Optimizing Energy and Memory Efficiency in Clone Detection for Wireless Sensor Networks

K. Mounika

B. Tech (CSE), Sree Rama Engineering College

Abstract:

In this study, we introduce an energy-efficient, location-aware clone detection protocol tailored for densely deployed Wireless Sensor Networks (WSNs), designed to ensure successful clone attack detection while maintaining a satisfactory network lifetime. Our approach leverages the location information of sensors and employs a random selection of witnesses positioned within a ring area to authenticate sensor legitimacy and report clone attacks. The ring structure enhances energy efficiency by facilitating data forwarding along optimal paths to the witnesses and the sink.

Our theoretical analysis demonstrates that this protocol can achieve a 100 percent clone detection probability when witnesses are trustworthy. Furthermore, we extend our research to evaluate the protocol's performance with untrustworthy witnesses, finding that the clone detection probability remains robust, approaching 98 percent even if 10 percent of the witnesses are compromised. Unlike many existing clone detection protocols that rely on random witness selection and have buffer storage requirements dependent on node density, our protocol's buffer storage requirement is independent of node density and instead depends on the hop length of the network radius. Extensive simulations confirm that our protocol can significantly enhance network lifetime by efficiently distributing the traffic load across the network.

Keywords: Wireless sensor network, Clone Detection

Introduction:

Wireless Sensor Network (WSN)

A wireless sensor network (WSN) comprises spatially distributed autonomous sensors designed to monitor physical or environmental conditions like temperature, sound, and pressure, and to transmit the collected data to a central location. Modern WSNs are often bi-directional, allowing for both data collection and control over sensor activities. Originally developed for military purposes such as battlefield surveillance, WSNs are now widely used in various industrial and consumer applications, including industrial process monitoring, machine health monitoring, and more.

A WSN is composed of "nodes," which can range from a few to several hundred or even thousands. Each node is typically equipped with one or more sensors and includes several key components: a radio transceiver with an internal or external antenna, a microcontroller, an electronic interface for the sensors, and a power source, which can be a battery or an energy harvesting device. The size of sensor nodes can vary significantly, from as large as a shoebox to as small as a grain of dust, although practical microscale nodes ("motes") have yet to be developed. The cost of these nodes also varies, from a few dollars to several hundred dollars, depending on their complexity. These constraints in size and cost affect the resources available for energy, memory, computational speed, and communication bandwidth.

The topology of WSNs can range from simple star configurations to complex multi-hop wireless mesh networks. Data propagation between nodes can be achieved through routing or flooding techniques. These networks are designed to efficiently manage the limited resources of the sensor nodes while ensuring reliable data collection and transmission across the network.

Existing System:

In the context of clone detection within wireless sensor networks (WSNs), a set of nodes, referred to as witnesses, are chosen to verify the authenticity of other nodes in the network. During the witness selection phase, the private information of the source node, such as its identity and location, is shared with these witnesses. When a node wishes to transmit data, it must first request legitimacy verification from the witnesses. If a node fails this verification, the witnesses will report an attack. For clone detection to be effective, the process of selecting witnesses and verifying legitimacy must meet two criteria: 1) the witnesses must be chosen randomly, and 2) at least one of the witnesses must be able to successfully receive all verification messages to detect any clones.

Existing protocols like the Randomized Efficient and Distributed (RED) protocol and the Line-Select Multicast (LSM) protocol often face challenges with energy efficiency. These protocols can lead to unbalanced energy consumption among nodes, causing some sensors to exhaust their batteries prematurely. This imbalance can result in dead sensors, leading to network partitioning and ultimately disrupting the normal operations of the WSNs.

Proposed System:

In this work, we propose a clone detection protocol that prioritizes not only the detection probability but also energy consumption and memory storage efficiency. Our protocol, designed for densely deployed multi-hop wireless sensor networks (WSNs), utilizes a random witness selection scheme to create an energy- and memory-efficient distributed system for detecting cloned nodes.

Our approach is robust against adversaries that may compromise and clone sensor nodes to execute attacks. The protocol, named Energy-Efficient Ring-Based Clone Detection (ERCD), extends existing analytical models by incorporating evaluations of the required data buffer and providing experimental results to support our theoretical analysis.

The ERCD protocol distributes witnesses evenly across the network, avoiding the creation of witness rings adjacent to the sink, which are designated as non-witness rings to conserve energy. We determine the optimal number of these non-witness rings based on an energy consumption function, ensuring balanced energy use throughout the WSN.

Additionally, we derive an expression for the required data buffer when using the ERCD protocol. Our findings indicate that the protocol is scalable, with the required buffer storage dependent solely on the size of the ring, making it suitable for large-scale WSN deployments.

System Design:

Input Design:

Input design serves as the bridge between the information system and its users, involving the creation of specifications and procedures for data preparation. This process transforms transaction data into a usable format for processing. Data can be inputted by instructing the computer to read from a written or printed document or by having users directly enter data into the system. Effective input design aims to:

- Minimize the amount of input required
- Control and reduce errors
- Avoid delays
- Simplify the process
- Ensure security and ease of use while maintaining privacy

The goal is to create an input system that is efficient, secure, and user-friendly.

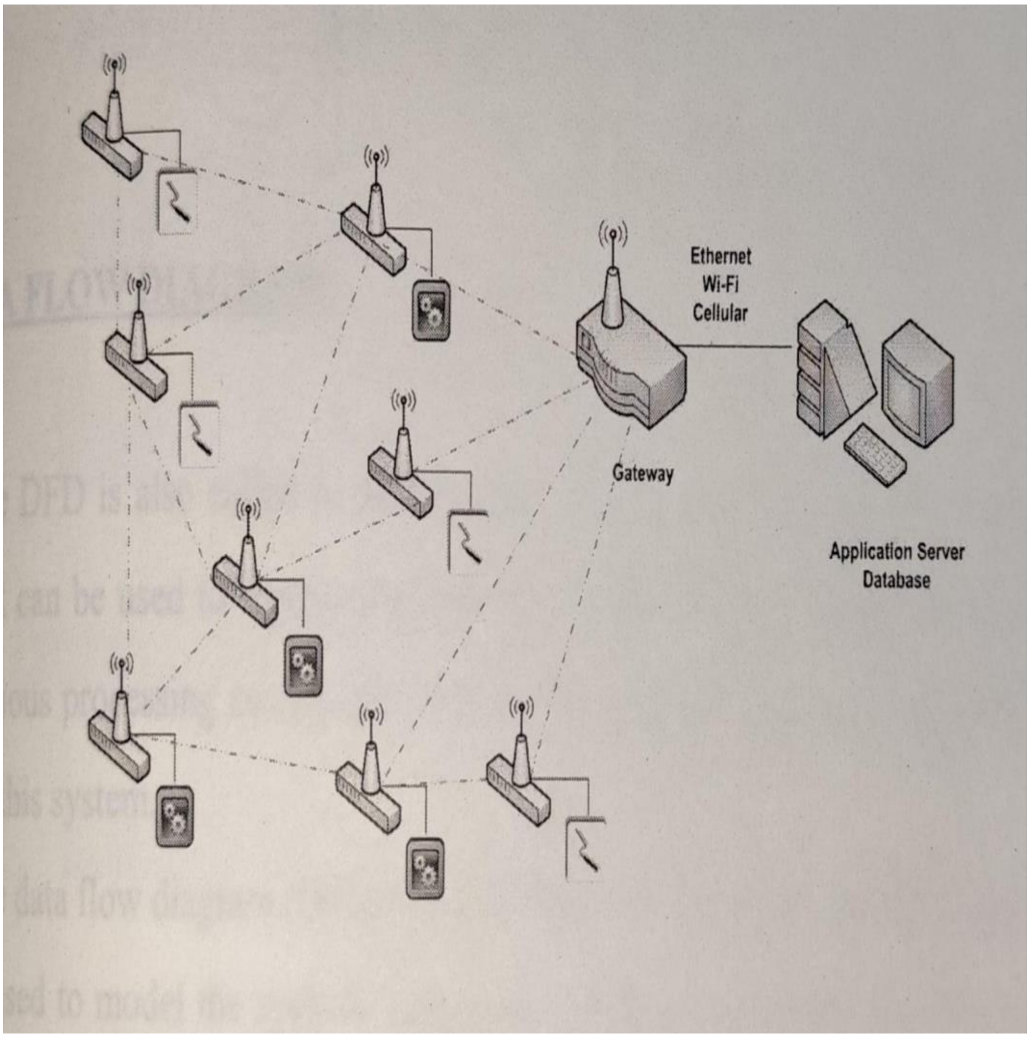
Output Design:

Output design is crucial as it determines how processed information is communicated to users and other systems. High-quality output meets end-user requirements and presents information clearly. Effective output design helps users make informed decisions and enhances the system's usability. The process involves:

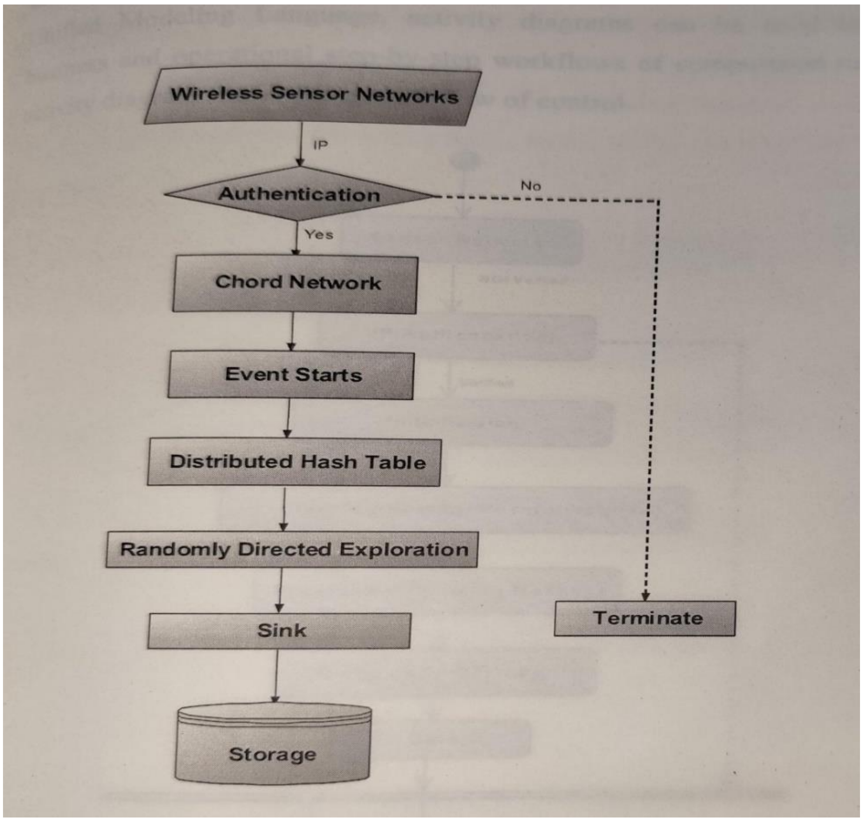
1. Identifying specific output needs to meet user requirements.
2. Selecting appropriate methods for presenting information.
3. Creating documents, reports, or other formats to display the information produced by the system.

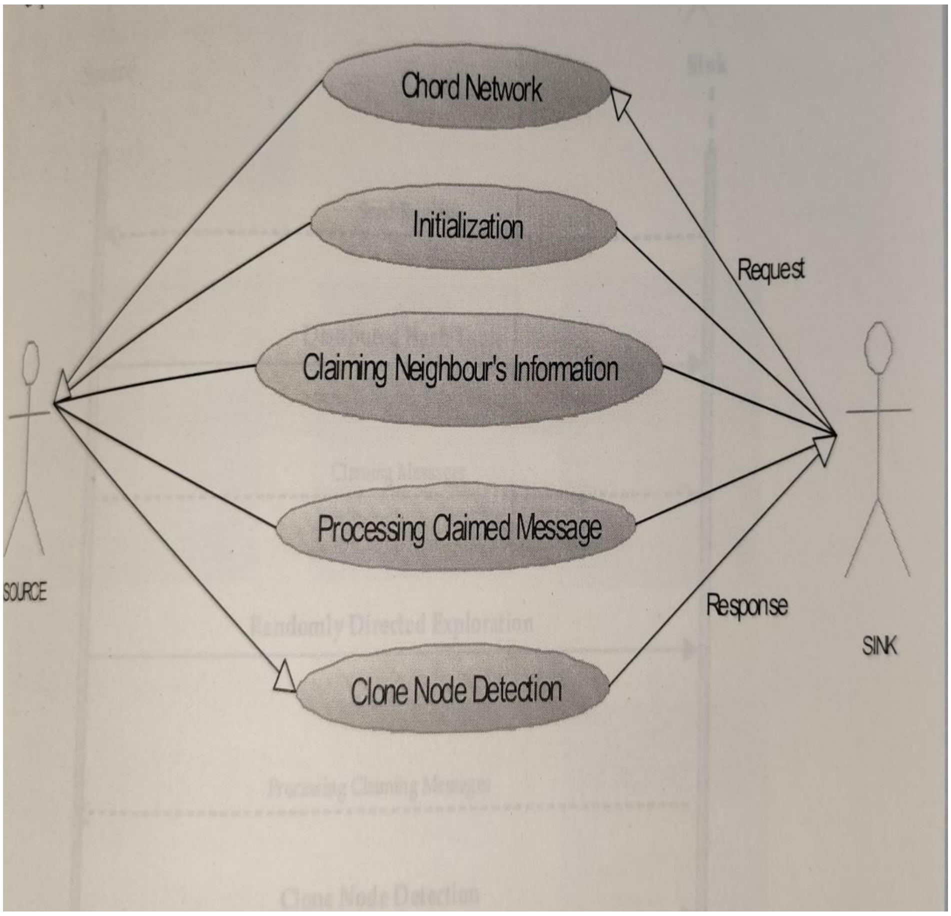
The design of computer outputs should be systematic and well-thought-out to ensure that users can easily and effectively utilize the system.

Architecture:

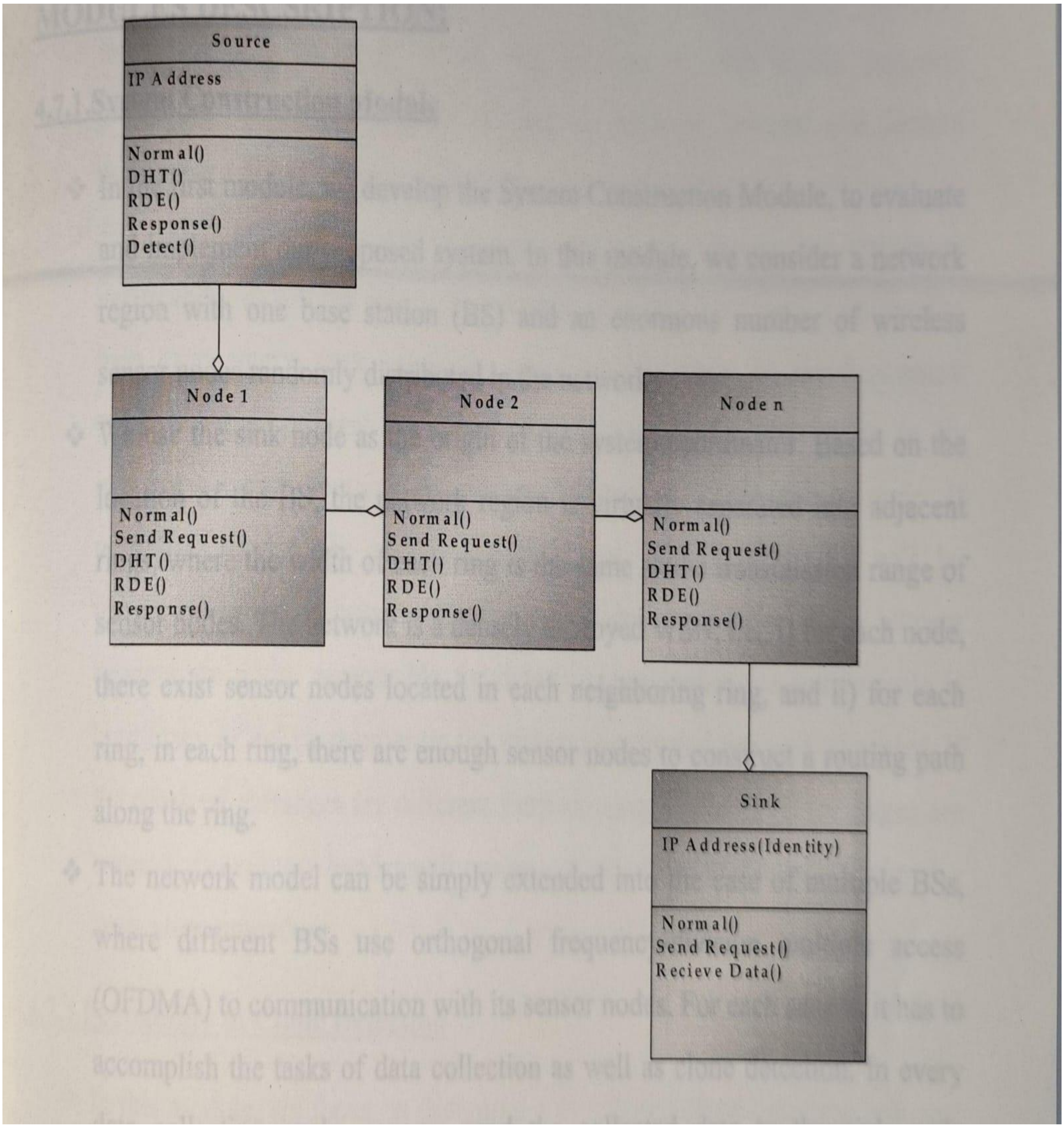


Flow Diagrams:





Class Diagram:



Conclusion:

In this work, we have introduced a distributed, energy-efficient clone detection protocol that utilizes random witness selection. Specifically, we developed the Energy-Efficient Ring-Based Clone Detection (ERCD) protocol, which encompasses both witness selection and legitimacy verification stages. Our theoretical analysis and simulation results indicate that the ERCD protocol can detect clone attacks with near certainty, thanks to the ring structure distribution of witnesses which facilitates efficient verification messaging.

Moreover, our protocol enhances network longevity and optimizes total energy consumption while maintaining a reasonable data buffer storage capacity. By leveraging location information to distribute the

traffic load across the wireless sensor networks (WSNs), we alleviate the energy consumption and memory demands on sensor nodes near the sink node, thereby extending the network's operational lifespan.
For future research, we plan to explore various mobility patterns under different network scenarios to further enhance the protocol's robustness and efficiency.

Reference:

1. Z. Zheng, A. Liu, L. X. Cai, Z. Chen, and X. Shen, "ERCD: An energy- efficient clone detection protocol in WSNs," in Proc. IEEE INFOCOM, Apr. 14- 19, 2013, pp. 2436-2444.
2. R. Lu, X. Li, X. Liang, X. Shen, and X. Lin, "GRS: The green, reliability, and security of emergingmachine to machine communications," IEEE Commun. Mag., vol. 49, no. 4, pp. 28-35, Apr. 2011.
3. 1. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: A survey," Comput. Netw., vol. 38, no. 4, pp. 393-422, Mar. 2002.
4. A. Liu, J. Ren, X. Li, Z. Chen, and X. Shen, "Design principles and improvement of cost function based energy aware routing algorithms for wireless sensor networks," Comput. Netw., vol. 56, no. 7, pp. 1951-1967, May. 2012.
5. T. Shu, M. Krunz, and S. Liu, "Secure data collection in wireless sensor networks using randomized dispersive routes," IEEE Trans. Mobile Comput., vol. 9, no. 7, pp. 941-954, Jul. 2010.
6. P. Papadimitratos, J. Luo, and J. P. Hubaux, "A randomized countermeasure against parasitic adversaries in wireless sensor networks," IEEE J. Sel. Areas Commun., vol. 28, no. 7, pp. 1036-1045, Sep. 2010.