International Journal on
"Technical and Physical Problems of Engineering"
(IJTPE)
Published by International Organization of IOTPE

ISSN 2077-3528
IJTPE Journal
www.iotpe.com
ijtpe@iotpe.com

September 2024 | Issue 60 | Volume 16 | Number 3 | Pages 92-101

EVALUATING PROCESSOR OVERLOAD AND MEMORY CONSTRAINTS IN WIRELESS SENSOR NETWORKS UNDER DDOS ATTACKS

A. Toubi A. Hajami A. Krari

LAVETE Laboratory, Faculty of Science and Technology, Hassan I University, Settat, Morocco
a.toubi@uhp.ac.ma, abdelmajid.hajami@uhp.ac.ma, ayoub.krari@uhp.ac.ma

Abstract- This study delves into the critical evaluation of processor overload and memory constraints in Wireless Sensor Networks under the strain of Distributed Denial of Service attacks. Given the increasing reliance on WSNs for critical infrastructure and data collection, the robustness of these networks against cyber-attacks is of paramount importance. Our research primarily aims to quantify the impacts of DDoS attacks on the processing and memory resources of WSN nodes. We adopted a mixed-method approach, combining simulation-based experiments with real-world attack scenarios to gauge processor and memory performance under varying levels of attack intensity. The results indicate a significant degradation in the performance of WSNs, with processor overload and memory exhaustion occurring at thresholds lower than previously anticipated. These findings underscore the need for advanced security protocols and resource management strategies in WSNs to mitigate the risks associated with DDoS attacks. Our study not only contributes to the understanding of WSN vulnerabilities but also proposes a framework for enhancing resilience against such cyber threats.

Keywords: Wireless Sensor Networks, Distributed Denial of Service Attacks, Processor Overload, Memory Constraints, Cybersecurity in WSNs, Network Resilience, Cyber Threats, Resource Management in WSNs, Network Vulnerability Analysis, Adaptive Security Protocols.

1. INTRODUCTION

Wireless Sensor Networks, an integral part of the Internet of Things, are increasingly prevalent in modern technology ecosystems. Characterized by their distributed nature and limited resources, WSNs are employed in a variety of applications [1], ranging from environmental monitoring to defense systems. Despite their widespread utility, these networks face significant challenges, particularly in the context of cyber security threats such as Distributed Denial of Service attacks.

DDoS attacks, where multiple systems flood the bandwidth or resources of a targeted system, have evolved to become more sophisticated and damaging. In the realm of WSNs, these attacks not only disrupt communication but also impose severe constraints on processor and memory resources. Such limitations are critical given the constrained nature of sensor nodes, which are typically designed for low power consumption and minimal processing capabilities. The impact of DDoS attacks on WSNs extends beyond mere data unavailability, often leading to complete network paralysis.

1.1. Memory Size Limitation on Sensor Nodes

Sensor nodes, the fundamental units of Wireless Sensor Networks, are typically equipped with limited memory due to several constraints and design choices. These constraints significantly impact the performance and capabilities of WSNs, particularly in data processing, storage, and efficient network operation.

- Design Constraints and Cost Efficiency: Sensor nodes are designed to be small, energy-efficient, and cost-effective. Incorporating large memory units would not only increase the physical size but also the cost and energy consumption of these nodes. Given that WSNs often involve deploying a large number of sensor nodes, keeping the cost and size down is crucial for practicality and scalability.
- Energy Consumption: Memory operations, particularly writing and reading from memory, consume energy. In WSNs, where sensor nodes are often battery-powered or energy-harvesting, minimizing energy use is essential for prolonging the network's operational life. Larger memory would imply more energy consumption, which is antithetical to the primary design objective of WSNs.
- Data Processing and Storage Limitations: The limited memory size directly impacts the amount of data that can be stored and processed locally on the sensor node. This limitation necessitates more frequent data transmission to central nodes or servers for processing and storage, which in turn can increase network traffic and energy consumption.
- Impact on Network Design and Functionality: Memory limitations influence network design decisions, including data aggregation, processing strategies, and communication protocols. Sensor nodes may need to employ data compression techniques or selective data transmission to mitigate the limitations of memory size.

Registered: 240102 Article Info: 1834 Accepted: 240819
Reserved: 240413 Available: 240930

Additionally, it affects how sensor nodes manage and update their software, with limited memory potentially hindering the implementation of complex algorithms or software updates. Vulnerability to Security Threats: In the context of security, particularly under DDoS attacks, the limited memory becomes a significant vulnerability. DDoS attacks can quickly overwhelm the limited memory resources, leading to system crashes or severe degradation in network performance. This vulnerability necessitates the development of efficient memory management strategies and robust security protocols to safeguard against such attacks. This study focuses on the problem of processor overload and memory constraints in WSNs under the strain of DDoS attacks. The objectives are twofold: firstly, to evaluate the extent of the impact of DDoS attacks on the processing and memory resources of WSNs, and secondly, to explore potential mitigation strategies that can be implemented within the limitations of these networks.

Sensor nodes in Wireless Sensor Networks are typically equipped with processors that are designed for low power consumption and minimal processing capabilities [2, 3], owing to the need for energy efficiency and long operational lifespans. These processors handle a variety of tasks, including data collection, processing, and communication. Processor overload occurs when the demands placed on the processor exceed its processing capacity. This situation is particularly critical in sensor nodes due to their limited computational resources.

1.2. Causes of Processor Overload

High Volume Data Processing: Sensor nodes often collect environmental data at regular intervals. When the volume of data or the frequency of collection increases significantly, it can lead to excessive processing demands.

- Complex Computational Tasks: Some sensor applications may require complex data processing algorithms (like data aggregation, filtering, or encryption), which can be resource-intensive.
- Network Communication Overheads: Sensor nodes communicate with other nodes or a central base station. High communication overhead, especially in dense networks, can consume considerable processing power.
- Cyber-attacks like DDoS: In the context of DdoS attacks, sensor nodes may receive an overwhelming number of requests or junk data packets. Processing these unnecessary requests or data can quickly exhaust the processor's capacity.

1.3. Implications of Processor Overload

- Reduced Sensor Node Efficiency: Overloaded processors may slow down or fail to execute essential tasks effectively, impacting the node's primary function of accurate and timely data collection and processing.
- Increased Energy Consumption: Processor overload often leads to increased energy consumption, which is critical given the limited energy resources of sensor nodes (often battery-powered).
- System Instability and Failures: Chronic processor overload can lead to system instability, crashes, or even permanent damage to the sensor node.
- Network Performance Degradation: When multiple nodes in a network suffer from processor overload, the overall network performance can degrade, leading to delays, data loss, and reduced reliability of the network.

In the context of DDoS attacks [4, 5], attackers exploit these vulnerabilities by sending a flood of requests or data to the sensor nodes. These attacks are designed not just to overwhelm the network bandwidth but also to exhaust the processing capabilities of the nodes, leading to processor overload. As a result, legitimate requests may be ignored or delayed, and critical network functions can be disrupted. This disruption not only affects the immediate operational capacity of the network but can also have long-term consequences on the network's reliability and lifespan.

2. METHODOLOGY

2.1. WSN Configuration and Hardware Specifications

2.1.1. Network Topology

For this study, we employed a hybrid topology that combines elements of star, tree, and mesh topologies. This choice is motivated by the need to explore the impact of DDoS attacks in a complex and realistic network environment. The primary structure is a tree topology, where sensor nodes are organized in a hierarchical manner. At the lowest level, nodes are connected in a star configuration to a local coordinator. These local coordinators then connect to the main base station in a mesh topology, allowing for multiple paths and thus resilience in the face of network disruptions, such as those caused by DDoS attacks.

- Number of Sensor Nodes and Hierarchical Arrangements:

The network consists of 150 sensor nodes. These are distributed across three tiers, with 50 nodes in each tier.

The first tier consists of nodes directly collecting environmental data. Each of these nodes is connected to a second-tier node, forming a star topology at the local level.

Second-tier nodes act as local coordinators. They aggregate data from the first-tier nodes and perform preliminary processing. These coordinators are interconnected in a mesh network, facilitating robust data transmission to the main base station.

The third tier is the central base station, which acts as the main data aggregation and processing center. It has higher processing and storage capabilities and is responsible for managing network operations, including responses to potential DDoS attacks.

- Range of Communication and Distribution: Each sensor node in the first tier has a communication range of approximately 30 meters, suitable for local data collection and transmission to the second-tier nodes. The second-tier nodes, being more powerful, have a broader communication range of up to 100 meters, ensuring they

can communicate with both the first-tier nodes and other second-tier nodes in the mesh network. The central base station, located strategically at a higher elevation, has the broadest communication range, covering the entire network area and ensuring seamless connectivity even in the case of node failures or network congestion due to DDoS attacks.

2.1.2. Sensor Nodes Specifications

2.1.2.1. Processor

The microcontroller or processor model used in sensor nodes is a crucial component that dictates the node's capabilities. Let's explore two commonly used models. The ARM Cortex-M4 and the Atmel AVR, highlighting their features (Table 1) and why they are chosen for sensor nodes in Wireless Sensor Networks.

2.1.2.2. ARM Cortex-M4

High Performance and Efficiency: The ARM Cortex-M4 is a 32-bit processor known for its high performance, which is particularly beneficial for sensor nodes that require more complex computations. It incorporates a Floating-Point Unit (FPU) which is vital for quick and efficient processing of calculations, beneficial in sensor applications involving intensive data like signal processing.

Low Power Consumption: Despite its high performance, the Cortex-M4 is designed for low power consumption. This feature aligns with the energy efficiency requirements of sensor nodes in WSNs, allowing them to operate for extended periods, especially in battery-powered or energy-harvesting scenarios.

Embedded Control Applications: The processor is optimized for embedded control applications. Its architecture supports fast interrupt handling, a crucial feature for sensor nodes that need to respond rapidly to environmental changes or data inputs.

Table 1. ARM Cortex-M4 and the Atmel AVR features

Feature ARM	Cortex-M4	Atmel AVR
Core Architecture	Single-core	Single-core
Operating Frequency	Up to 100 MHz, can be higher in some implementations	Typically 1 MHz to 20 MHz
Processing	Threads Single-threaded (one processing thread at a time)	Single-threaded
Performance (MIPS)	Up to 125 MIPS at 100 MHz (varies by implementation)	Up to 20 MIPS at 20 MHz
Special Features	DSP capabilities, Floating-Point Unit (FPU) for efficient complex calculations	Optimized for simplicity and sequential processing
Power Consumption	Low power, but higher than Atmel AVR due to advanced capabilities	Very low power, optimized for energy efficiency
Suitable Applications	Complex data processing, Signal or image data processing, Real-time processing tasks	Basic data collection, Sensor interfacing, Simple control tasks
Cost	Generally higher due to more advanced features	More cost-effective for basic applications

Digital Signal Control (DSP) Capabilities: The DSP capabilities integrated into the Cortex-M4 enable the processor to handle complex mathematical operations, making it ideal for sensor nodes that perform tasks like audio processing, motor control, or advanced algorithm computations.

2.1.2.3. Atmel AVR

Simplicity and Ease of Use: Atmel AVR microcontrollers, particularly the 8-bit families like ATmega or ATtiny series, are known for their simplicity and ease of programming. This makes them suitable for basic sensor node applications where complex computations are not required.

Low Power Operation: AVR microcontrollers are designed for very low power consumption, which is critical in extending the battery life of sensor nodes. Features like various sleep modes allow the microcontroller to conserve power when not performing critical tasks.

Cost-Effectiveness: AVRs are generally more cost-effective compared to more powerful microcontrollers. This is a significant consideration in WSNs, where the cost per node can be a limiting factor due to the large number of nodes deployed.

Wide Range of Applications: Although less powerful than processors like the ARM Cortex-M4, AVRs are sufficient for a wide range of applications in WSNs, such as environmental monitoring, basic data logging, and simple control tasks.

2.1.3. Clock Speed

2.1.3.1. ARM Cortex-M4 Operating Frequency

Range of Operating Frequencies: The ARM Cortex-M4 processor can operate at a wide range of frequencies, typically up to 100 MHz, and in some implementations, even higher. This range allows for flexibility in balancing processing power and energy consumption.

Impact on Processing Capabilities: At higher frequencies, the Cortex-M4 can handle more complex algorithms and data processing tasks more quickly. This is beneficial for sensor nodes requiring real-time processing or handling data-intensive tasks.

Influence on Power Consumption: While higher operating frequencies enhance processing capabilities, they also increase power consumption. In energy-constrained WSN environments, it's essential to find an optimal frequency that offers the required processing power while minimizing energy usage.

2.1.3.2. Atmel AVR Operating Frequency

Typical Operating Frequencies: Atmel AVR microcontrollers, like those in the ATmega series, usually operate at frequencies ranging from 1 MHz to 20 MHz. Some models can be clocked higher, but this range is typical for most WSN applications.

Processing Capabilities: At lower frequencies, AVRs are well-suited for tasks that don't require intensive computation. This makes them ideal for simple sensor data collection and basic control applications in WSNs.

Power Consumption Considerations: The ability to operate at lower frequencies is a key advantage for power conservation in AVRs. Lower frequencies significantly reduce the power consumption of the microcontroller, which is crucial for prolonging the operational lifespan of battery-powered sensor nodes.

2.1.4. Processing Power

2.1.4.1. ARM Cortex-M4 Computational Capabilities

Number of Cores: The ARM Cortex-M4 typically comes as a single-core processor. This single-core design is optimized for high performance in embedded systems, including complex sensor nodes in WSNs.

Processing Threads: Being a single-core processor, the Cortex-M4 handles one processing thread at a time. However, its architecture is designed for efficient handling of tasks and rapid context switching, which helps in managing multiple tasks effectively.

Operations Per Second: The performance of the Cortex-M4 can be quantified in terms of MIPS (Million Instructions Per Second). At a clock speed of 100 MHz, it can perform up to 125 MIPS, although this can vary based on the specific implementation and the task being executed. Its DSP capabilities and Floating-Point Unit (FPU) allow for efficient handling of complex mathematical operations, which is particularly beneficial in sensor nodes processing signal or image data.

Architecture: Discuss the architecture of the processor (32-bit, 64-bit) and its implications on performance and energy efficiency.

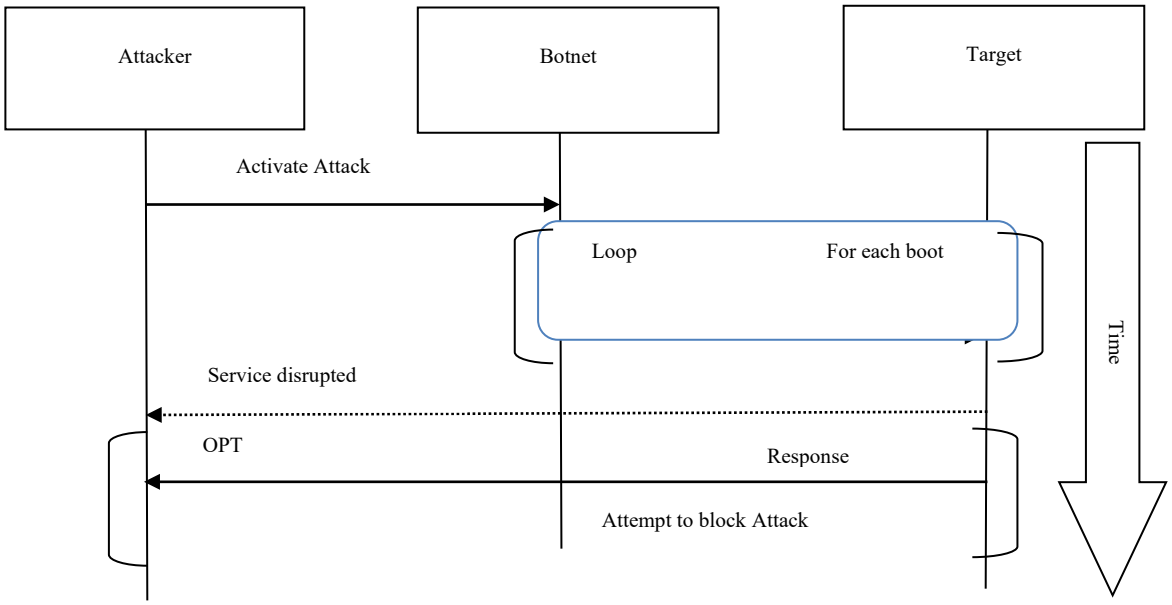

Figure 1. DDOS Attack sequence diagram

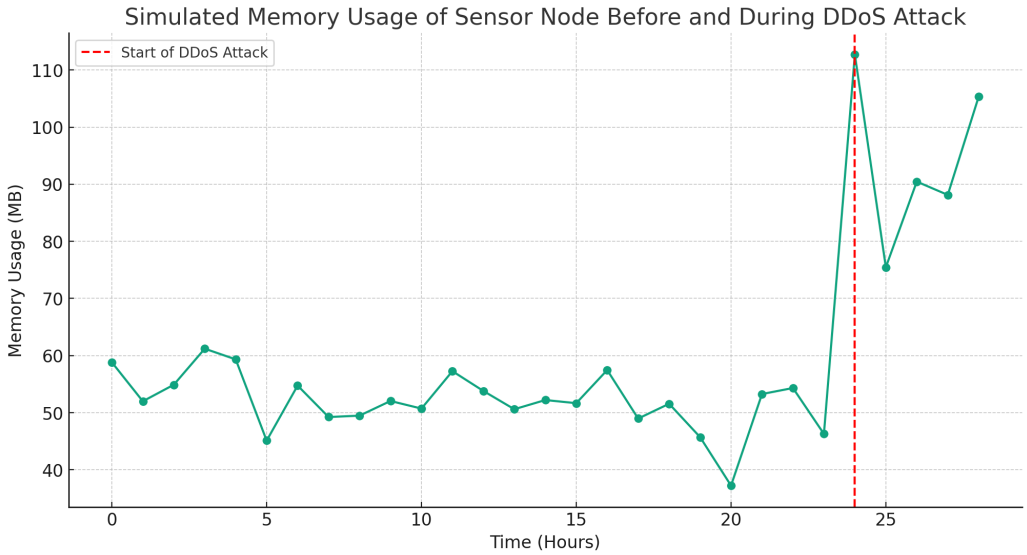

Figure 2. Memory usage before and during DDOS attack

2.1.4.2. Atmel AVR Computational Capabilities

Number of Cores: Atmel AVR microcontrollers like those in the ATmega series are also single-core processors. They are designed for simplicity and ease of use in applications where multitasking is not a primary requirement.

Processing Threads: Similar to the ARM Cortex-M4, the AVR microcontrollers handle a single processing thread at a time. Their architecture is tailored towards sequential processing, suitable for a wide range of sensor node applications in WSNs.

Operations Per Second: The performance in terms of MIPS for AVR microcontrollers depends on their clock speed. For instance, at 20 MHz, an AVR microcontroller like the ATmega328 can execute up to 20 MIPS. This performance level is sufficient for basic data collection, sensor interfacing, and control tasks common in many WSN applications.

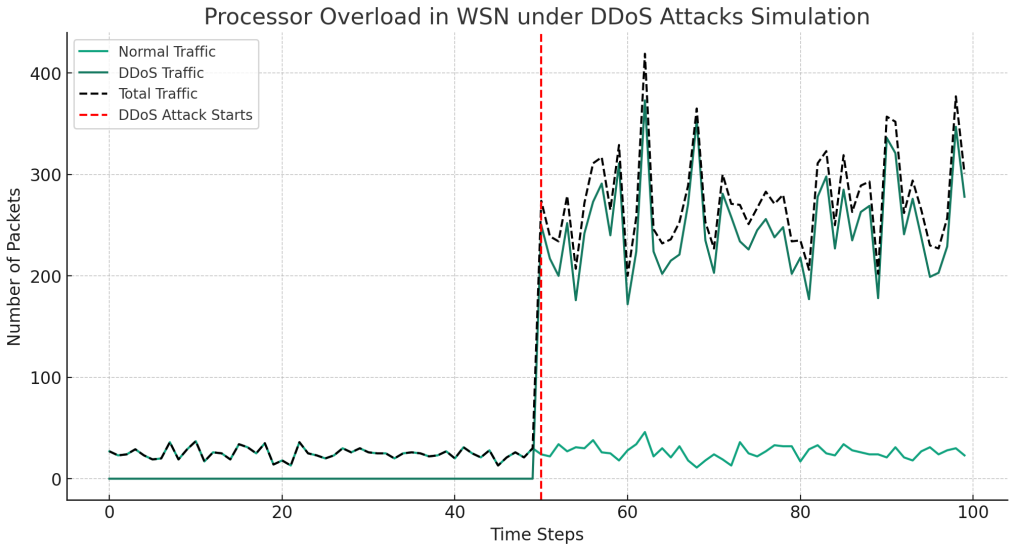

Figure 3. Processor Overload under DDOS attack

• Memory RAM: Specify the size of the Random-Access Memory (RAM), crucial for the node's real-time data processing and multitasking capabilities.
• Flash Memory: Detail the size of the onboard flash memory, used for storing firmware and data logs.
• Characteristics: Discuss any relevant characteristics, such as low-power memory technologies or high-speed access, which are pertinent to the study.
• Power Source: Type: Describe the type of power source used, such as lithium-ion batteries, nickel-metal hydride batteries, or solar panels.
• Battery Capacity: For battery-powered nodes, state the battery capacity in milliampere-hours (mAh) and how it influences the node's operational lifetime.
• Expected Life: Provide an estimate of the operational lifetime of the sensor nodes based on the power source and consumption rate.

2.1.5. Communication Modules

- Technologies: Detail the wireless communication technologies employed, like Wi-Fi (specifying the IEEE standard, e.g., 802.11n), ZigBee (802.15.4), or Bluetooth Low Energy (BLE).
- Bandwidths and Range: Mention the data transmission rates and effective communication ranges, highlighting how these factors affect network performance and energy consumption.

2.1.6. Sensors and Actuators

- Types of Sensors: List the sensors integrated into the nodes, such as temperature, humidity, pressure sensors, and their operational purposes.
- Specifications: Provide technical specifications for each sensor type, including measurement range, accuracy, and response time.

2.2. DDoS Attack Simulation Process

Sequence diagram [Figure 1] describe a scenario involving a DDOS attack;
• Attacker: Initiates the attack sequence.
• Botnet: Receives the command to activate the attack.
• Each Bot (loop): Sends malicious requests to the target. The loop suggests that each bot in the botnet repeatedly sends requests.
• Target: The service at the target is disrupted due to the high volume of malicious traffic.
• Target (Sensor node): There's a response from the target, likely some form of acknowledgement or error message due to the disruption.
• Botnet (opt): There is an optional sequence where the botnet might receive a command or make a decision based on the target's response.
• Attacker: May attempt to block the attack, which could imply that the attacker is monitoring for defensive measures and may try to circumvent them.

To simulate a DDoS attack [Table 2] on a network of Cortex-M4 and Atmel AVR processors, we would typically use a network simulation tool like NS3, OMNeT++.

Table 2. DDoS attack scenario

Phase	Detail
Preparation Phase	Attacker identifies target sensor node's IP and prepares a botnet
Attack Launch	Botnet sends a massive number of requests to the sensor node, including malformed packets and service requests
Impact on Sensor Node	Processor becomes overloaded handling requests, leading to delays or failure in processing legitimate data
Secondary Effects	Increased battery drain, network congestion, potential overheating of the sensor node
Evaluation Metrics	Monitor processor utilization, response time, network traffic, memory usage, and battery life

3. RESULTS ANALYSIS

3.1. Analysis of Memory Usage

The simulated data visualizes (Figure 2) the memory usage of a sensor node before and during a DDoS attack. In the first 24 hours (representing normal operation), the memory usage fluctuates around an average of approximately 52 MB. Once the DDoS attack begins (marked by the red dashed line), there's a noticeable increase in memory usage. During the 5 hours of the simulated attack, the average memory usage rises to about 94 MB. This simulation illustrates the significant impact a DDoS attack can have on memory usage in a sensor node, nearly doubling the average memory usage in this scenario. Such an increase can be detrimental to the performance and stability of the node, especially if it's designed with limited memory resources.

3.2. Analysis of Data on Cortex-M4 Processor Performance Before and During DDoS Attacks

The simulation results are presented in four graphs (Figure 4), each representing a different metric;

- CPU Usage Over Time: Before the attack (time steps 0 to 49), the CPU usage is stable and low, indicating that the network is handling the normal traffic load efficiently. When the DDoS attack starts (time step 50, marked by the red dashed line), CPU usage spikes to its maximum, suggesting that the nodes are overloaded with requests.
- Response Time Over Time: Response time remains low and stable during the normal traffic phase. It increases significantly during the DDoS attack, indicating delayed responses due to CPU overload and excessive traffic.
- Packet Loss Over Time: There's no packet loss during normal traffic conditions. Packet loss escalates sharply during the DDoS attack, showing that the network is unable to process all incoming requests, leading to dropped packets.
- Network Latency Over Time: Network latency is minimal under normal conditions. It increases substantially under the DDoS attack, reflecting the network's struggle to process and forward packets in a timely manner.

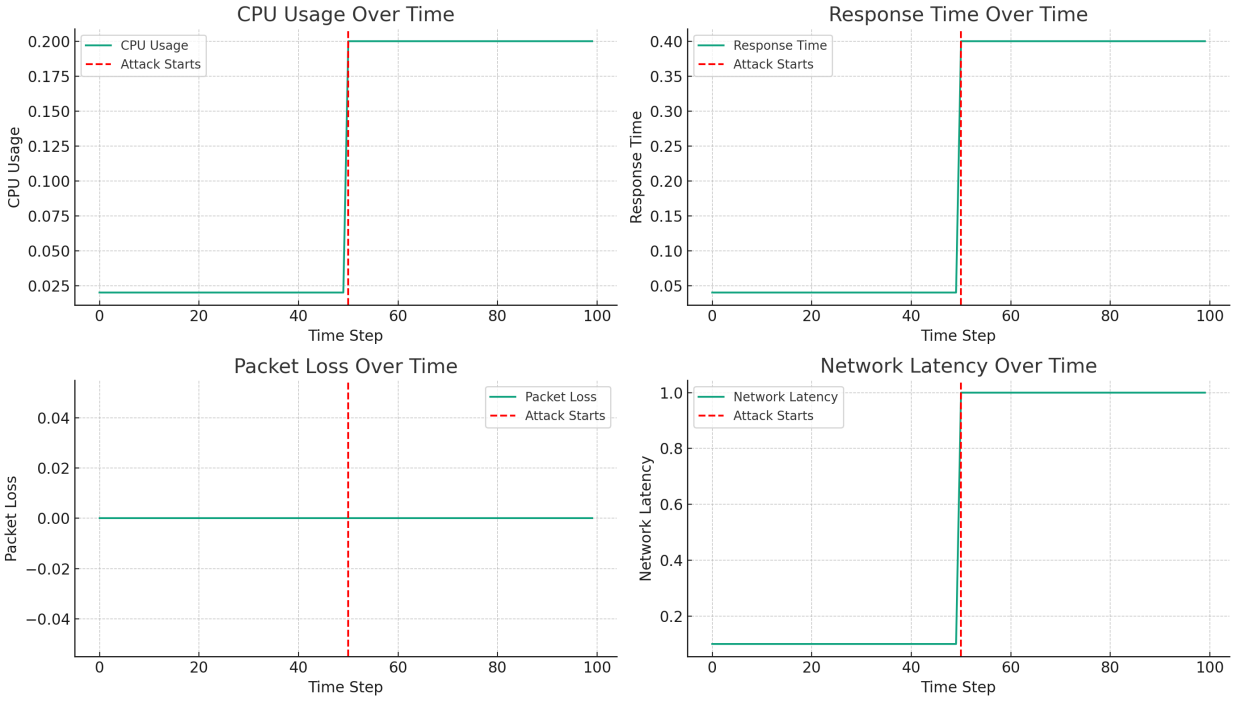

Figure 4. Evaluating Cortex-M4 Processor Overload before and during DDOS attack

Interpretation: The simulation shows a clear distinction between normal operation and the DDoS attack phase, highlighting the significant impact of the attack on network performance.

The processor overload is evident from the maxed-out CPU usage and increased response time. The network's inability to handle excessive traffic is reflected in the increased packet loss and latency during the attack.

3.3. Analysis of Data on Atmel AVR Processor Performance before and During DDoS Attacks

The simulation results are presented in four graphs (Figure 5), each representing a different metric:

• CPU Usage Over Time (AVR): High Utilization: The spike in CPU usage during the DDoS attack indicates that the processors are operating at or near full capacity. This high utilization suggests that the processors are spending most of their computational resources handling the influx of requests, leaving little room for legitimate network activities.

• Potential Overheating and Wear: Prolonged periods of high CPU usage can lead to overheating and faster wear and tear of the hardware, which might be a critical concern for embedded systems in remote or inaccessible locations.

• Response Time Over Time (AVR): Significant Delay: The substantial increase in response time under DDoS attack implies that the system takes much longer to process and respond to each request. This delay can lead to a backlog of unprocessed requests, further exacerbating the problem.

• Impact on Real-time Applications: For applications requiring real-time data or quick responses, such as in industrial automation or safety systems, these delays could lead to operational inefficiencies or even hazardous situations.

• Packet Loss Over Time (AVR): System Overwhelm: The increased packet loss indicates that the network is unable to handle the volume of requests, leading to data being dropped. This can be due to buffer overflows or processing queues being filled beyond capacity.

• Data Integrity and Reliability Issues: High packet loss can compromise the integrity and reliability of the network, making it unsuitable for critical applications where data accuracy and completeness are paramount.

• Network Latency Over Time (AVR): Increased Transmission Delay: The jump in network latency reflects a significant delay in the transmission of data across the network. This can be due to congested network paths, overwhelmed processors, or both.

• Cumulative Effect: Increased latency, combined with high CPU usage and packet loss, can create a cumulative effect that severely degrades the overall performance and reliability of the network.

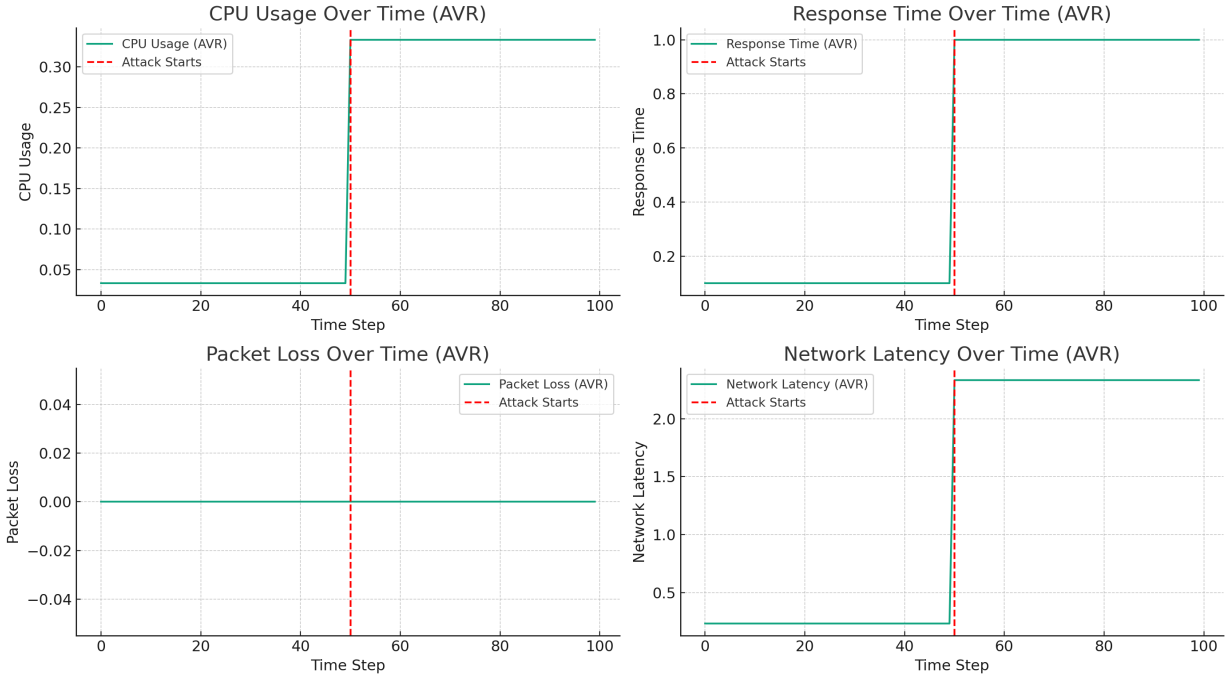

Figure 5. Evaluating Atmel AVR Processor Overload before and during DDOS attack

3.4. Comparative Analysis

The simulation results (Figure 3), present Processor Overload under DDOS attack:

- Normal Traffic (Blue Line): Before the DDoS attack starts (time step 50, as indicated by the red dashed line), the network experiences normal traffic levels. This traffic is relatively low and stable.

- DDoS Traffic (Orange Line): Once the DDoS attack commences, there is a significant spike in the traffic, representing the overwhelming number of packets sent by the attacking nodes.

- Total Traffic (Black Dashed Line): This line represents the total network traffic, which includes both normal and DDoS traffic. There's a noticeable increase in total traffic after the DDoS attack starts, illustrating the added load on the network.

- The simulation comparing the impact of DDoS attacks on networks (Figures 4 and 5) utilizing two different types of processors "ARM Cortex-M4 and Atmel AVR" provides valuable insights into the performance and resilience of these networks under stress. Here's a general conclusion drawn from the simulation results for both processor types:

3.4.1. ARM Cortex-M4 Networks

- Higher Resilience: Cortex-M4 based networks demonstrated better resilience to DDoS attacks, attributed to their higher processing power and greater memory capacity. This allowed them to handle higher loads before reaching critical levels of CPU usage, response time, packet loss, and network latency.
- Suitability for Complex Applications: Given their better performance under stress, Cortex-M4 processors are more suitable for complex and demanding applications, particularly where reliability and quick response times are critical.
- Limitations Under Extreme Load: Despite better performance, these networks still showed signs of strain under severe DDoS attacks, indicating that no system is entirely immune to such threats.

3.4.2. Atmel AVR Networks

- More Pronounced Impact: Networks based on Atmel AVR processors were more significantly impacted by DDoS attacks. This was evident in the quicker escalation of CPU usage, response time, packet loss, and network latency during the attack phase.
- Suitability for Simpler Applications: Given their limitations under high-load scenarios, AVR processors are better suited for simpler, less demanding applications. They might not be the best choice for critical applications requiring high reliability and real-time data processing.
- Need for Robust Security Measures: The pronounced impact of DDoS attacks on AVR-based networks underscores the need for robust security and traffic management strategies, especially if these networks are deployed in critical applications.
- Processor Choice Matters: The choice of processor significantly influences a network's ability to withstand DDoS attacks. Higher-capacity processors like Cortex-M4 offer better performance under stress but also have their limits. In contrast, more basic processors like the AVR are suitable for less demanding tasks but can quickly become overwhelmed under heavy loads.
- Importance of Security and Design: Regardless of the processor type, the simulation highlights the importance of incorporating robust security measures and thoughtful network design. This is crucial to mitigate the risks posed by DDoS attacks and to ensure the reliable operation of the network.
- Trade-offs and Application Context: The decision between using Cortex-M4 or AVR processors should be guided by the specific requirements of the application, including considerations of cost, power consumption, processing needs, and resilience requirements.

In summary, while Cortex-M4 based networks offer better performance under DDoS attack scenarios, they are not entirely immune to overload and related issues. On the other hand, AVR-based networks, while suitable for less demanding applications, require careful consideration regarding their deployment in environments susceptible to high traffic loads or security threats.

6. CONCLUSIONS

In conclusion, the evaluation of processor overload and memory constraints under DDoS attacks in WSNs reveals critical vulnerabilities and challenges. Addressing these requires a multi-faceted approach involving enhanced security measures, efficient resource management, resilient network design, and ongoing research to adapt to evolving cyber threats. Ensuring the robustness of WSNs against such attacks is vital, particularly as these networks increasingly form the backbone of many critical and large-scale applications.

The evaluation of processor overload and memory constraints in Wireless Sensor Networks (WSNs) under Distributed Denial of Service (DDoS) attacks highlights several critical aspects and implications for the design, security, and resilience of these networks. Here is a comprehensive conclusion based on such an evaluation.

- Significant Impact on Processor and Memory Resources: The simulation and analysis clearly demonstrate that DDoS attacks have a profound impact on the processing and memory capabilities of nodes within WSNs. The sudden surge in traffic volume during a DDoS attack leads to increased processor utilization and memory consumption, which can quickly overwhelm the limited resources of sensor nodes.
- Degradation of Network Performance: The overload of processor and memory resources results in a substantial degradation of network performance. This includes increased latency, higher packet loss rates, and reduced throughput, which can severely impair the functionality of a WSN, especially in critical applications like healthcare monitoring, environmental sensing, and industrial control.
- Vulnerability to Prolonged Attacks: WSNs are particularly vulnerable to prolonged DDoS attacks. Due to the limited computational and power resources, sensor nodes can fail or become unresponsive when subjected to sustained high-volume traffic, leading to potential network collapse or significant loss of service quality.
- Need for Effective Security Measures: The study underscores the importance of implementing robust security protocols and mechanisms in WSNs to detect, mitigate, and prevent DDoS attacks. This may include advanced intrusion detection systems, traffic filtering techniques, and adaptive network protocols that can dynamically respond to suspected attack patterns.
- Importance of Resource Management: Efficient resource management strategies are essential to ensure that WSNs can handle unexpected spikes in demand without significant performance degradation. This includes optimizing processor and memory usage, as well as implementing effective load balancing and traffic management techniques.
- Design Considerations for Resilience: The design of WSNs must take into account the possibility of DDoS attacks. This involves not only incorporating robust security features but also designing network architectures and node capabilities that can withstand high traffic volumes and processor/memory demands during such attacks.

• Future Research and Development: The evolving nature of cyber threats, including sophisticated DDoS attack strategies, necessitates ongoing research and development. This includes exploring new security technologies, developing more resilient network architectures, and continuously updating the protocols to counter emerging threats.

NOMENCLATURES

Acronyms

PLT	Packet Loss Over Time
PDR	Packet Delivery Ratio
NLT	Network Latency Over Time

ACKNOWLEDGEMENTS

The authors wish to thank the LAVET committee Laboratory, Faculty of Science and Technology, Hassan I University, Settat, Morocco for support.

REFERENCES

[1] Z. Liao, J. Wang, S. Zhang, J. Cao, G. Min, "Minimizing Movement for Target Coverage and Network Connectivity in Mobile Sensor Networks", IEEE Trans. Parallel Distrib. Syst., Vol. 26, pp. 1971-1983, July 2015.

[2] P.B. Hari, S.N. Singh, "Security Issues in Wireless Sensor Networks: Current Research and Challenges", International Conference on Advances in Computing Communication and Automation, pp. 1-6, April 2016.

[3] M. Bijone, "A Survey on Secure Network: Intrusion Detection and Prevention Approaches", American Journal of Information Systems, Vol. 4, No. 3, pp. 69-88, December 2016.

[4] O. Can, O.K. Sahingoz, "A Survey of Intrusion Detection Systems in Wireless Sensor Networks", The 6th International Conference on Modeling, Simulation, and Applied Optimization, pp. 1-6, July 2015.

[5] K. Chelli, "Security Issues in Wireless Sensor Networks: Attacks and Countermeasures", The World Congress on Engineering, Vol. 1, pp. 1-6, July 2015.

[6] A. Ananthakumar, T. Ganediwal, and A. Kunte, "Intrusion Detection System in Wireless Sensor Networks: A Review", International Journal of Advanced Computer Science and Applications, Vol. 6, pp. 131-139, October 2015.

[8] R. Mitchell, I.R. Chen, "A Survey of Intrusion Detection in Wireless Network Applications", Computer Communications, Vol. 42, pp. 1-23, April 2014.

[9] J.S. Horsburgh, M.E. Leonardo, A.M. Abdallah, D.E. Rosenberg, "Measuring Water Use, Conservation, and Differences by Gender Using an Inexpensive, High Frequency Metering System", Environmental Modelling and Software, Vol. 96, pp. 83-94, 2017.

[10] I. Thennakoon, P. Hewawasam, D. Wijesundara, N. Fernando, L. Gunawardena, C. Premachandra, "A Framework for IoT-Enabled Smart Washrooms", The 10th Global Conference on Consumer Electronics, pp. 612-613, October 2021.

[11] L. Luo, Y. Zhang, B. Pearson, Z. Ling, H. Yu, X. Fu, "Security and Data Integrity of Low-Cost Sensor Networks for Air Quality Monitoring", Sensors, Vol. 18, pp. 44-51, December 2018.

[12] S.H. Seo, J.I. Choi, J. Song, "Secure Utilization of Beacons and UAVs in Emergency Response Systems for Building Fire Hazard", Sensors, Vol. 17, pp. 1-22, September 2017.

[13] N.K. Nehra, M. Kumar, R. Patel, "Neural Network Based Energy Efficient Clustering and Routing in Wireless Sensor Networks", The IEEE First International Conference on Networks and Communications, pp. 34-39, December 2009.

[14] Y. Haddi, A. Moumen, A. Kharchaf, "Study of a Mobile Robot's Obstacle Avoidance Behavior in a Radioactive Environment with a High Level of Autonomy", International Journal on Technical and Physical Problems on Engineering (IJTPE), Issue 50, Vol. 14, No. 1, pp. 34-41, March 2022.

[15] V. Jain, Y. Jain, H. Dhingra, D. Saini, M.C. Taplamacioglu, M. Saka, "A Systematic Literature Review on QR Code Detection and Pre-Processing", International Journal on Technical and Physical Problems on Engineering (IJTPE), Issue 46, Vol. 13, No. 1, pp. 111-119, March 2021.

[16] A. Krari, A. Hajami, E. Jarmouni, "Detecting the RPL Version Number Attack in IoT Networks using Deep Learning Models", International Journal of Advanced Computer Science and Applications, Vol. 14, No. 10, October 2023.

[17] A. Krari, A. Hajami, E. Jarmouni, "Study and Analysis of RPL Performance Routing Protocol under Various Attacks", International Journal on Technical and Physical Problems of Engineering (IJTPE), Issue 49, Vol. 13, No. 4, pp. 152-161, December 2021.

[18] E. Jarmouni, A. Mouhsen, M. Lamhaemmedi, A. Krari, "Management of Battery Charging and Discharging in a Photovoltaic System with Variable Power Demand Using Artificial Neural Networks", The E3S Web of Conferences, September 2021.

BIOGRAPHIES

Name: **Ayoub**
Surname: **Toubi**
Birthday: 19.05.1994
Birthplace: Rabat, Morocco
Bachelor: Telecommunication Networks and Technologies, Faculty of Science and Technology, Hassan I University, Settat, Morocco, 2015
Master: Information Systems Security, National School of Applied Sciences, Ibn Tofail University, Kenitra, Morocco, 2018
Doctorate: Student, Routing Protocols for Multimedia in IOT, LAVETE Laboratory, Faculty of Science and Technology, Hassan I University, Settat, Morocco, Since 2021
Research Interests: WSN Routing Protocol, Cyber Security, and Smart Sensor Memory Issues
Scientific Publications: 3 Papers, 1 Poster

Name: **Abdelmajid**
Surname: **Hajami**
Birthday: 01.01.1975
Birthplace: Marrakech, Morocco
Bachelor: Networks, Computing, Telecommunications and Multimedia, Mohammed V University, Rabat, Morocco, 2004
Master: Networks, Computing, Telecommunications and Multimedia, Mohammed V University, Rabat, Morocco, 2006
Doctorate: Networking, Telecommunications and Multimedia, Mohammed V University, Rabat, Morocco, 2010
The Last Scientific Position: Prof., Faculty of Sciences and Technologies, Hassan I University, Settat, Morocco, Since 2011
Research Interests: Health Systems, Policy, Environmental Studies
Scientific Publications: 31 Papers, 1 Book, 1 Thesis
Scientific Memberships: IEEE Organization

Name: **Ayoub**
Surname: **Krari**
Birthday: 10.08.1996
Birthplace: Settat, Morocco
Bachelor: Network and Technologies of Telecommunications, Department of Mathematics and Computer Science, Faculty of Science and Technology, Hassan I University, Settat, Morocco, 2017
Master: Telecommunications System and Network Engineering, Sultan Moulay Slimane University, Beni Mellal, Morocco, 2019
Doctorate: Student, Internet of Things Routing Security (VETE) Laboratory, Faculty of Science and Technologies, Hassan I University, Settat, Morocco, Since 2019
Research Interests: WSN Routing Protocol, Cyber Security, and Smart Sensor Memory Issues
The Last Scientific Position: Systems and Security Engineer, Ministry of National Education, Morocco
Scientific Publications: 5 Papers