Uluslararası Sürdürülebilir Mühendislik ve Teknoloji Dergisi
International Journal of Sustainable Engineering and Technology
Sayı: 1, Cilt: 7, (2023), Sayfa: 41-54

DETAILED ANALYSIS OF SYBIL ATTACK IN WIRELESS SENSOR NETWORKS

Abdullah ORMAN*1, Yunus ÜSTÜN[2], Murat DENER[2]

[1] Ankara Yıldırım Beyazıt Üniversitesi, Teknik Bilimler Meslek Yüksekokulu, Bilgisayar Teknolojileri Bölümü, Ankara
[2] Gazi Üniversitesi, Fen Bilimleri Enstitüsü, Bilgi Güvenliği Mühendisliği, Ankara

Article Info
Received: 28.05.2023
Accepted: 25.06.2023
Published: 29.06.2023

ABSTRACT

Wireless sensor networks often operate in unprotected, unavailable, or adverse conditions. Therefore, the security of wireless sensor networks is of great importance. Some of the most popular attacks among wireless sensor networks are DDOS attack, Sybil attack, Selective Routing attack, Wormhole attack and Blackhole attack. In the literature, there are many definitions of Sybil attack, which can be the most effective attack potential in wireless sensor networks, but most studies do not describe the Sybil attack in detail. They do not give detailed information about the implementation of the Sybil attack in the simulation environment. In a Sybil attack, the malicious node presents itself to neighboring nodes, along with many randomly generated or stolen identities. Unaware of anything, the victim node perceives the packet from the malicious node as if it came from another node with a different identity. By sending fake packets to the network in this way, it can negatively affect network traffic and cause nodes to be unable to exchange packets. In other effects, bogus packets generated by fake identities are collected at the base node, and the continuity and stability of the network can be compromised with phony information instead of accurate information on the network. In this study, the Sybil attack, a dangerous attack in wireless sensor networks, is explained in detail, and a step-by-step Sybil attack is carried out in the NS2 simulation environment. In addition, the application of 9 different scenarios created in the NS2 simulation environment and the effects of the Sybil attack on the system were analyzed. Each scenario was prepared with a different location and number of Sybil and replication nodes. In this way, the effects of the Sybil attack on the system have been observed in many cases. All data obtained by NS2 was used for analysis. As a result of the data, packet delivery speed, throughput, normalized forwarding load and end-to-end latency values were compared.

Keywords; Wireless sensor networks, security, Sybil attacks, nsGTFA

KABLOSUZ SENSÖR AĞLARDA SYBIL SALDIRISININ AYRINTILI ANALİZİ

Makale Bilgisi
Geliş tarihi: 28.05.2023
Kabul Tarihi: 25.06.2023
Yayın tarihi: 29.06.2023

ÖZET

Kablosuz algılayıcı (sensör) ağlar genellikle korumasız, kullanılamayan veya olumsuz koşullarda çalışmaktadır. Bu nedenle kablosuz algılayıcı ağların güvenliği büyük önem taşımaktadır. Kablosuz sensör ağları üzerinde en popüler saldırılardan bazıları DDOS saldırısı, Sybil saldırısı, Seçici Yönlendirme saldırısı, Wormhole saldırısı ve Blackhole saldırısıdır. Kablosuz sensör ağlarında en etkili saldırı potansiyeli olabilen Sybil saldırısının literatürde birçok tanımı bulunmakla birlikte çoğu çalışma Sybil saldırısını detaylı olarak açıklamamaktadır. Sybil saldırısının simülasyon ortamında uygulanması hakkında detaylı bilgi verilmemektedir. Bir Sybil saldırısında, kötü amaçlı düğüm kendisini komşu düğümlere rastgele oluşturulmuş veya çalınmış birçok kimlikle birlikte göstermektedir. Hiçbir şeyden habersiz olan kurban düğüm, kötü niyetli düğümden gelen paketi farklı bir kimliğe sahip başka bir düğümden gelmiş gibi algılar. Bu şekilde ağa sahte paketler göndererek ağ trafiğini olumsuz etkileyebilir ve düğümlerin paket alışverişi yapamamasına neden olabilir. Diğer

etkilerde, sahte kimlikler tarafından üretilen sahte paketler temel düğümde toplanır ve ağdaki doğru bilgiler yerine sahte bilgilerle ağın sürekliliği ve kararlılığı tehlikeye atılabilir. Bu çalışmada, kablosuz sensör ağlarında tehlikeli bir saldırı olan Sybil saldırısı detaylı bir şekilde anlatılmış ve NS2 simülasyon ortamında adım adım bir Sybil saldırısı gerçekleştirilmiştir. Ayrıca NS2 simülasyon ortamında oluşturulan 9 farklı senaryonun uygulaması ve Sybil saldırısının sisteme etkileri analiz edilmiştir. Her senaryo, farklı konum ve sayıda Sybil ve replikasyon düğümleri ile hazırlanmıştır. Bu sayede birçok durumda Sybil saldırısının sistem üzerindeki etkileri gözlemlenmiştir. NS2 tarafından elde edilen tüm veriler analiz için kullanılmıştır. Veriler sonucunda paket teslim hızı, verim, normalleştirilmiş iletim yükü ve uçtan uca gecikme değerleri karşılaştırılmıştır.

Anahtar Kelimeler; Kablosuz sensör ağları, güvenlik, Sybil saldırıları, nsGTFA

1. Introduction

Wireless sensor networks consist of small sensor nodes that work together to monitor and acquire data about an environment (Wadii et al.,2019). Wireless sensor networks are used in many areas, such as environmental protection, smart home and office applications, military surveillance, medical observation, etc. The main task of wireless sensor networks is to detect events, collect data and send it to the desired destination (Wadii et al., 2019). Wireless sensor networks are often used in remote and unprotected locations or where there are adverse operating conditions or even hostile operating conditions, so they are highly susceptible to intrusions and security attacks (Ezhilarasi et al., 2022). Therefore, wireless sensor networks are vulnerable to attack. Sybil attacks are classified as passive and active. In a passive attack, the attacker silently listens for communication and watches for packets. Attempts to change packages in an active attack (Sadeghizadeh, 2022). There are many attacks encountered by wireless sensor networks, including Sybil attack, Denial-of-Service (DoS), Worm Hole attack, Hello Flood attack, Node Capture attack, Sink Hole and Selective Forwarding attack (Pushpa and Raja, 2022).

Cyber-attacks fall into two categories:

- Deception attacks,
- Denial of service (DoS) attacks.

Deception attacks aim to manipulate the data packet to degrade the performance of the systems. On the other hand, DoS attacks try to block the transmission channel and consequently increase the communication error rate (Zhang et al., 2022). Sybil attack is one of the most harmful deception attacks targeting the security of wireless sensor networks. It is a powerful attack in which a malicious node illegitimately obtains the identities of legitimate nodes to gain high authority within the network, modify packets and damage the routing protocol. Since the duplicate nodes created by the Sybil node can be in different locations at the same time, the malicious node can create many fake routing paths and adversely affect the operation of the routing protocols (Almesaeed and Al-Salem, 2022).

There are methods used to identify and prevent Sybil attacks. These;

- Cryptographic Schemes: The most basic way to detect a Sybil attack on wireless sensor networks is to use symmetric encryption. However, it is challenging to implement in wireless sensor networks due to high memory usage and energy consumption.
- Random password comparison method (RPC): The dynamically randomly generated passwords by the base node are distributed to the nodes along with a routing table containing information about each node in the network. Incoming packets are compared with this table, and if the incoming packet is not from the Sybil node, it is understood that it came from a normal node. However, this method detects fewer Sybil nodes than other methods.
- Trust-based identification method (TBID): In this method, the network is divided into clusters, and a cluster head manages each cluster. Nodes calculate the trust value of neighboring nodes around them and send it per cluster. Nodes with low confidence are removed from the routing table. This method is the recommended method for Sybil attacks.
- Message authentication and passing method (MAP): In this method, all nodes have a crucial message authenticated by the authority. Before communication, nodes must establish the message authentication

method. Unverified identities cannot communicate with any other node again.

- Triangulation method: It uses triangulation to verify the positions of nodes to detect Sybil attacks. This method assumes that the Sybil nodes are in the exact location. Three nodes are used to form a triangle to identify the Sybil node and determine its place in the network. A specific location will be calculated based on the received signal strengths.

The detailed description of the Sybil attack, a type of attack in wireless sensor networks, and its implementation in the simulation environment are not available in the literature and are seen as a need for new researchers. In this study, the Sybil attack is described in detail and implemented in the NS2 simulation environment to meet this need. In line with the results obtained, the effect of the Sybil attack on wireless sensor networks can be analyzed against different scenarios. Briefly, the contributions of this study to the literature;

- Detailed description of the Sybil attack
- Practical demonstration of the steps of the Sybil attack
- Implementation of Sybil attack in 9 different scenarios in NS2 simulation environment
- Analyzing the Sybil node and its impact on the system based on the number and location of duplicate nodes
- Analyzing the effect of the Sybil attack on wireless sensor networks in line with the scenarios realized

The remaining parts of the study are listed as follows. Chapter 2 explains the definitions made for the Sybil attack in the literature and the simulation environments used. Chapter 3 talks about the Sybil attack. In Chapter 4, the implementation of the Sybil attack in the NS2 simulation environment is explained in detail. In Chapter 5, the results obtained from the application are mentioned. In the 6th section, the results are given.

2. Related Works

In the literature, there are various studies on the definition and implementation of the Sybil attack. According to Sadeghizadeh, Sybil node creates multiple routes with the help of duplicate nodes and confuses the routing protocol (Ezhilarasi et al., 2022). According to Vamsi and Kant, a Sybil attack is a node duplication attack in which a malicious node tries to mislead the system for its purposes by using the node identity and location information (Vamsi and Kant, 2014). According to Ezhilarasi et al., Sybil attacker creates nodes with stolen or forged IDs and locates them in different network locations. Therefore, fake nodes will be created by a single node, which affects the network performance (Sadeghizadeh, 2022). According to Avila et al., the purpose of the Sybil attack is to isolate network traffic from legitimate nodes and pull them towards duplicate nodes. This attack is carried out after the identity of legitimate nodes is stolen when a node is in several places simultaneously or the same node pretends to be several. This attack means incorrect information in the routing tables (Avila et al., 2021). According to Chen et al., Sybil attack is a security threat to wireless networks where a malicious node request multiple fake identity (Chen et al., 2021). According to Wadii et al., the Sybil attacker either steals the identity of a legitimate node or inserts a randomly generated node into the network whose identity does not exist. Therefore, the malicious node uses processes such as data collection, voting, and reputation evaluation against itself (Wadii et al., 2019). According to Ardakani et al., the attacker in the Sybil attack is an attacker in the network who uses the identity of other nodes for their benefit (Ardakani et al., 2022). According to Biswas et al., a Sybil attack that steals the identity of some legitimate nodes to interfere with the localization process is a replay attack that replaces localization information with false information to misidentify estimated locations (Biswas et al., 2022). According to Mehbodniya et al., in the Sybil attack, the malicious node introduces its neighbor nodes along with many randomly generated or stolen identities. The victim node, unaware of anything, perceives the packet from the malicious node with a different identity as if it came from another node. Sending fraudulent packets into the network in this way may adversely affect network traffic and cause nodes to be unable to exchange packets. In other effect, fake packets generated by fake identities are collected at the base node, and the continuity and stability of the network can be compromised with fake information instead of real information on the network (Mehbodniya et al., 2021). According to Singh et al., the Sybil attack could create multiple stolen or fabricated identities within the network to retrieve data from wireless sensors. This attack is also known as a single person with multiple identities. Each fake node created tries to steal important information flowing in the network (Singh and Saini, 2018). According to Zhukabayeva et al., Sybil attacks can seriously affect routing

protocol performance and compromise the entire system (Zhukabayeva, et al., 2020). According to Almesaeed et al., the Sybil attack is one of the most devastating attacks to compromise the security of wireless sensor networks. A malicious node is an effective attack by stealing or copying the identities of other legitimate nodes to gain high authority over the network and damage the routing protocol. Many routing paths occur because the fake duplicate nodes that the Sybil node creates can reside in different locations simultaneously. In this case, it can significantly affect the operation of the routing protocols of the system (Almesaeed and Al-Salem, 2022). According to Shehnaz and Nital, the malicious node obtaining a stolen or fabricated identity is called a Sybil attack. In a Sybil attack, a duplicate node can be in different locations simultaneously, or we can say that a single real node presents multiple fake identities to other nodes in the network (Shehnaz and Nital, 2017). According to Shehni et al., a legitimate node whose identity is stolen by the Sybil node and referred to as a "malicious node" advertises itself to the network by broadcasting stolen or randomly generated fake identities to the network from other legitimate nodes. Fake IDs represent nodes that don't exist (Shehni, Faez et al., 2018). According to Karakaya and Akleylek, the Sybil attack is an attack consisting of a node and multiple identities. In other words, an enemy can be in different positions simultaneously. A Sybil attack significantly reduces the efficiency of fault-tolerant systems. Since more than one identity can be defined for a node, location information can also be changed. It can perform a selective routing attack by causing the nodes to malfunction (Karakaya and Akleylek, 2018). According to Wang et al., the Sybil attack is hazardous. In the attack, malicious nodes can act as multiple nodes by stealing the identity of the target node or using randomly generated identities (Wang, Ma, and Bai, 2020). According to Sengupta et al., in a Sybil attack, a single malicious node uses multiple and manifests itself in different locations on the network. Malicious nodes with multiple identities are known as Sybil nodes. A Sybil attack on wireless sensor networks is devastating for protocols that use location information for routing. According to Jamshidi et al., in a Sybil attack, an adversary places a malicious node on the network, which becomes a multi-identity node, either randomly generated or stolen from legitimate nodes in the network, and after this, is referred to as Sybil. nodes. The malicious node can corrupt the routing tables by identifying itself to the network with multiple identities, making the real nodes believe that they have many neighbors that don't exist. Therefore, it causes system crash by corrupting routing protocols and affecting network operations such as data collection, voting, reputation evaluation, and fair resource allocation (Jamshidi et al., 2019). According to Angappan et al., the Sybil attack is initiated by spoofing existing identities or creating fake identities via a compromised node. A Sybil node in wireless sensor networks can change the decision of the voting mechanism in a group and severely disrupt network services. Such attacks increase network energy consumption, data cannot be verified, and break the routing protocol (Angappan et al., 2020). In this attack method, a malicious node with many fake identities prevents the target node from working as expected, causing the packet not to reach the sink (Ceyhan and Sagıroğlu, 2013).

There are various studies on the definition and implementation of the Sybil attack in the literature. However, they all have in common that the Sybil attack is not explained in detail in theory and practice. No detailed information is given about the steps and simulation of the Sybil attack. This study aims to describe, implement and convey the Sybil attack in the most detailed way against all studies in the literature.

3. Sybil Attack

In the Sybil attack, the malicious node introduces its neighbor nodes along with many randomly generated or stolen identities. The victim node, unaware of anything, perceives the packet from the malicious node with a different identity as if it came from another node. Sending fraudulent packets into the network in this way may adversely affect network traffic and cause nodes to be unable to exchange packets. In another effect, fake packets generated by fake identities are collected at the base node, and the continuity and stability of the network can be compromised with phony information instead of accurate information on the network (Mehbodniya et al., 2021).

It can classify Sybil attacks according to various features. The classification of Sybil attacks according to their communication, timing and identity is given in Figure 1 (Ardakani et al., 2022).

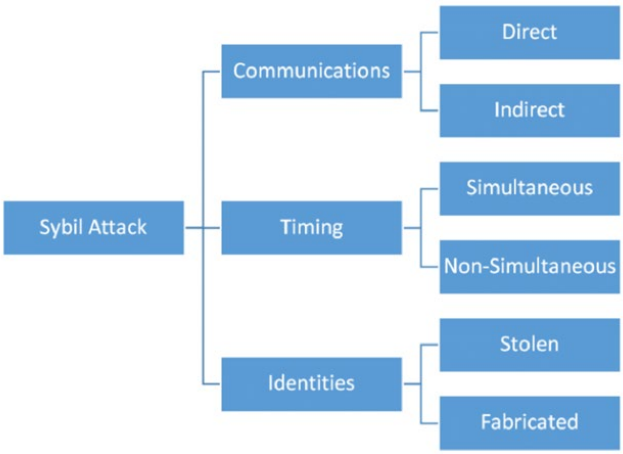

Figure 1. Classification of sybil attack

Regarding direct communication, the malicious node directly communicates with the real nodes and pulls the traffic towards itself. In indirect communication, the malicious node communicates via duplicate nodes instead of communicating directly with real nodes. In timing type Sybil attack, the malicious node either serves the data of all Sybil IDs simultaneously or in packets respectively (Zhukabayeva et al., 2020). In an identity type Sybil attack, the malicious node can create new identities or steal the identities of legitimate nodes. Creating new identities can cause the routing protocol to malfunction, thereby crashing the entire system. If the identities of legitimate nodes are stolen, especially if the stolen legitimate nodes are removed from the network, the attack may not be recognized in the network (Almesaeed and Al-Salem, 2022).

If network access is obtained using any of the methods mentioned above, the effect on the network can be achieved by any of the following ways (Zhukabayeva et al., 2020).

- Routing. Sybil attacks can disrupt routing protocols in wireless sensor networks, particularly the multicast routing mechanism. Another critical situation is that those duplicate nodes can be in multiple locations simultaneously, negatively affecting the routing protocol.
- They are interfering with voting and reputation systems. Sybil attack can be potent in any environment where there is a voting system for reporting and detecting misbehavior of nodes in the system, updating reputation scores, etc. For example, an attacker could generate enough malicious rogue nodes to exploit these reports and information and then remove legitimate nodes from the network (Zhukabayeva, Mardenov, and Abdildaeva, 2020).
- Fair distribution of resources. Sybil attacks can also allow an attacker to take an unfair and disproportionate share of resources that must be equally distributed among all nodes in the network. This attack deprives legitimate nodes of their rightful share of resources and ensures that the malicious nodes have more opportunities for further attacks.
- Distributed storage. Sybil can compromise file storage systems in peer-to-peer and wireless sensor networks. Data loss and duplication can be made in the file system. A system can be tricked into storing data in multiple Sybil IDs of the same host on the network.
- Data collecting. Sensor network readings are calculated through query protocols on the network and do not return assignments from each sensor. This is done to save the energy of the nodes. Duplicate nodes may report false sensor readings affecting the calculated total population. An attacker can significantly alter the set with sufficient identifiers.

3.1. Attack Steps

In Figure 2, the locations of the nodes in the environment are given.

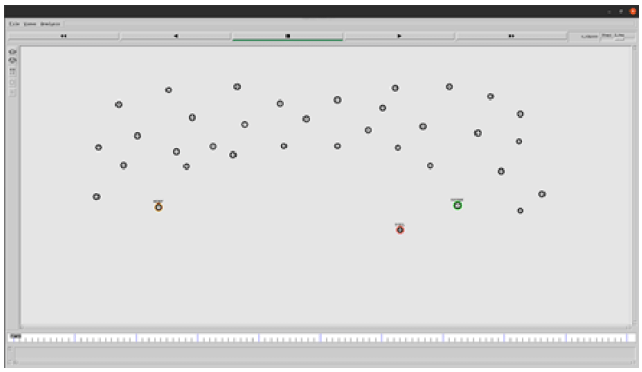

Figure 2. Attack steps - 1

The source node is green, the destination is orange, and the Sybil node is red. The source node wants to send data to the destination node, and the Sybil node intends to manipulate the flow of the network.

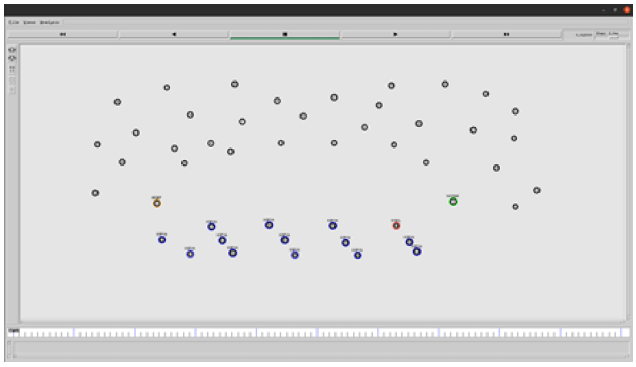

Figure 3. Attack steps - 2

As shown in Figure 3, the red Sybil node wants to influence the flow of the network by creating blue duplicate nodes.

In Figure 4, the source node in green is broadcasting to determine which route it will use to transmit data to the destination node in orange.

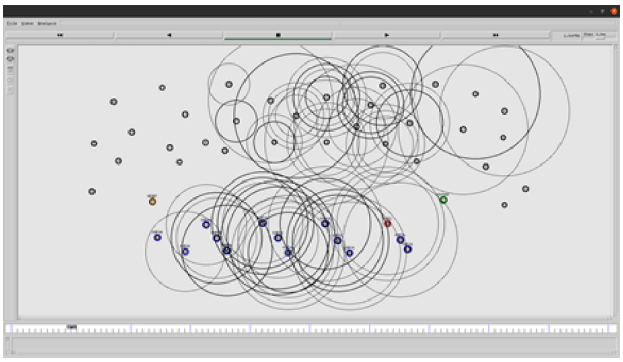

Figure 4. Attack steps - 3

Sybil attack is seen as safe by the source node as it creates too many duplicate nodes in the network. In addition, being closer to the destination node affects the route decision of the source node. Therefore, as a result of the broadcast in Figure 5, the green source node prefers to transmit the data over the blue colored copy nodes and the packets it sends do not reach the orange source node. Sybil attack has been carried out in the environment.

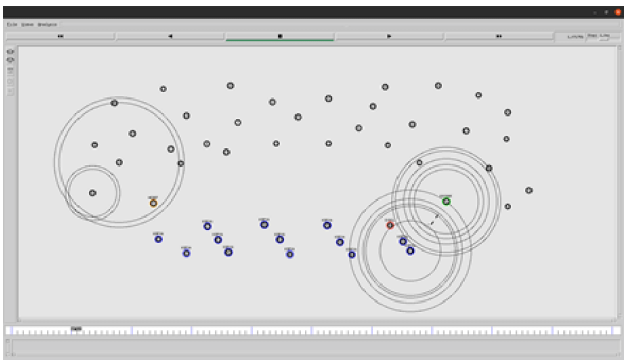

Figure 5. Attack steps - 4

4. Practice Scenario

The scenarios realized were carried out using the network simulation tool called NS2, which was installed on the Ubuntu 20.04 operating system. The 2.35 version of the NS2 tool was used. The NS2 tool is one of the most popular network simulators. The NS2 tool is a simple event simulation tool for studying the dynamic nature of communication networks and supports a wide variety of protocols at all layers (Ezhilarasi et al., 2022). It is aimed to simulate the Sybil attack by using various scenarios in applications and to observe the effect of the Sybil attack on wireless sensor networks. The simulation parameters are given in Table 1.

Table 1. Simulation parameters

No	Parameter	Value
1	Channel type	Channel/WirelessChannel
2	Propagation model	Propagation/TwoRayGround
3	Phy type	Phy/WirelessPhy
4	Mac protocol type	Queue/DropTail/PriQueue
5	Link layer type	LL
6	Antenna type	Antenna/OmniAntenna
7	Max packet in queue	50
8	Routing protocol	AODV
9	Agent trace	ON
10	Router trace	ON
11	Mac trace	ON
12	Movement trace	ON

4.1. Scenario 1

Scenario 1 ran for 10 seconds and is expected to send data from source to destination successfully. In this scenario, the Sybil node behaves like a normal node, and no behavior can be described as an attack on the network. Figure 6 gives the locations of the nodes in scenario 1.

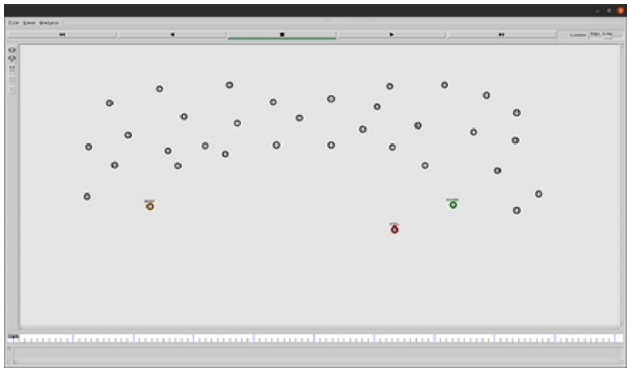

Figure 6. 1. Scenario Picture

4.2. Scenario 2

In Scenario 2, it is ensured that the Sybil node creates 3 duplicate nodes. Scenario 2 ran for 10 seconds. In this scenario, the Sybil node aims to disrupt the flow of the network through the 3 duplicate nodes it has created. Figure 7 gives the locations of the nodes in scenario 2.

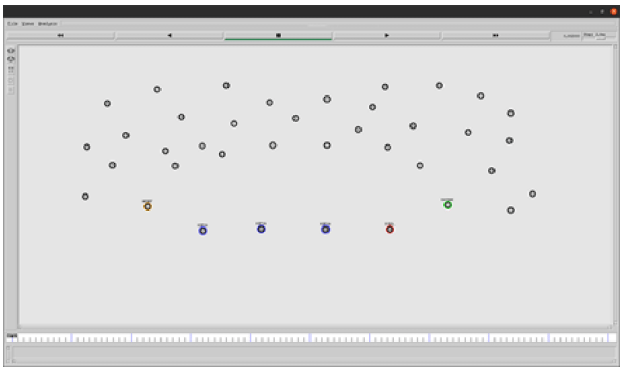

Figure 7. 2. Scenario Picture

4.3. Scenario 3

In Scenario 3, it is ensured that the Sybil node creates 8 duplicate nodes. Scenario 3 ran for 10 seconds. In this scenario, the Sybil node aims to disrupt the flow of the network through 8 duplicate nodes it has created. Figure 8 gives the locations of the nodes in scenario 3.

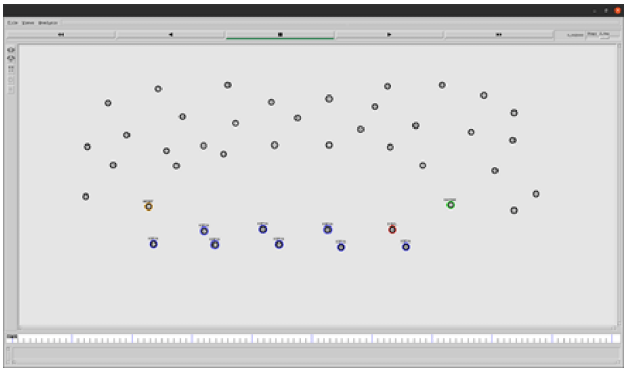

Figure 8. 3. Scenario Picture

4.4. Scenario 4

In scenario 4, the Sybil node is provided to create 13 duplicate nodes. Scenario 4 ran for 10 seconds. In this scenario, the Sybil node aims to disrupt the flow of the network through the 13 duplicate nodes it has created. In Figure 9, the locations of the nodes in scenario 4 are given.

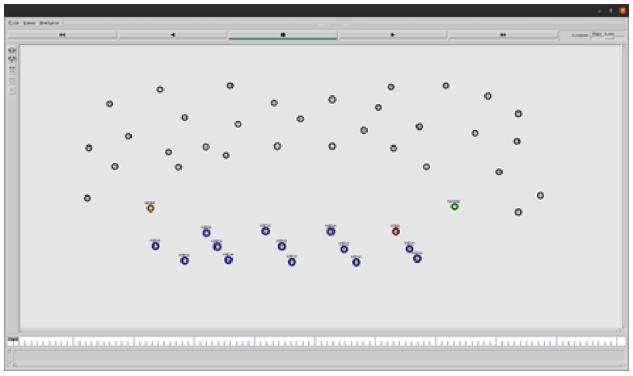

Figure 9. 4. Scenario Picture

4.5. Scenario 5

Scenario 5 ran for 30 seconds and is expected to send data from individual sources to the destination successfully. In this scenario, there is no Sybil node in the environment. Figure 10 gives the locations of the nodes in scenario 5.

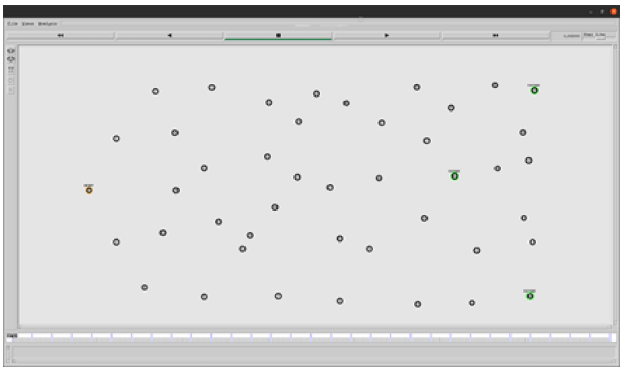

Figure 10. 5. Scenario Picture

4.6. Scenario 6

In Scenario 6, 1 Sybil node is positioned around the node that is thought to have the highest data flow, and it is ensured that the Sybil node creates 3 duplicate nodes. Scenario 6 ran for 30 seconds. This scenario aims to disrupt the flow of the network through 3 duplicate nodes created by a Sybil node. In Figure 11, the locations of the nodes in scenario 6 are given.

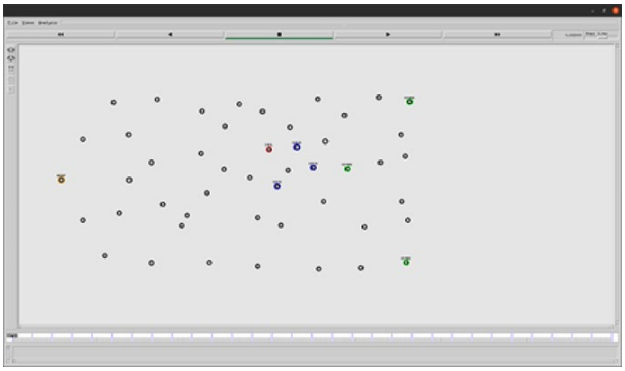

Figure 11. 6. Scenario Picture

4.7. Scenario 7

In scenario 7, 2 Sybil nodes are positioned around the nodes that are thought to have the highest data flow, and Sybil nodes are provided to create 6 duplicate nodes. Scenario 7 ran for 30 seconds. In this scenario, Sybil nodes aim to disrupt the flow of the network through the 6 duplicate nodes they have created. Figure 12 gives the locations of the nodes in scenario 7.

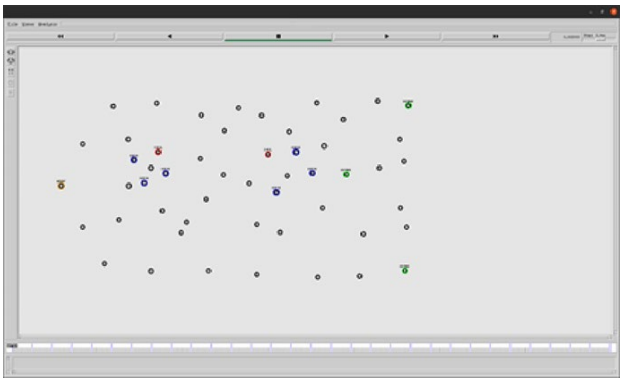

Figure 12. 7. Scenario Picture

4.8. Scenario 8

In scenario 8, 2 Sybil nodes are positioned around a node at the environment's edges, and Sybil nodes are provided to create 6 duplicate nodes. Scenario 8 ran for 30 seconds. In this scenario, Sybil nodes aim to disrupt the flow of the network through the 6 duplicate nodes they have created. Figure 13 gives the locations of the nodes in scenario 8.

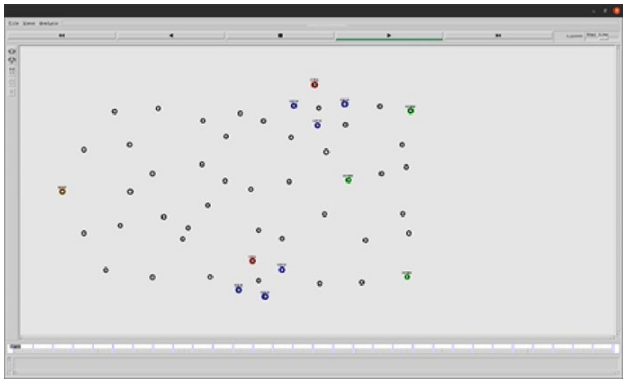

Figure 13. 8. Scenario Picture

4.9. Scenario 9

In scenario 9, 4 Sybil nodes are positioned around a node at the environment's edges, and Sybil nodes are provided to create 12 duplicate nodes. Scenario 9 ran for 30 seconds. In this scenario, Sybil nodes aim to disrupt the flow of the network through the 12 duplicate nodes they have created. Figure 14 gives the locations of the nodes in scenario 9.

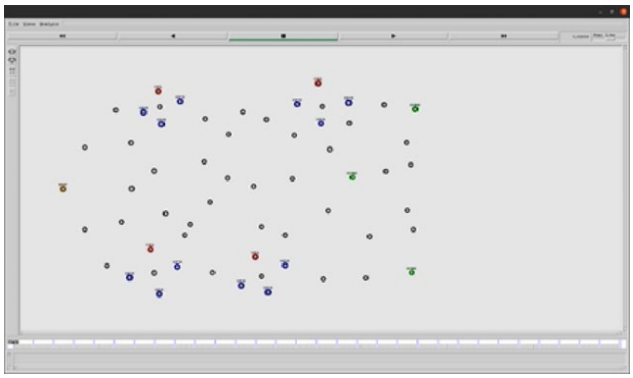

Figure 14. 9. Scenario Picture

5. Experimental Results

Tracing files were analyzed using the nsGTFA tool, and statistical results were obtained about the experiments. NsGTFA is a tool that can analyze NS2 wireless monitoring files in both old and new formats. This tool is fast enough to read millions of events in seconds, analyze trace files (performance metrics), and generate graphs and statistics about the behavior of streams in the simulation (Ibrahim et al., 2015).

The statistical results obtained show packet delivery rate, throughput, normalized forwarding load and end-to-end delay graphs. The general definitions of these graphs are given below.

- Packet delivery rate: It is defined as the ratio between the packets received by the destination and the packets generated by the

source. The package delivery rate may be low in 2 cases. First, there is a lot of data flow in the network, and packets are dropped. Second, an attack is taking place on the network.

- Throughput: The number of successfully received packets per unit time is represented in kbps. Low throughput can occur in two cases, as in the package delivery rate. First, there is a lot of data flow in the network, and packets are dropped. Second, an attack is taking place on the network.
- Normalized routing load: It is the ratio of all routing control packets sent by all nodes to the number of data packets received at the destination nodes. The normalized routing load will be excessive if there is a deficiency in the received routing control packets versus the packets sent. This can be interpreted as an attack on the network.
- End-to-end delay: It refers to the time it takes for a packet to be transmitted from source to destination over a network. End-to-end delay will also be excessive if the transmitted packets get stuck in an obstacle on the way. The presence of an attack on the network can also be an obstacle to how packages are sent.

The matplotlib library in the Python programming language was used to display the statistical results obtained by nsGTFA graphically. Python's version 3.8.10 and matplotlib version 3.5.2 were used. In Figure 15, the package delivery rate of the scenarios created from the data obtained as a result of the experiments is given.

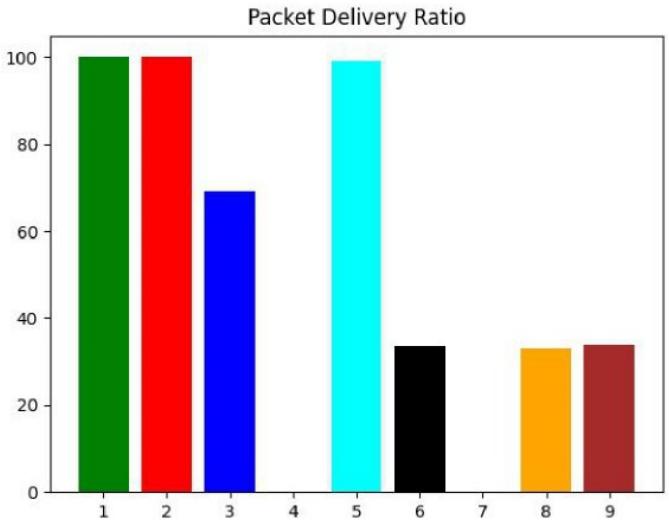

Figure 15. Packet delivery ratio

Package delivery rate; 100% in Scenario 1, 100% in Scenario 2, 69% in Scenario 3, 0% in Scenario 4, 100% in Scenario 5, 33% in Scenario 6, 0% in Scenario 7 33% in Scenario 8 and 34% in Scenario 9. The analyzes of why these results came out this way are given below based on a ratio.

It is seen that the package delivery rate is 100% in Scenario 1, Scenario 2 and Scenario 5. Due to the absence of Sybil attack in Scenario 1 and Scenario 5, it is expected to be 100%. In scenario 2, there are 3 duplicate nodes created by the Sybil node. None of these duplicate nodes communicates with legitimate nodes. In this scenario, Sybil and duplicate nodes communicate only with the source node. It is seen that the 3 duplicate nodes created are not sufficient for the route determined by the AODV routing protocol to go through the Sybil node.

In scenario 3, it is seen that the package delivery rate is 69%. In scenario 3, there are 8 duplicate nodes created by the Sybil node. None of these duplicate nodes communicates with legitimate nodes. Sybil and duplicate nodes only communicate with the source node. It is seen that the 8 duplicate nodes created are sufficient for a part of the route determined by the AODV routing protocol to go through the Sybil node. It is seen that the packages to be sent over the Sybil node are not delivered, and the package delivery rate is 69%.

It is seen that the package delivery rate is 33% in Scenario 6, 33% in Scenario 8 and 34% in Scenario 9. In scenario 6, 1 Sybil node and 3 duplicate nodes are placed in the middle of the network, at a point where packet exchange will be the most. In Scenario 8, 2 Sybil nodes and 6 duplicate nodes. In Scenario 9, 4 Sybil nodes and 12 duplicate nodes are placed at the edges of the network, that is, at the points where packet exchange is the least. According to the results obtained, Scenario 6, with 1 Sybil node in the middle of the network and Scenario 9, with 4 Sybil nodes at the edges of the network have the same packet delivery rate.

In Scenario 4 and Scenario 7, it is seen that the package delivery rate is 0%. In scenario 4, 13 duplicate nodes are used to fool the AODV routing protocol. In scenario 7, 2 Sybil nodes and 8 duplicate nodes are placed in the middle of the network, that is, at the points where the packet exchange will be the most. The Sybil attack showed its full effect, and the package delivery rate decreased to 0%.

As a result, In Scenario 1, Scenario 2, Scenario 3 and Scenario 4, the number of duplicate nodes gradually increased. There are 0, 3, 8 and 13 duplicate nodes, respectively. As a result of increasing the number of copy nodes, it was observed that the packet delivery rate of the system was 100%, 100%, 69% and 0% respectively. In this context, it is concluded that the presence of only one copy node in the environment is not sufficient to perform a Sybil attack; additionally, it is necessary to create an adequate number of duplicate nodes. In Scenario 6, Scenario 7, Scenario 8 and Scenario 9, the number and location of Sybil and duplicate nodes have been changed. In Scenario 6 and Scenario 7, Sybil and the duplicate nodes are located in the middle of the network, while in Scenario 8 and Scenario 9 they are at the edges of the network. Package delivery rates in Scenario 6, Scenario 8 and Scenario 9 are 33%, 33% and 34% respectively. In scenario 7, the package delivery rate is 0%. In this context, the effect of 4 Sybils and 12 duplicate nodes found at the network's edges on the system is equivalent to the effect of 1 Sybil and 3 duplicate nodes found in the middle of the network. In Figure 16, the efficiency of the scenarios created from the data obtained as a result of the experiments is given.

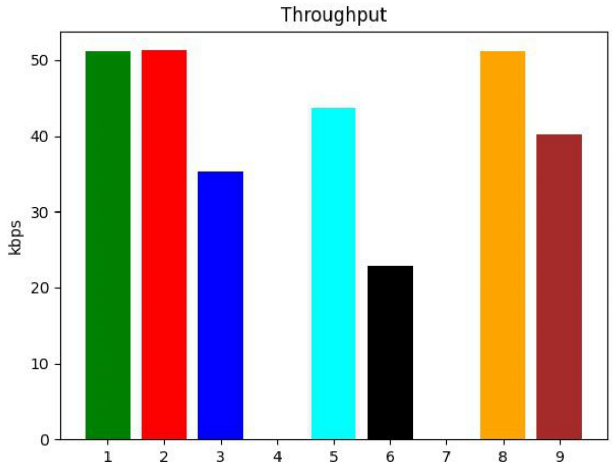

Figure 16. Throughput

Throughput; 51 kbps in Scenario 1, 51 kbps in Scenario 2, 35 kbps in Scenario 3, 0 kbps in Scenario 5, 44 kbps in Scenario 5, 23 kbps in Scenario 6, 0 kbps in Scenario 7, Scenario 8 51 kbps and 40 kbps in Scenario 9 were obtained. The analyzes of why these results came out this way are given below based on a ratio.

In Scenario 1, Scenario 2 and Scenario 8, it is seen that the throughput is 51 kbps. Scenario 2 has 3 duplicate nodes. In scenario 2, Sybil node wants to trick the routing protocol of the system through 3 duplicate nodes. Despite this, it is seen that the throughput is 51 kbps. Duplicate nodes in scenario 2 are not communicating with any legitimate nodes. They only communicate with the source node. Because of this, the routing protocol of the system wanted to send the packet over the legitimate nodes, not the Sybil node. As a result, their efficiency is equal.

It is seen that the throughput is 35 kbps in Scenario 3 and 40 kbps in Scenario 9. Scenario 3 has 8 duplicate nodes. Duplicate nodes do not communicate with legitimate nodes. It only communicates with the target node. Scenario 9 does not have 4 Sybil and 12 duplicate nodes. These nodes are located at the edges of the network, at the points where packet exchange is most miniature. In this context, the Sybil attack slightly affected the routing protocol, and some packets were intended to be sent over Sybil nodes. Packets arriving at Sybil nodes could not reach the destination. Because of this, it is seen that the throughput is 15 kbps on average compared to Scenario 1 and Scenario 2.

In scenario 6, it is seen that the throughput is 23 kbps. Scenario 6 has 1 Sybil and 3 duplicate nodes. These nodes are located in the middle of the network, at the point where the most packet exchange will occur. Although there were 4 Sybil and 12 duplicate nodes in Scenario 9, the throughput was 23 kbps lower in Scenario 6. Accordingly, the fact that the Sybil node is on the possible route increases the effect of the attack.

Scenario 4 and Scenario 7 are the scenarios where the Sybil attack is most effective. The routing protocol of the system wants to send all packets from the source to the destination via the Sybil node. Packets arriving at the Sybil node are unable to reach the source. Therefore, the throughput of these scenarios is 0 kbps.

As a result, it is seen that the Sybil attack also has a significant effect on the throughput. In Scenario 4 and Scenario 7, where the entire network is captured, it is seen that the throughput is 0 kbps. In scenario 4, there are 13 duplicate nodes for the throughput to be 0 kbps. In scenario 7, 2 Sybil and 6 duplicate nodes are positioned in the middle of the network so that the throughput can be 0 kbps. The low number of duplicate nodes or the location of duplicate nodes away from the route reduces the effectiveness of the attack or neutralizes the attack.

In Figure 17, the end-to-end delays of the scenarios created from the data obtained as a result of the experiments are given.

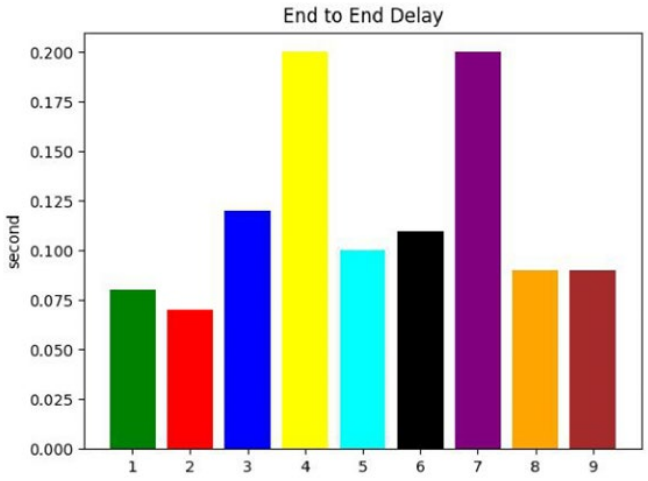

Figure 17. End to end delay

End-to-end delay; Scenario 1 is 0.08 seconds, Scenario 2 is 0.07 seconds, Scenario 3 is 0.12 seconds, Scenario 4 is 0.20 seconds, Scenario 5 is 0.10 seconds, Scenario 6 is 0.11 seconds, Scenario 7 is 0.20 seconds, Scenario 0.09 seconds were obtained in 8 and 0.09 seconds in Scenario 9. The analyzes of why these results came out this way are given below based on a ratio.

It is seen that the end-to-end delay in Scenario 4 and Scenario 7 is 0.20 seconds. The Sybil attack is most effective in Scenarios 4 and 7. As a result of the Sybil node receiving all the packets flowing on the system, the packages cannot reach the source. As a result, the end-to-end latency values are the highest.

The end-to-end delay is 0.12 seconds in Scenario 3 and 0.11 seconds in Scenario 6. The end-to-end delay in scenario 3 is 0.12 seconds because the Sybil node has created 8 duplicate nodes. The end-to-end delay is 0.11 seconds in scenario 6 because Sybil and duplicate nodes are placed in the middle of the network. The 8 duplicate nodes created and the duplicate nodes placed in the middle of the network slightly affected the routing protocol of the system. The routing protocol has chosen to send some packets over the Sybil node, and the packets arriving at the Sybil node could not reach the destination node. In this case, it causes delays in the system.

In Scenario 8 and Scenario 9, the end-to-end delay is 0.09 seconds. This is because in Scenario 8 and Scenario 9, Sybil and duplicate nodes are placed at the edges of the network, that is, at the points where packet exchange is most miniature. This prevents the Sybil attack from significantly impacting the routing protocol. Therefore, end-to-end latency values are lower in Scenario 8 and Scenario 9 compared to scenarios where Sybil and duplicate nodes are placed in the middle.

The end-to-end delay is 0.08 seconds in Scenario 1 and 0.07 seconds in Scenario 2. In scenario 2, Sybil attack is desired to be carried out. However, the 3 duplicate nodes created by the Sybil node cannot affect the routing protocol of the system. For this reason, the end-to-end delay values of Scenario 1 and Scenario 2 are close.

As a result, the most effective Sybil attack was carried out in Scenarios 4 and 7. For this reason, it is seen that the packets transmitted from the source to the destination in Scenario 4 and Scenario 7 are delayed to a large extent. The end-to-end latency in Scenario 6 with 1 Sybil and 3 duplicate nodes placed in the middle of the network is higher than in Scenario 8, with 2 Sybil and 6 duplicate nodes placed at the network's edges, and Scenario 9 with 4 Sybil and 12 duplicate nodes. The location of the Sybil node in the network makes the attack even more effective.

In Figure 18, the normalized routing load values of the scenarios created from the data obtained as a result of the experiments are given.

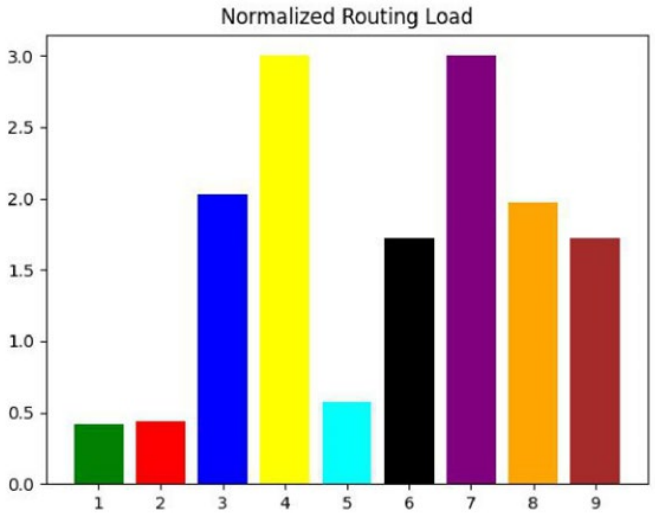

Figure 18. Normalized routing load

Normalized routing payload; 0.42 in Scenario 1, 0.44 in Scenario 2, 2.03 in Scenario 3, 3.0 in Scenario 4, 0.57 in Scenario 5, 1.72 in Scenario 6, 3.0 in Scenario 7, 1.97 in Scenario 8, and Scenario 9, 1.72 was

obtained. The analyzes of why these results came out this way are given below based on a ratio.

In Scenario 4 and Scenario 7, the normalized routing payload is 3.0. In these scenarios, the Sybil attack is most effective. The number of packets received versus routing packets sent is low in these scenarios. As a result, the normalized routing overhead is the highest.

Normalized routing overhead is 2.03 in Scenario 3, 1.72 in Scenario 6, 1.97 in Scenario 8 and 1.72 in Scenario 9. Sybil attack has been tried in these scenarios. In scenario 3, there are 8 duplicate nodes that do not communicate with legitimate ones. In scenario 6, 1 Sybil and 3 duplicate nodes are in the middle of the network. In Scenario 8, 2 Sybil and 6 duplicate nodes are at the edges of the network, while in Scenario 9, 4 Sybil and 12 duplicate nodes are at the edges of the network. Although not the scenarios in which the Sybil attack was most effective, they impacted the system's routing protocol. Due to this, the received packet rates of the routing control packets sent were high.

In scenario 5, it is seen that the normalized forwarding load is 0.57. There is no behavior in scenario 5 that would qualify as an attack.

The normalized routing load is 0.42 in Scenario 1 and 0.44 in Scenario 2. In Scenario 1, no behavior can be qualified as an attack. In scenario 2, there are 3 duplicate nodes. In scenario 2, the Sybil attack was attempted, but the routing protocol of the system could not be fooled. However, it is seen that the control packets sent in Scenario 2, according to Scenario 1 are higher than the received packet rates. Although the Sybil attack was not fully realized, this situation affected the system.

As a result, Sybil attack does not significantly affect the ratio of the routing control packets sent to the received packets. While the normalized routing load is expected to be close to 0 in a non-attack network, it is seen that it increases to 3.0 in the scenarios where the Sybil attack is most effective.

6. Conclusions and Future Works

The usage area of wireless sensor networks is increasing day by day. Various sensor network structures are used in applications such as environment, industry, military, health, security, and advertising (Ceyhan and Sagıroğlu, 2013). Most of the time, wireless sensor networks are vulnerable to external attacks due to the environment in which they are located. There are many types of seizures in wireless sensor networks, such as Sybil, Blackhole, Sinkhole, Wormhole, Selective Forwarding and DoS. Among these attacks, the Sybil attack is potentially the most dangerous for the system's flow. According to all the results obtained, In Scenario 1, where there is no Sybil attack, the packet delivery rate is 100%. In Scenario 2, where there are 3 duplicate nodes, it is seen that the packet delivery rate is 100%. Despite the Sybil attack, the 3 duplicate nodes could not fool the routing mechanism of the system. In scenario 3, when the number of duplicate nodes is 8, it is seen that the packet delivery rate drops to 69%, and the attack affects the routing protocol slightly. In Scenario 4, where the Sybil attack is fully effective, it is seen that the package delivery rate drops to 0%. In Scenario 6 and Scenario 7, Sybil and duplicate nodes are located in the middle of the network. In Scenario 8 and Scenario 9, Sybil and duplicate nodes are situated on the network's edges. In line with the results obtained, 33% and 0% packet delivery were made, respectively, in scenarios where malicious nodes were in the middle of the network. In scenarios where malicious nodes are located at the network's edges, 33% and 34% packet delivery were made, respectively. Positioning the Sybil and duplicate nodes along the route determined by the routing protocol was more effective in reducing the packet delivery rate. As a result of increasing copy nodes for Scenario 1, Scenario 2, Scenario 3 and Scenario 4, it is seen that the efficiency gradually decreases. The efficiency of scenario 2 is 100% because the 3 duplicate nodes in the network do not cheat the routing protocol. In Scenario 5, Scenario 6 and Scenario 7, it is seen that the efficiency decreases with increasing Sybil and copy node. Although there is 1 Sybil and 3 duplicate nodes in scenario 6, positioning it in the middle of the network, that is, in the area where the route will be most used, caused the system's efficiency to decrease. In scenarios where the Sybil attack affects the routing protocol, the source wants to forward the packet over the Sybil node. Since the packet transmitted to the Sybil node does not reach the destination, it causes delays in the system. For this reason, it is seen that the highest delay values in Scenario 4 and Scenario 7, namely 0.20 seconds. In Scenario 1 and Scenario 7, where there is no Sybil attack, it is seen that the end-to-end delay is 0.08 and 0.10 seconds, respectively. In Scenario 4 and Scenario 7, it is seen that the normalized routing load is 3.0. This is because routing control packets are

sent for each package to be transmitted, the route is determined, and the package is shipped. Since these packets arriving at the Sybil node do not reach the destination, the number of packets received is meagre. For this reason, the normalized routing load is very high.

This study it is aimed to describe in detail the Sybil attack, which is missing in the literature, to explain the attack steps, apply it in the NS2 simulation environment, and analyze the adverse effects of the attack initiated by Sybil nodes located in different numbers and different locations on the system. In 9 different scenarios run, Sybil and duplicate nodes were found at various locations and other numbers. In line with all the results obtained, it is seen how dangerous the Sybil attack can be in wireless sensor networks. It can cause the whole system to crash by causing its routing protocol to work incorrectly. For the Sybil attack to have the highest impact on the system, it was seen that the location of the Sybil node and the number of fake identities it created depended on it. Building a sufficient number of duplicate nodes and the presence of these duplicate nodes close to the possible data transmission path maximizes the impact of the Sybil attack.

The Sybil attack in the simulation environment sheds light on future studies. The following research will lay the groundwork for detecting and preventing deception and denial-of-service attacks on wireless sensor networks using artificial intelligence methods such as machine learning and deep learning.

7. References

Almesaeed, R., & Al-Salem, E. (2022). Sybil attack detection scheme based on channel profile and power regulations in wireless sensor networks. Wireless Networks, 28(4), 1361-1374. https://doi.org/10.1007/s11276-021-02871-0

Angappan, A., Saravanabava, T. P., Sakthivel, P., & Vishvaksenan, K. S. (2020). Novel sybil attack detection using rssi and neighbour information to ensure secure communication in wsn. Journal of Ambient Intelligence and Humanized Computing, 12(6), 6567-6578. https://doi.org/10.1007/s12652-020-02276-5

Ardakani, M. M., Tabarzad, M. A., & Shayegan, M. A. (2022). Detecting sybil attacks in vehicular ad hoc networks using fuzzy logic and arithmetic optimization algorithm. Journal of Supercomputing, 78(14), 16303-16335. https://doi.org/10.1007/s11227-022-04526-z

Avila, K., Sanmartin, P., Jabba, D., & Gomez, J. (2021). An analytical survey of attack scenario parameters on the techniques of attack mitigation in wsn. Wireless Personal Communications, 122(4), 3687-3718. https://doi.org/10.1007/s11277-021-09107-6

Biswas, R. N., Mitra, S. K., & Naskar, M. K. (2022). Localization under node capture attacks using fuzzy based anchor mobility control. Journal of Ambient Intelligence and Humanized Computing. https://doi.org/10.1007/s12652-021-03619-6

Ceyhan, E. B. & Sağıroğlu, Ş. (2013). Kablosuz algılayıcı ağlarda güvenlik sorunları ve alınabilecek önlemler. Politeknik Dergisi , 16, (4), 155-163. https://dergipark.org.tr/tr/pub/politeknik/issue/33068/367995

Chen, S., Pang, Z., Wen, H., Yu, K., Zhang, T., & Lu, Y. (2021). Automated labeling and learning for physical layer authentication against clone node and sybil attacks in industrial wireless edge networks. IEEE Transactions on Industrial Informatics, 17(3), 2041-2051. https://doi.org/10.1109/tii.2020.2963962

Ezhilarasi, M., Gnanaprasanambikai, L., Kousalya, A., & Shanmugapriya, M. (2022). A novel implementation of routing attack detection scheme by using fuzzy and feed-forward neural networks. Soft Computing. https://doi.org/10.1007/s00500-022-06915-1

Ibrahim, I. S., King, P. J. B., & Loidl, H. W. (2015). Nsgtfa: A gui tool to easily measure network performance through the ns2 trace file. Journal of Intelligent Systems, 24(4), 467-477. https://doi.org/10.1515/jisys-2014-0153

Jamshidi, M., Esnaashari, M., Darwesh, A. M., & Meybodi, M. R. (2019). Detecting sybil nodes in stationary wireless sensor networks using learning automaton and client puzzles. IET Communications, 13(13), 1988-1997. https://doi.org/10.1049/iet-com.2018.6036

Karakaya, A., & Akleylek, S. (2018). A survey on security threats and authentication approaches in wireless sensor networks. In 2018 6th International Symposium on Digital Forensic and Security (ISDFS) (pp. 1-6). IEEE. https://doi.org/10.1109/ISDFS.2018.8355381

Mehbodniya, A., Webber, J. L., Shabaz, M., Mohafez, H., & Yadav, K. (2021). Machine learning technique to detect sybil attack on iot based sensor network. IETE Journal of Research, 1-9. https://doi.org/10.1080/03772063.2021.2000509

Pushpa, X. S., & Raja, S. K. S. (2022). Enhanced ecc based authentication protocol in wireless sensor network with dos mitigation. Cybernetics and Systems, 53(8), 734-755. https://doi.org/10.1080/01969722.2022.2055403

Sadeghizadeh, M. (2022). A lightweight intrusion detection system based on rssi for sybil attack detection in wireless sensor networks. International Journal of Nonlinear Analysis and Applications, 13(1), 305-320. https://doi.org/10.22075/ijnaa.2022.5491

Shehni, R. A., Faez, K., Eshghi, F., & Kelarestaghi, M. (2018). A new lightweight watchdog-based algorithm for detecting sybil nodes in mobile wsns. Future Internet, 10(1), 1. https://doi.org/10.3390/fi10010001

Shehnaz, T. P., & Nital, H. M. (2017). A review: Sybil attack detection techniques in wsn. In 2017 4th International Conference on Electronics and Communication Systems (ICECS) (pp. 1116-1121). IEEE. https://doi.org/10.1109/ecs.2017.8067865

Singh, S., & Saini, H. S. (2018). Security approaches for data aggregation in wireless sensor networks against sybil attack. In The 2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT) (pp. 656-661). IEEE. https://doi.org/10.1109/icicct.2018.8473091

Vamsi, P. R., & Kant, K. (2014). A lightweight sybil attack detection framework for wireless sensor networks. In 2014 Seventh International Conference on Contemporary Computing (IC3) (pp. 293-298). IEEE. https://doi.org/10.1109/IC3.2014.6897205

Wang, H., Ma, L., & Bai, H. (2020). A three-tier scheme for sybil attack detection in wireless sensor networks. In 2020 5th International Conference on Computer and Communication Systems (ICCCS 2020) (pp. 54-58). IEEE. https://doi.org/10.1109/ICCCS49078.2020.9118478

Wadii, J., Rim, H., & Ridha, B. (2019). Detecting and preventing sybil attacks in wireless sensor networks. In 2019 IEEE 19th Mediterranean Microwave Symposium (MMS) (pp. 1-4). IEEE. https://doi.org/10.1109/MMS48040.2019.9157321

Zhang, J., Sun, J., & Zhang, C. (2022). Stochastic game in linear quadratic gaussian control for wireless networked control systems under dos attacks. IEEE Transactions on Systems Man Cybernetics-Systems, 52(2), 902-910. https://doi.org/10.1109/tsmc.2020.3010515

Zhukabayeva, T. K., Mardenov, E. M., & Abdildaeva, A. A. (2020). Sybil attack detection in wireless sensor networks. In 2020 IEEE 14th International Conference on Application of Information and Communication Technologies (AICT2020) (pp. 1-6). IEEE. https://doi.org/10.1109/AICT50176.2020.9368790