Technology (iCEEiCT)*, pages 168–173. IEEE, 2018.

[10] Giovanni Vigna, Fredrik Valeur, and Richard A. Kemmerer. Designing and implementing a family of intrusion detection systems, 2003.

[11] Kevin Hoffman, David Zage, and Cristina Nita-Rotaru. A survey of attack and defense techniques for reputation systems. *ACM Comput. Surv.*, 42(1):1–31, 2009.

[12] S. Laniepce, L. Lancieri, M. Achemlal, and A. Bouabdallah. A cross-layer reputation system for routing non-cooperation effects mitigation within hybrid ad-hoc networks, 2010.

[13] D. McCoy, Doug Sicker, and D. Grunwald. A mechanism for detecting and responding to misbehaving nodes in wireless networks. In *Sensor, Mesh and Ad Hoc Communications and Networks, 2007. SECON '07. 4th Annual IEEE Communications Society Conference on*, pages 678–684, 2007.

[14] T Padmavathy, G Sumathi, and K Srinivasan. Reputation based efficient isolation of wormhole nodes. *International Journal of Computer Applications*, 70(7), 2013.

[15] Shabina Parbin and Leeladhar Mahor. Analysis and prevention of wormhole attack using trust and reputation management scheme in manet. In *2016 2nd International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT)*, pages 225–228. IEEE, 2016.

[16] Gruia Calinescu. Computing 2-hop neighborhoods in ad hoc wireless networks. In *International Conference on Ad-Hoc Networks and Wireless*, pages 175–186. Springer.

[17] Marco Fiore, Claudio Ettore Casetti, Carla-Fabiana Chiasserini, and Panagiotis Papadimitratos. Discovery and verification of neighbor positions in mobile ad hoc networks. *IEEE Transactions on Mobile Computing*, 12(2):289–303, 2013.

[18] Jin Guo and Zhi-yong Lei. A kind of wormhole attack defense strategy of wsn based on neighbor nodes verification. In *Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on*, pages 564–568. IEEE, 2011.

[19] Panos Papadimitratos, Marcin Poturalski, Patrick Schaller, Pascal Lafourcade, David Basin, Srdjan Capkun, and Jean-Pierre Hubaux. Secure neighborhood discovery: a fundamental element for mobile ad hoc networking. *IEEE Communications Magazine*, 46(2), 2008.

[20] Radu Stoleru, Haijie Wu, and Harshavardhan Chenji. Secure neighbor discovery in mobile ad hoc networks. In *2011 IEEE Eighth International Conference on Mobile Ad-Hoc and Sensor Systems*, pages 35–42. IEEE, 2011.

[21] Anil Kumar Fatehpuria and Sandeep Raghuwanshi. An efficient wormhole prevention in manet through digital signature. *International Journal of Emerging Technology and Advanced Engineering*, 3(3), 2013.

[22] Daniele Raffo, dric Adjih, Thomas Clausen, Paul M, 252, and hlethaler. An advanced signature system for olsr, 2004.

[23] P. Sharma and A. Trivedi. An approach to defend against wormhole attack in ad hoc network using digital signature. In *2011 IEEE 3rd International Conference on Communication Software and Networks*, pages 307–311, 2007.

[24] Neil Hurley, Zunping Cheng, and Mi Zhang. Statistical attack detection, 2009.

[25] Lijun Qian, Ning Song, and Xiangfang Li. Detecting and locating wormhole attacks in wireless ad hoc networks through statistical analysis of multi-path. In *Wireless Communications and Networking Conference, 2005 IEEE*, volume 4, pages 2106–2111. IEEE, 2005.

[26] Sejun Song, Haijie Wu, and Baek-Young Choi. Statistical wormhole detection for mobile sensor networks. In *Ubiquitous and Future Networks (ICUFN), 2012 Fourth International Conference on*, pages 322–327. IEEE, 2012.

[27] Zhibin Zhao, Bo Wei, Xiaomei Dong, Lan Yao, and Fuxiang Gao. Detecting wormhole attacks in wireless sensor networks with statistical analysis. In *2010 WASE International Conference on Information Engineering*, volume 1, pages 251–254. IEEE, 2010.

[28] Turgay Korkmaz. Verifying physical presence of neighbors against replay-based attacks in wireless ad hoc networks. In *Information Technology: Coding and Computing, 2005. ITCC 2005. International Conference on*, volume 2, pages 704–709. IEEE, 2005.

[29] Alfonso Bahillo, Patricia Fernández, Javier Prieto, Santiago Mazuelas, Rubén M Lorenzo, and Evaristo J Abril. *Distance estimation based on 802.11 RTS/CTS mechanism for indoor localization*. IntechOpen, 2011.

[30] Phuong Van Tran, Le Xuan Hung, Young-Koo Lee, Sungyoung Lee, and Heejo Lee. Ttm: An efficient mechanism to detect wormhole attacks in wireless ad-hoc networks. In *Consumer Communications and Networking Conference, 2007. CCNC 2007. 4th IEEE*, pages 593–598. IEEE, 2007.

[31] Jane Zhen and Sampalli Srinivas. Preventing replay attacks for secure routing in ad hoc networks. In *International Conference on Ad-Hoc Networks and Wireless*, pages 140–150. Springer.

[32] Siwar Kriaa. Modeling the stuxnet attack with bdmp: Towards more formal risk assessments, 2012.

[33] LUKAS MILEVSKI. Stuxnet and strategy.

[34] Nicole Van der Meulen. Diginotar: Dissecting the first dutch digital disaster. *Journal of strategic security*, 6(2):46–58, 2013.

[35] Dávid János Fehér and Barnabas Sandor. Effects of the wpa2 krack attack in real environment. In *2018 IEEE 16th international symposium on intelligent systems and informatics (SISY)*, pages 000239–000242. IEEE, 2018.

[36] Zhen Ling, Junzhou Luo, Yang Zhang, and Ming Yang. A novel network delay based side-channel attack: Modeling and defense. *INFOCOM, 2012 Proceedings IEEE*, pages 2390–2398, 2012.

[37] Sumit Gwalani, Elizabeth M Belding-Royer, and Charles E Perkins. Aodv-pa: Aodv with path accumulation. In *Communications, 2003. ICC'03. IEEE International Conference on*, volume 1, pages 527–531. IEEE, 2003.

[38] Björn Wiberg. Porting aodv-uu implementation to ns-2 and enabling trace-based simulation, 2002.

[39] Ian D Chakeres and Luke Klein-Berndt. Aodvjr, aodv simplified. *ACM SIGMOBILE Mobile Computing and Communications Review*, 6(3):100–101, 2002.

[40] Charles Perkins, Elizabeth Belding-Royer, and Samir Das. Ad hoc on-demand distance vector (aodv) routing. Report 2070-1721, Nokia Research Center, 2003.

[41] Karim Seada, Cedric Westphal, and Charles Perkins. Analyzing path accumulation for route discovery in ad hoc networks. In *2007 IEEE Wireless Communications and Networking Conference*, pages 4377–4382. IEEE, 2007.

[42] Kimaya Sanzgiri, Daniel LaFlamme, Bridget Dahill, Brian Neil Levine, Clay Shields, and Elizabeth M Belding-Royer. Authenticated routing for ad hoc networks. *IEEE Journal on selected areas in communications*, 23(3):598–610, 2005.

[43] Jinyang Li, Charles Blake, Douglas S.J. De Couto, Hu Imm Lee, and Robert Morris. Capacity of ad hoc wireless networks, 2001.

[44] Yih-Chun Hu, Adrian Perrig, and David B Johnson. Wormhole detection in wireless ad hoc networks. *Department of Computer Science, Rice University, Tech. Rep. TR01-384*, 2002.

[45] Piyush Gupta and Panganmala R Kumar. The capacity of wireless networks. *IEEE Transactions on information theory*, 46(2):388–404, 2000.

[46] Nital Mistry, Devesh C Jinwala, and Mukesh Zaveri. Improving aodv protocol against blackhole attacks. In *Proceedings of the International Multi Conference of Engineers and Computer Scientists*, volume 2.

[47] Parvinder Singh, Dinesh Singh, and Vikram Singh. *Evaluation of Routing Protocols in MANETs with Varying Network Scope*. 2012.

[48] Ning Song, Lijun Qian, and Xiangfang Li. Wormhole attacks detection in wireless ad hoc networks: A statistical analysis approach. In *Parallel and distributed processing symposium, 2005. Proceedings. 19th IEEE international*, page 8 pp. IEEE, 2005.