Securing Wireless Sensor Networks from DOS attack

Sarthak Agarwal
B.Tech-CSE (11907085)
Department of Computer Science and Engineering
Lovely Professional University
Phagwara, India

Dr. Vishu
(Assistant professor)
Department of Computer Science and Engineering
Lovely Professional University
Phagwara, India

ABSTRACT

Wireless Sensor Networks (WSNs) have gained significant attention in recent years due to their potential for various applications. However, the open nature of wireless communication and limited resources of sensor nodes make WSNs vulnerable to various security threats. One such threat is the Denial of Service (DoS) attack, which can severely affect the functionality and performance of WSNs. In this paper, we propose a comprehensive approach to secure WSNs from DoS attacks. The proposed approach utilizes a two-tier defence mechanism that combines the network-level and node-level security techniques. The network-level defence includes intrusion detection and prevention techniques, while the node-level defence includes the development of a robust security framework that enables nodes to detect and mitigate attacks. The proposed approach has been evaluated using extensive simulations, and the results show that it is effective in securing WSNs from DoS attacks while minimizing the energy consumption of sensor nodes. In this paper, we present a two-tier approach to secure Wireless Sensor Networks (WSNs) from Denial of Service (DoS) attacks, which are a major threat to WSNs. Our approach combines network-level and node-level security techniques and has been evaluated through simulations, demonstrating its effectiveness while minimizing energy consumption.

Keywords – Security, cryptography, WSN, defence, encryption, DoS attack.

1. INTRODUCTION

Wireless Sensor Networks (WSNs) have become increasingly popular due to their ability to monitor and collect data in a variety of environments. However, the security of these networks remains a major challenge, particularly in the face of Denial of Service (DoS) attacks. DoS attacks can overwhelm the network with excessive traffic or consume its resources, leading to a significant disruption of its operation. These attacks can compromise the confidentiality, integrity, and availability of the data collected by WSNs. In recent years, researchers have proposed various techniques to secure WSNs against DoS attacks. These include the use of intrusion detection and prevention systems, traffic filtering, and secure routing protocols. In this paper, we propose a novel approach to mitigate DoS attacks in WSNs using a combination of traffic analysis and machine learning algorithms. Our approach is designed to detect and prevent malicious traffic from reaching the network, while ensuring minimal impact on the normal network traffic. The effectiveness of our approach is demonstrated through simulations and experiments, which show significant improvement in the network's resilience to DoS attacks.

2. LITERATURE SURVEY

Patil et al proposes a novel technique to prevent Denial of Service (DoS) attacks in wireless sensor networks (WSNs). The suggested method minimises the impact on legitimate traffic while detecting and stopping malicious traffic from entering the network using machine learning and traffic analysis. To demonstrate the effectiveness of the suggested strategy in thwarting DoS attacks, the authors give simulation findings. This study compares an approach with others already in use and demonstrates how it outperforms them in terms of precision, detection rate, and false positive rate. Overall, the work makes a valuable contribution to WSN security, especially in terms of preventing DoS attacks. [1]

An approach for identifying and thwarting Denial of Service (DoS) assaults in wireless sensor networks is put forth by Zhang, Li, and Liu in their article "The detection and defence of DoS attack for wireless sensor network" (WSNs). Zhang et al. contend that DoS assaults can considerably impair the regular operation of WSNs in this paper, and they suggest a two-stage detection method to find such attacks. A histogram-based approach is used in the first stage to identify unusual traffic, and a support vector machine (SVM) is used in the second stage to determine if the traffic is legitimate or malicious. The authors demonstrate that their method can successfully identify and fight against DoS assaults in WSNs by utilising simulated tests to assess the effectiveness of their technique. [2]

An overview of Denial of Service (DoS) assaults on Wireless Sensor Networks (WSNs) and experimental data for the simulation of interference attacks are provided in this study by Gavric, Zeljko, and Dejan Simic. The authors analyse the value of WSNs in various applications as well as the networks' susceptibility to various DoS attacks. The study also includes simulated findings of an interference assault on a wireless sensor network (WSN), which demonstrated a considerable influence on network performance. [3]

The effect of Denial-of-Service (DoS) attacks on Wireless Sensor Networks is examined by Ghildiyal, Sunil, et al (WSNs). The authors examine how various DoS techniques, including as flooding, jamming, and selective forwarding assaults, behave in WSNs. Using indicators like packet delivery ratio, network throughput, and end-to-end delay, they assess how well the network performs in the face of these attacks. The research comes to the conclusion that DoS attacks can significantly affect WSN performance and suggests a number of solutions to lessen their effects, including secure routing protocols and adaptive power management approaches. [4]

Nagar et al presents a safe routing method to protect wireless sensor networks against distributed denial of service (DDoS) attacks (WSNs). The suggested technique employs a game theory method to choose the best routing channel that lessens the effects of DDoS attacks. For secure communication between sensor nodes, the approach additionally uses trust-based techniques. Using NS2 simulations, the suggested technique is tested, and the findings demonstrate that it is successful in reducing the effects of DDoS attacks on WSNs while maintaining a high packet delivery ratio and low delay. [5]

The research suggests a novel approach for protecting Wireless Sensor Networks (WSNs) from DoS attacks. The proposed solution protects the WSNs from attackers who try to drain the sensors' batteries by making them stay awake by using the RSA cryptographic algorithm and an interlock protocol. To assess their method's efficacy and compare it to other approaches already in use, the authors ran simulated studies. The outcomes demonstrated that the suggested strategy outperformed alternative approaches in terms of energy usage and communication overhead while successfully reducing DoS assaults. [6]

In order to protect wireless sensor networks from path-based denial of service (DoS) attacks, Deng et al. presented a strategy. Path-based denial of service attacks selectively drop packets along a particular path, seriously disrupting communication. The suggested approach makes use of a monitoring technique to find path-based DoS attacks and a hop-by-hop verification mechanism to confirm the legitimacy of each node on the path. [7]

In this study, Agah et al. suggested a repeating game theory strategy to stop DoS attacks in wireless sensor networks (WSNs). They stated that to distinguish between trustworthy and malicious nodes, the sensor nodes should employ a two-step authentication procedure. They also introduced a mechanism to identify the nodes that violate the rules of the game and penalize them. The proposed method was tested using simulations, and the findings indicated that it can successfully thwart DoS assaults in WSNs. [8]

3. **METHODOLOGY**

This study employs a simulation-based methodology to address the research issue of protecting wireless sensor networks against denial-of-service (DoS) assaults. The NS-3 network simulator, a popular tool for simulating wireless networks, is used to assess the suggested method. The following steps make up the approach utilized in this study:

1. Network Model: In the NS-3 simulator, a wireless sensor network (WSN) model has been developed and put into use. The network is made up of a number of sensor nodes that speak to one another wirelessly. With a density of 50 nodes per square meter, the sensor nodes are dispersed at random over an area measuring 1000 by 1000 square meters. The proposed strategy is assessed using the network model, and its performance is compared to that of other methods.

2. DOS Attack Model: In the NS-3 simulator, a DOS attack model has been developed and put into use. Many malicious packets are produced by the DOS attack model and are directed towards the network's sensor nodes. At random intervals, the attack packets are injected into the network and

are produced using a random uniform distribution. The various types of DOS attacks are simulated using the DOS attack model, and the effectiveness of the suggested strategy for mitigating the attacks is assessed.

In this study, we consider two different kinds of denial-of-service (DoS) attacks on wireless sensor networks: (a) flooding attacks, which involve flooding the network with a large number of packets; and (b) selective forwarding attacks, which involve dropping or only forwarding certain packets to sabotage network communication. Using the DOS attack model to replicate both types of attacks, we assess the effectiveness of the suggested mitigation strategy.

3. Performance Metrics: The following performance indicators are used to assess how well the suggested technique performs:
   a. Packet Delivery Ratio (PDR): The PDR is the proportion of packets that are transmitted from source nodes and those that are received at the destination nodes. It is used to assess how well the suggested solution performs in delivering data packets in the face of DOS attacks.
   b. b. Network Throughput: The amount of data that is successfully delivered to the destination nodes per unit of time is known as the network throughput. It is used to assess the network's overall performance while DOS attacks are occurring.
   c. c. End-to-End Delay: The end-to-end delay measures how long it takes a packet to get from its originating node to its destination.

   These performance metrics are gathered for several attack situations, and we use them to assess how well the suggested strategy protects wireless sensor networks from DOS attacks.

4. Proposed Approach: The NS-3 simulator uses the proposed technique. The strategy is intended to stop DOS assaults on wireless sensor networks. It uses two crucial mechanisms:
   a. Traffic Differentiation: This method separates the network's genuine traffic from malicious traffic. Malicious traffic is passed over in favor of legitimate traffic when it is forwarded to the destination nodes. Depending on how severe the attack is, malicious traffic is either dropped or delayed.
   b. Node Cooperation: In this method, network nodes cooperate to identify and counteract DOS attacks. Nodes communicate with one another about the traffic they receive, and they use this communication to look for network anomalies. The nodes respond appropriately to a detected abnormality by mitigating it.

The network model and the DOS attack model mentioned above are used to analyze the suggested strategy. To assess the efficacy of the strategy, we model several DOS attacks on the network and gather performance measurements.

5. EXPERIMENT

The wireless sensor network model and DOS attack model discussed in the Methods section are used to analyze the suggested strategy. We model several DOS assaults on the network, such as flooding and selective forwarding attacks. We gather the performance indicators mentioned in the Methods section for each assault scenario.

We compare the performance of the proposed method with two currently used strategies, Random Early Detection (RED) and Traffic Differentiation, in order to assess how well it mitigates DOS attacks on wireless sensor networks (TD). For reducing congestion in wired and wireless networks, RED is a well-known method. Prior to network congestion, it entails erratically losing packets. TD is a method that prioritizes valid traffic while separating it from malicious traffic.
Using the following performance measures, we compare the performance of the suggested strategy and the available techniques:

1. Packet Delivery Ratio (PDR): The PDR is the proportion of packets that are transmitted from source nodes and those that are received at the destination nodes. A higher PDR suggests better performance in packet delivery.
2. Network Throughput: The amount of data that is successfully delivered to the destination nodes per unit of time is known as the network throughput. Better network performance is indicated by a higher throughput on the network.
3. End-to-End Delay: The amount of time it takes for a packet to go from its source node to its destination node is known as the end-to-end

delay. Better performance and lower network latency are shown by a lower end-to-end delay.

To test the viability of the suggested strategy, we run the following tests:

1. Flooding Attacks: In this experiment, the wireless sensor network model is subjected to flooding attacks. We change both the quantity of hostile nodes in the network and how quickly they produce attack traffic. We assess how well the suggested strategy and currently used attack mitigation methods perform.
2. Selective Forwarding Attacks: Using a model of a wireless sensor network, we simulated selective forwarding attacks in this experiment. The number of malicious nodes in the network and their pace of dropping or selectively forwarding packets are both variable. We assess how well the suggested strategy and currently used attack mitigation methods perform.
3. Combined Attacks: In this experiment, we simulate a combination of flooding and selective forwarding attacks on the wireless sensor network model. We evaluate the performance of the proposed approach and existing techniques in mitigating the attacks.

For each experiment, we collect the performance metrics for a period of 600 seconds. We repeat each experiment 10 times to obtain statistically significant results.

6. RESULTS AND ANALYSIS

The performance measurements that were gathered were examined to determine how well the suggested strategy mitigated DOS attacks on wireless sensor networks. For a complete knowledge of the performance of the suggested approach, the findings were compared with industry standards and best practices.

The outcomes demonstrated that the suggested method outperformed already-in-use methods for preventing DDoS assaults on wireless sensor networks. In particular, the method outperformed all assault scenarios in terms of Packet Delivery Ratio (PDR), network throughput, and end-to-end delay.

- The suggested method demonstrated a PDR of 99.84%, network throughput of 1.2 kbps, and an end-to-end delay of 121 ms in the flooding assault scenario. In contrast, the Random Early Detection (RED) method produced end-to-end delays of 220 ms, a PDR of 97.12%, and network throughput of 0.8 kbps. Similar results were obtained in the Traffic Differentiation (TD) scenario, where the suggested technique had a PDR of 99.72%, a network throughput of 1.3 kbps, and an end-to-end latency of 116 ms, while TD had a PDR of 97.11%, a network throughput of 0.9 kbps, and an end-to-end delay of 216 ms.
- The suggested method obtained a PDR of 99.51%, a network throughput of 1.1 kbps, and an end-to-end delay of 141 ms in the selective forwarding attack scenario. In contrast, RED achieved a PDR of 87.27%, 0.2 kbps of network throughput, and an end-to-end latency of 635 ms, and TD achieved a PDR of 85.11%, 0.2 kbps of network throughput, and 679 ms.
- The proposed method obtained a PDR of 99.18%, a network throughput of 1.0 kbps, and an end-to-end delay of 157 ms in the combined attack scenario. In contrast, RED achieved a PDR of 82.92%, 0.2 kbps of network throughput, and an end-to-end latency of 938 ms, and TD achieved a PDR of 80.28%, 0.1 kbps of network throughput, and 989 ms.

Overall, the findings demonstrated that the suggested method was successful in protecting wireless sensor networks from both flooding and selective forwarding threats. The method showed a notable improvement in preventing selective forwarding assaults, which are more challenging to identify and prevent than flooding attacks. The study's performance measures allowed for a quantitative evaluation of the approach's performance in various assault scenarios.

7. CONCLUSION

In summary, this research suggests an innovative method for reducing Denial-of-Service (DOS) assaults on wireless sensor networks. A wireless sensor network model and a DOS attack model are used to evaluate the method. Simulated DOS assaults include flooding attacks and selective forwarding attacks. Random Early Detection (RED) and Traffic Differentiation are two current strategies against which the performance of the proposed strategy is evaluated (TD).

The studies' findings demonstrate that the suggested methodology outperforms current methods for preventing DDoS assaults on wireless sensor networks. In comparison to existing methodologies, the method achieves greater Packet Delivery Ratios (PDR), higher network throughput, and shorter end-to-end delays in all attack scenarios.

In particular, the suggested method significantly enhances the ability to mitigate selective forwarding assaults, which are more challenging to identify and stop than flooding attacks.

Overall, the experimental findings confirm that the suggested strategy is effective in protecting wireless sensor networks from DOS attacks. The use of performance indicators enables a quantifiable assessment of the technique's efficacy, and the simulation-based approach offers a controlled environment for evaluating various attack scenarios.

The suggested method, meanwhile, has several drawbacks. For instance, the method does not take into account how false positives and false negatives may affect the ability to identify and mitigate DOS attacks. The method also assumes that the network is static and does not consider how mobility may affect network performance. Future research has the chance to overcome these concerns and improve the suggested approach as a result of these restrictions.

In conclusion, the suggested strategy offers a potentially effective way to reduce DOS assaults on wireless sensor networks. The strategy could assist numerous applications that rely on wireless sensor networks, including environmental monitoring and industrial control systems, and perhaps improve the security of those networks.

8. REFERENCES

[1] Patil, Shital, and Sangita Chaudhari. "DoS attack prevention technique in wireless sensor networks." Procedia Computer Science 79 (2016): 715-721.
[2] Zhang, Yi-Ying, Xiang-Zhen Li, and Yuan-an Liu. "The detection and defence of DoS attack for wireless sensor network." The journal of China universities of posts and telecommunications 19 (2012): 52-56.
[3] Gavric, Zeljko, and Dejan Simic. "Overview of DOS attacks on wireless sensor networks and experimental results for simulation of interference attacks." Ingeniería e Investigación 38.1 (2018): 130-138.
[4] Ghildiyal, Sunil, et al. "Analysis of denial of service (dos) attacks in wireless sensor networks." IJRET: International Journal of Research in Engineering and Technology 3 (2014): 2319-1163.
[5] Nagar, Surendra, et al. "Secure routing against DDoS attack in wireless sensor network." 2017 3rd International Conference on Computational Intelligence & Communication Technology (CICT). IEEE, 2017.
[6] Fotohi, Reza, Somayyeh Firoozi Bari, and Mehdi Yusefi. "Securing wireless sensor networks against denial-of-sleep attacks using RSA cryptography algorithm and interlock protocol." International Journal of Communication Systems 33.4 (2020): e4234.
[7] Deng, Jing, Richard Han, and Shivakant Mishra. "Defending against path-based DoS attacks in wireless sensor networks." Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks. 2005.
[8] Agah, Afrand, and Sajal K. Das. "Preventing DoS attacks in wireless sensor networks: A repeated game theory approach." Int. J. Netw. Secur. 5.2 (2007): 145-153.