Communications on Applied Nonlinear Analysis
ISSN: 1074-133X
Vol 31 No. 2s (2024)

Impact of RREQ Packet Flooding Attack on Wireless Sensor Networks: A Simulation-Based Study

Vivek Sharma[1], Dr. Devershi Pallavi Bhatt[*2]

[1] Manipal University Jaipur, Rajasthan-303007, India

[*2] Manipal University Jaipur, Rajasthan-303007, India

Article History:

Received: *20-03-2024*

Revised: *14-05-2024*

Accepted: *26-05-2024*

Abstract: This paper analyzes the impact of RREQ packet flooding on WSNs through simulations. WSNs are vital for applications like surveillance, healthcare, and environmental monitoring. However, they are susceptible to DoS attacks, such as RREQ packet flooding, which disrupts normal operations by overwhelming the network with excessive route requests. The study evaluates the effect of RREQ flooding on WSN performance metrics, including throughput, end-to-end delay, packet delivery ratio, energy consumption, and routing load. It also reviews relevant literature to provide background information and identify gaps in current knowledge.

Introduction: WSNs consist of distributed sensor nodes that collect and transmit data to a central base station for processing. WSNs face significant challenges, including malicious activities like DoS attacks, which aim to disrupt normal operations. RREQ packet flooding is a severe form of DoS attack that overwhelms the network with excessive Route REQuest packets, leading to communication channel saturation and congestion, thus hindering legitimate data transmission and compromising network performance.

Objectives: The objective of this paper is to conduct an in-depth analysis of the effects of RREQ packet flooding on various performance metrics of WSNs through extensive simulations. The study aims to understand the repercussions of this attack on throughput, end-to-end delay, packet delivery ratio, energy consumption, and routing load. Additionally, the paper seeks to identify existing gaps in the understanding of the impact of RREQ packet flooding and provide insights that can inform the development of effective countermeasures to safeguard WSNs.

Methods: The paper employs simulation-based methods to assess the impact of RREQ packet flooding on WSN performance. Various performance metrics such as throughput, end-to-end delay, packet delivery ratio, energy consumption, and routing load are evaluated. A thorough literature review is also conducted to contextualize the analysis and identify knowledge gaps. The simulations are designed to mimic real-world scenarios to provide accurate and relevant results.

Results: The simulations reveal that RREQ packet flooding significantly affects WSN performance. Key findings include a decrease in throughput, an increase in end-to-end delay, a reduction in packet delivery ratio, higher energy consumption, and increased routing load. These results highlight the detrimental impact of RREQ packet flooding on the overall functionality and efficiency of WSNs.

Conclusions: The paper concludes that RREQ packet flooding poses a substantial threat to the performance of WSNs. The findings underscore the importance of developing robust defense mechanisms to protect WSNs from such attacks. The insights gained from this study can inform the creation of more resilient and reliable WSNs, capable of withstanding RREQ packet flooding and similar threats.

Keywords: *WSN, RREQ Flooding attack, Routing, Network performance, Energy, Security.*

1. Abstract

This paper provides a thorough analysis using simulation to examine how RREQ (Route REQuest) packet flooding affects Wireless Sensor Networks (WSNs). WSNs are critical to many applications, including as surveillance, healthcare, and environmental monitoring. However, certain factors, including as network protocols and threats, can have a major impact on their performance. A sort of Denial of Service (DoS) attack known as "RREQ packet flooding" can cause excessive route request packet flooding, which interferes with WSNs' ability to function normally. This study assesses impact of the flooding of RREQ packets on WSN performance measures, including, Throughput, end-to-end delay, packet delivery ratio, energy consumption, and routing load using a number of simulations. The article also evaluates relevant literature to give background information and point out any current gaps in the field's knowledge.

2. Introduction

Wireless Sensor Networks (WSNs) have become integral in facilitating a diverse array of applications, spanning from environmental monitoring to healthcare and surveillance. These networks comprise distributed sensor nodes that collaborate in the collection and transmission of data to a central base station for further processing. Despite their wide-ranging utility, WSNs face numerous challenges that can significantly increase their overhead.

One prominent challenge arises from malicious activities in the form of denial-of-service (DoS) attacks, which seek to disrupt the normal operations of WSNs. Among the various forms of DoS attacks, "RREQ packet flooding" emerges as a particularly pernicious threat. This type of attack involves adversaries inundating the network with an excessive volume of Route REQuest (RREQ) packets, resulting in the saturation of communication channels and subsequent congestion. Consequently, legitimate data transmission becomes hindered, thereby compromising the performance of the network and potentially jeopardizing critical applications reliant on WSNs.

A comprehensive understanding of the repercussions of RREQ packet flooding on WSNs is imperative for the development of robust defense mechanisms aimed at fortifying the reliability and resilience of these networks. In this paper, we present an in-depth analysis of the effects of RREQ packet flooding on various performance metrics inherent to WSNs. Through extensive simulations, we explore how this form of attack influences pivotal parameters such as Throughput, end-to-end delay, packet delivery ratio, energy consumption, and routing load.

Furthermore, we conducted a thorough review of relevant literature to contextualize our analysis and identify existing gaps in understanding regarding the impact of RREQ packet flooding on WSNs. By synthesizing insights gleaned from prior research and our own simulation-based study, our objective is to contribute to a deeper comprehension of the vulnerabilities posed by RREQ packet flooding. Additionally, we endeavor to provide insights that can inform the development of effective countermeasures aimed at safeguarding WSNs against this formidable threat.

In essence, this paper underscores the critical imperative of addressing the security challenges posed by RREQ packet flooding in WSNs. By doing so, we aim to equip researchers and practitioners with valuable insights to bolster the resilience of these networks amidst the ever-evolving landscape of security threats.

3. Literature Review

We have reviewed some papers showing effects of RREQ packet flooding on WSNs that tackle related problems.
Y. Kim et al. (2009) [1] investigated how to improve the Ad hoc On-Demand Distance Vector (AODV) routing protocol specifically for IEEE 802.11 and IEEE 802.15.4 wireless communication standards. To meet the requirements of these standards, the study probably proposes adjustments or optimizations to the AODV protocol, for enhancing network performance metrics including routing efficiency, packet delivery ratio, and energy usage. A comparison of the suggested improvements with the AODV protocol was included in the paper to show how these enhancements improve the wireless networking scenarios.

Yu Y. et al. (2012) [2] examined wireless sensor network (WSN) trust methods. It provided an in-depth analysis of vulnerabilities in security and attacks on WSN trust mechanisms, including malicious routing, false data injection, and node spoofing. To fight these attacks and improve the formation and maintenance of trust in WSNs, the study provided a number of mitigation techniques and countermeasures. These countermeasures, which are intended to guarantee the dependability and integrity of data transmission and node cooperation within the network, included cryptography techniques, trust-based systems, and anomaly detection approaches.

Fatema and Brad (2014) [3] examined a variety of attacks against wireless sensor networks (WSNs) and potential security mechanisms against them. The paper provides an overview of common security concerns that wireless sensor networks (WSNs) encounter, such as jamming, eavesdropping, denial of service (DoS), and node compromise. In order to protect network availability, data integrity, and confidentiality, this study also offered security techniques and strategies to strengthen WSNs' protection against these types of attacks.

Ayaz Hassan Moon et al. (2016) [4] investigated the impact of RREQ (Route REQuest) flooding attacks Using simulation-based study on WSNs. This study analyzed that how these attacks affect important performance indicators including energy usage, packet delivery ratio, network lifetime, and end-to-end latency. It also reveals a notable reduction in network performance under attack conditions. To mitigate impact of such attacks on wireless sensor networks (WSNs), the study emphasized the need for strong security measures and intrusion detection approaches.

A simulation-based investigation was carried out by Wang et al. (2017) [5] to assess how different routing attacks, such as RREQ packet flooding, affect WSN performance. Their findings showed that, in the event of an attack, the packet delivery ratio and network performance significantly declined. On the other hand, key performance parameters like energy usage and network longevity were not thoroughly analyzed in the study.

Mohammad J. F. et al (2017) [6] analyzed RREQ (Route REQuest) flooding attacks and proposed how to improve security in vehicular ad hoc networks (VANETs). The authors provided an approach to improve security that makes use of the balance index. They probably contend that VANETs can identify and counteract RREQ flooding attacks by utilizing the balance index, which improves the networks' overall security posture. The efficacy and efficiency of the authors' suggested technique in preventing such assaults and guaranteeing the dependable and secure operation of VANETs is probably the main focus of their assertions.

Ewa N.S. et al. [7] proposed a Secure Low Energy AODV (Ad hoc On-Demand Distance Vector) Protocol designed specifically for Wireless Sensor Networks (WSNs). The protocol attempts to minimize energy usage in WSNs and improve security. Through the use of AODV's on-demand route formation and maintenance, the protocol ensures effective resource management. It also has security methods that protect against different kinds of threats, which makes it useful in WSN applications where security and energy efficiency are extremely important.

Akourmis Sana et al. (2018) [8] analyzed the vulnerability of the AODV (Ad hoc On-Demand Distance Vector) routing system in Wireless Sensor Networks (WSNs) in presence of the flooding attacks. The paper examines how flooding attacks affect the AODV protocol, network performance indicators like packet delivery ratio, end-to-end latency, and energy usage. It also suggested mitigation or countermeasure techniques to strengthen the security of AODV-based WSNs against flooding attacks.

Y. Zhang et al. (2019) [9] explores the evaluation and comparison of N-hop anchor-based localization techniques in wireless sensor networks (WSNs). The study looks at many localization methods based on N-hop anchors, which include estimating the locations of other nodes in the network by using a subset of nodes known as anchors. The authors carefully compare and contrast different algorithms, assessing how well they work in terms of accuracy, efficiency, and energy usage. By analyzing localization accuracy and computational complexity in detail, the research seeks to provide useful guidance for choosing the best method for various WSN scenarios. This study presents localization approaches in WSNs, which will help to establish reliable and efficient sensor networks in a variety of fields, including industrial automation, healthcare, and environmental monitoring.

Lakshmi S. Anand et al. (2019) [10] analyzed the potential risks of flooding attacks on wireless sensor networks (WSNs) and suggested countermeasures. They also examined the features and effects of flooding attacks on WSNs as well as several approaches to prevention. By reducing the risks associated with flooding assaults, their research proposes to improve the security of WSNs and improve reliability and effectiveness in environmental monitoring and other applications.

Ngoc T. Luong et al. (2019) [11] addressed the challenge of RREQ packet flooding attacks in MANETs. According to this paper existing detection algorithms use thresholds based on RREQ rates, and these algorithms suffer from high rate of false or wrong detections as well as reduced network performance due o it. To mitigate these issues, this paper proposed a novel approach called FADA based on machine learning. FADA leverages the route discovery history of nodes to identify malicious behavior, improving detection accuracy. Furthermore, the paper introduces FAPRP, as an extension of the AODV protocol by integrating FADA with it. The performance of this approach is calculated through simulations in NS2 with and without RREQ attack scenarios. Results indicated that FAPRP detects more than 99% of flooding RREQ using route discovery frequency vectors which become larger than 35. Moreover, it demonstrates reduced routing load and improved packet delivery ratio when compared to existing solutions, highlighting its effectiveness in enhancing network security and performance.

Here's a table for the comparative study of the literature surveys we provided in this paper. This Table-1 provides a structured overview of the main focus, key findings, proposed solutions/techniques, and evaluation methodologies of each literature survey.

Table 1: Comparative study of the literature surveys

Literature with Y.O.P.	**Main Focus**	**Key Findings**	**Proposed Solutions/Techniques**	**Evaluation Methodology**
Y. Kim et al. (2009) [1]	Improving AODV routing protocol for WSNs	Adjustments to AODV for IEEE 802.11 and IEEE 802.15.4 standards. Enhancements improve routing efficiency, packet delivery ratio, and energy usage.	Optimization of AODV protocol for specific wireless standards.	Comparison with original AODV protocol.
Yu Y. et al. (2012) [2]	WSN trust methods and vulnerabilities	Analysis of WSN trust vulnerabilities and attacks. Provided mitigation techniques including cryptography, trust-based systems, and anomaly detection.	Cryptography, trust-based systems, anomaly detection.	Analytical review of vulnerabilities and proposed solutions.
Fatema and Brad (2014) [3]	Security mechanisms for WSNs	Overview of WSN security concerns and attacks. Provided security techniques to protect against jamming, eavesdropping, DoS, and node compromise.	Various security techniques and strategies.	Analytical review of security concerns and proposed solutions.
Ayaz Hassan Moon et al. (2016) [4]	Effect of RREQ flooding attacks on WSNs	Analysis of flooding of RREQ packets, impact on WSN performance. Emphasized need for strong security measures and intrusion detection approaches.	Mitigation measures, intrusion detection.	Simulation-based study on WSNs.
Wang et al. (2017) [5]	Effects of routing attacks on WSN performance	Decline in packet delivery ratio and network performance during attacks. Energy usage and network longevity not thoroughly analyzed.	Focus on packet delivery ratio and network performance during attacks.	Simulation-based investigation.
Mohammad J. F. et al (2017) [6]	Security improvement in VANETs	Proposal to improve VANET security against RREQ flooding attacks using balance index. Emphasis on efficacy and efficiency of suggested technique.	Utilization of balance index for security improvement in VANETs.	Analytical review of VANET security and proposed improvement.
Ewa N.S. et al. (2017) [7]	Secure Low Energy AODV Protocol for WSNs	Development of a secure and energy-efficient AODV protocol for WSNs. Focus on resource management and security against threats.	Secure AODV protocol for WSNs emphasizing energy efficiency and security.	Development and analysis of proposed protocol.
Akourmis Sana et al. (2018) [8]	Vulnerability of AODV in WSNs due to flooding	Examination of AODV vulnerability to flooding attacks. Suggested mitigation techniques to strengthen security against flooding attacks.	Countermeasure techniques against AODV vulnerability to flooding.	Analysis of AODV vulnerability and suggested countermeasures.
Y. Zhang et al. (2019) [9]	Comparison of localization algorithms based on N-hop anchors	Performance Comparison of Localization Algorithm Based on the N-hop Anchors for Wireless Sensor Networks	Utilization of N-hop anchors in localization algorithms	Experimental evaluation through simulations
Lakshmi S. Anand et al. (2019) [10]	Risks of flooding attacks on WSNs	Analysis of flooding attacks' risks on WSNs. Suggested countermeasures for	Countermeasures to reduce risks associated	Analytical review of flooding attacks and

Literature with Y.O.P.	Main Focus	Key Findings	Proposed Solutions/Techniques	Evaluation Methodology
		improving security and reliability in WSN applications.	with flooding attacks on WSNs.	proposed countermeasures.
Ngoc T. Luong et al. (2019) [11]	Detection and prevention of RREQ flooding	Proposal of FADA for detection and FAPRP for prevention of RREQ flooding attacks in MANETs. Improved detection accuracy and performance evaluation through simulations.	FADA for detection, FAPRP for prevention of RREQ flooding attacks in MANETs.	NS2 simulations evaluating FAPRP performance under normal and attack scenarios.

4. Methods

We performed simulation-based studies to look at the effects of RREQ packet flooding on WSNs using the NS-2 network simulator, which is a popular, adaptable and expandable framework for simulating and assessing a range of networking scenarios. In order to simulate real-world WSN deployment scenarios, we set up characteristics including attack strength, traffic patterns, and network topology in our simulation tests.

4.1 Experimental Setup

We analyze a normal wireless sensor network (WSN) configuration, comprising one sink node (base station) and one hundred sensor nodes distributed in an arbitrary topology. Sensor nodes are outfitted with transceivers that use the AODV routing protocol to operate over a shared communication channel. To investigate their effects on network performance under both normal and attack scenarios, we change the number of sensor nodes, transmission range, packet size, and traffic load. We construct an adversary node that can generate and broadcast a large number of route request packets in an indiscriminate manner in order to carry out the RREQ packet flooding attack.

The intensity of the attack can be managed by modifying variables like the rate and duration of packet generation. We evaluated the impact of the attack using various key performance metrics including throughput, *end-to-end delay, packet delivery ratio, energy consumption, and routing load*. The above metrics are explained in detail here:

Throughput: It represents the rate of data packets successfully reached to destination nodes from source nodes within the network. It is measured in bits per second (bps) or packets per second (pps). Formula for calculating the throughput in a WSN can be expressed as:

$$Throughput \;= \frac{Amount\ of\ data\ successfully\ delivered}{Total\ time\ taken\ for\ delivery}$$

Packet Delivery Ratio: It represents the ratio of the successfully delivered data packets to the total number of data packets transmitted by the source nodes within the network. It is typically expressed as a percentage.

$$Packet\ Delivery\ Ratio\ (PDR) = \frac{Number\ of\ Successfully\ Delivered\ Packets}{Total\ Number\ of\ Packets\ Sent} \text{ x } 100\ \%$$

End-to-end delay(ETE delay): It is referred as the time taken by a packet to travel from source to destination node, encompassing all the intermediate hops and processing delays along the route. It represents the total latency experienced by a packet during transmission through the network.

$$Average\ End - to - End\ Delay = \frac{\sum_{k=0}^{n} ETEk}{M}$$

Where, ETE_k = Time of packet reception at destination for packet k - Time of packet transmission from source for packet k and M is number of data packets travelled in network.

Average residual energy: It represents the average amount of energy remaining across all sensor nodes in the network at a given point in time. It provides insight into the overall energy status of the network and helps in assessing the network's health and longevity.

$$Average\ Residual\ Energy = \frac{\sum_{i=0}^{n} Ei}{N}$$

Where, E_i represents the residual energy of each sensor node I and N represents the total number of sensor nodes in the network.

Table 2: Simulation parameters for wireless sensor network.

Parameter	Values
Network interface type	PHY/Wireless PHY
MAC type	IEEE 802.11
Propagation model	Two ray ground radio model
Environment size	1000 m * 1000 m
Number of nodes	100
Initial Energy	10 J
Transmission Power	0.01 J
Receive Power	0.005 J
Sleep Power	0.00001 J/s
Idle Power	0.0001 J/s
Transmission range	250 m
Queuing policy	Queue/DropTail/PriQueue
Queue size	50 Packets
Antenna Type	Antenna/OmniAntenna
Mobility	OFF
Routing protocol	AODV
MAC Type	Mac/802_11
Simulation time	100 s
Packet size	512 Bytes

5. Results and Discussion

Our simulation results indicate that RREQ packet flooding has a major effect on WSN performance indicators. We see a sharp decline in the packet delivery ratio during an attack because of higher packet loss and network congestion. Due to the attack traffic, packets encounter lengthier queue times and routing delays, which significantly increase the end-to-end delay. In addition, the network lifetime decreases drastically since the handling of attacking packets consumes sensor nodes' battery life more quickly. This worsens the attack's impacts by causing early node failure and network fragmentation. Furthermore, the increased energy usage due to managing attack traffic accelerates battery draining and lowers network efficiency in particular.

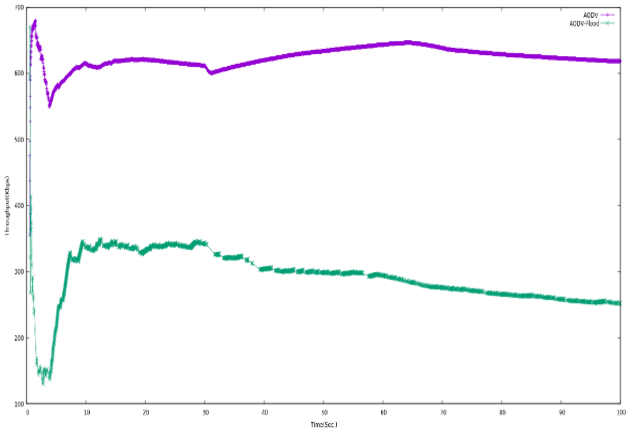

Figure 1.a: Throughput w.r.t. Time

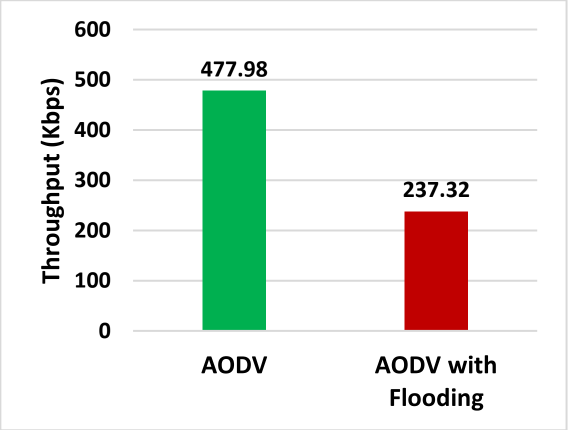

Figure 1.b: Throughput

Figure 1.a illustrates the throughput values over the simulation duration. The diagram clearly indicates that throughout the simulation period, the throughput of AODV with flooding is lower than that of AODV without flooding. In AODV without flooding, the throughput initially remains slightly lower due to path establishment and routing activity, but it increases after route is established. As time progresses, additional routing activities may temporarily decrease throughput. However, in AODV with flooding, the presence of malicious flooding nodes results in a higher number of RREQ packets and significantly increased overhead load, leading to a severe impact on throughput. Once route is established and packet delivery begins, throughput improves. However, with increasing traffic, throughput may decrease again depending on the traffic load and the occurrence of RREQ flooding.

Figure 1.b represents the rate of packets successfully transmitted from source to the destination node or sink node within the network. The first bar indicates a throughput of 477.98 units (which could be bits per second, packets per second, etc.), while the second bar indicates a lower throughput of 237.32 units. A higher throughput generally indicates better network performance in terms of data delivery.

Figure 2 represents the ratio of successfully delivered data packets to the total data packets sent by the source nodes. The first bar shows a high PDR of 97.96%, indicating that nearly all packets sent were successfully delivered. The second bar has a PDR of 93.35%, indicating lower than the first scenario.

Figure 3 represents the average time taken for a data packet to travel from the source node to the destination node, considering all intermediate hops and processing delays along the route. The first bar shows an ETE delay of 22.621 units (which could be in milliseconds, seconds, etc.), while the second bar indicates a higher ETE delay of 40.8649 units. A lower ETE delay indicates faster data transmission and is desirable for real-time applications.

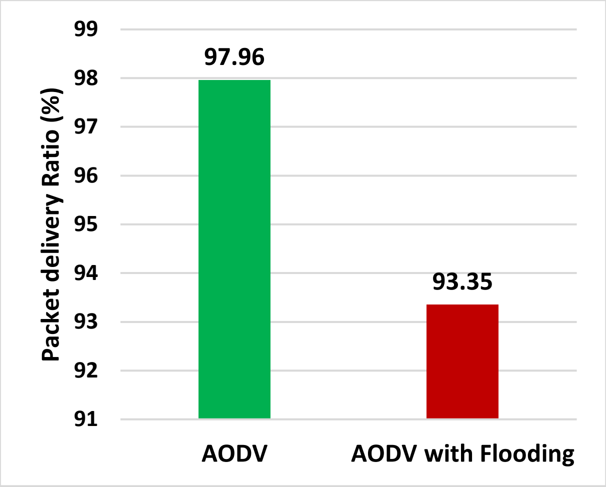

Figure 2: Packet Delivery Ratio

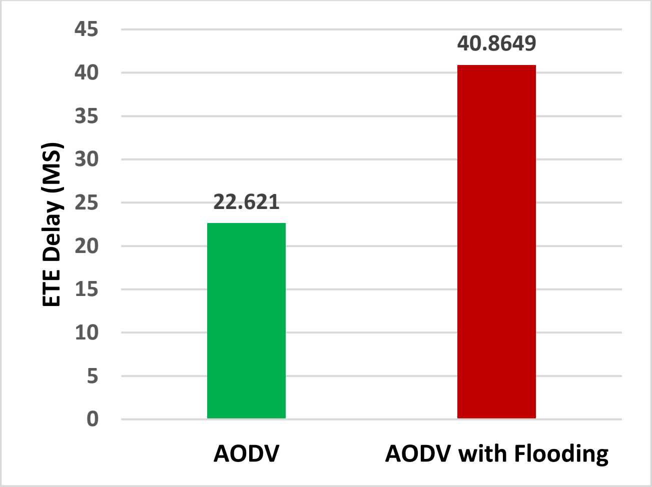

Figure 3: Average End-to-End Delay

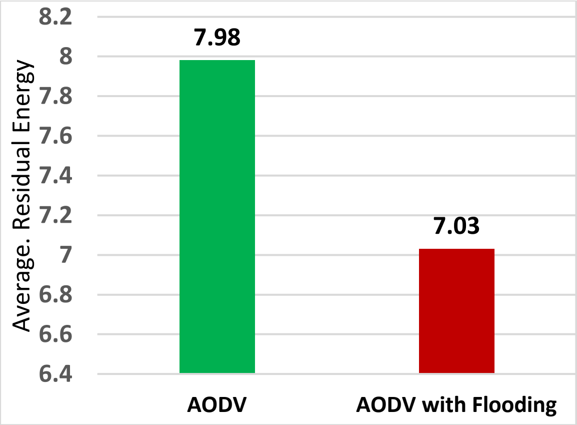

Figure 4: Average Residual Energy

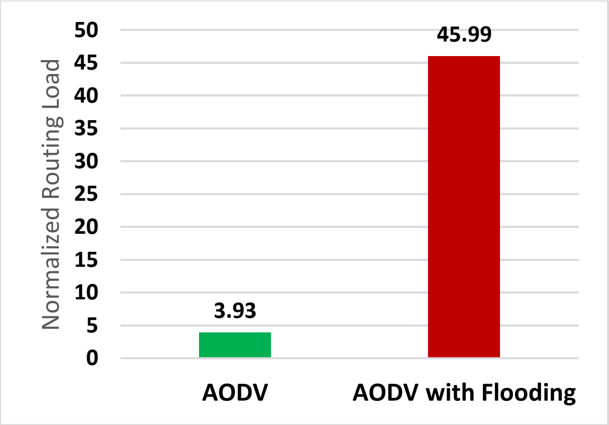

Figure 5: Normalized Routing Load

Figure 4 represents the average residual energy in the network after the simulation or experiment. The first bar shows average 7.98 units of energy is remaining in the network, while the second bar indicates that lower energy is remaining in the network which is 7.03 units. Lower residual energy in the network is considered as reduced network lifetime and increased overhead costs.

Figure 5 represents the metric of normalized routing overhead incurred by the network. It could include factors such as control message exchange, routing table maintenance, and signalling overhead. The first row shows a normalized routing load of 3.93, while the second row indicates a much higher routing load of 45.99. Lower routing loads are preferred as they reduce network overhead and improve efficiency.

6. Conclusion

In present study, we reviewed the effects of RREQ packet flooding attacks on Wireless Sensor Networks (WSNs) in various domains such as surveillance, healthcare, and environmental monitoring; however, they are inclined to security breaches, denial-of-service (DoS) attacks like RREQ packet flooding. Through literature review, we have identified numerous studies investigating the effects of RREQ flooding attacks on WSNs, along with a multitude of mitigation techniques proposed by different researchers. These studies emphasize the sever degradation in WSN performance metrics, including throughput, end-to-end delay, packet delivery ratio, energy consumption, and routing load during such attacks. To further explain the impact of RREQ flooding attacks, we conducted simulation-based analysis using the NS-2 network simulator. Our experiments showed a considerable decline in WSN performance under attack scenarios, decrease in packet delivery ratio, increased packet loss and network congestion, with significant increase in end-to-end delay causing longer routing delays. Furthermore, the network lifetime declined due to overheads of handling of attacking packets battery consumption is accelerated and caused early node failure. Based on results, we emphasize the importance of developing robust security mechanisms to counter the risks caused by RREQ flooding attacks and maintain the reliability and efficiency of WSNs. Future research may be exploring approaches for intrusion detection and prevention, as well as assessing the efficacy of novel routing protocols in mitigating the impact of such attacks. In conclusion, strengthening the security of WSNs against RREQ flooding attacks is necessary to ensure their effectiveness across miscellaneous application domains.

Refrences

[1] Yu-Doo, Kim & Il-Young, Moon & Sung-Joon, Cho. (2009). A comparison of improved AODV routing protocol based on ieee 802.11 and IEEE 802.15.4. Journal of Engineering Science and Technology. 4.

[2] Yanli Yu, Keqiu Li, Wanlei Zhou, Ping Li, “Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures”, Journal of Network and Computer Applications, Volume 35, Issue 3, 2012, Pages 867-880, ISSN 1084-8045, https://doi.org/10.1016/j.jnca.2011.03.005.

[3] Fatema, Nusrat and Remus Brad. “Attacks And Counterattacks On Wireless Sensor Networks.” ArXiv abs/1401.4443 (2013): n. pag.

[4] A. H. Moon, U. Iqbal, G. M. Bhat and Z. Iqbal, "Simulating and analyzing RREQ flooding attack in Wireless Sensor Networks," 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), Chennai, India, 2016, pp. 3374-3377, doi: 10.1109/ICEEOT.2016.7755330.

[5] Li, Jianpo, Dong Wang and Yanjiao Wang. “Security DV-hop localisation algorithm against wormhole attack in wireless sensor network.” IET Wirel. Sens. Syst. 8 (2017): 68-75.

[6] Faghihniya, M.J., Hosseini, S.M. & Tahmasebi, M. Security upgrade against RREQ flooding attack by using balance index on vehicular ad hoc network. Wireless Netw 23, 1863–1874 (2017). https://doi.org/10.1007/s11276-016-1259-2

[7] E. Niewiadomska-Szynkiewicz and F. Nabrdalik, "Secure low energy AODV protocol for wireless sensor networks", 2017 27th International Telecommunication Networks and Applications Conference (ITNAC), Melbourne, VIC, Australia, 2017, pp. 1-6, doi: 10.1109/ATNAC.2017.8215366.

[8] A. Sana, F. Youssef and R. M. Driss, "FLOODING ATTACK ON AODV IN WSN," 2018 Renewable Energies, Power Systems & Green Inclusive Economy (REPS-GIE), Casablanca, Morocco, 2018, pp. 1-5, doi: 10.1109/REPSGIE.2018.8488836.

[9] Y. Zhang and Y. Ding, "Performance Comparison of Localization Algorithm Based on the N-hop Anchors for Wireless Sensor Networks," 2019 8th International Symposium on Next Generation Electronics (ISNE), Zhengzhou, China, 2019, pp. 1-3, doi: 10.1109/ISNE.2019.8896653.

[10] Lakshmi HN, Santosh Anand and Somnath Sinha, “Flooding Attack in Wireless Sensor Network-Analysis and Prevention”, International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249-8958, Volume-8 Issue-5, June 2019.

[11] Ngoc T. Luong, Tu T. Vo, Doan Hoang, "FAPRP: A Machine Learning Approach to Flooding Attacks Prevention Routing Protocol in Mobile Ad Hoc Networks", Wireless Communications and Mobile Computing, vol. 2019, Article ID 6869307, 17 pages, 2019.https