Journal Homepage: www.ijarpr.com ISSN: 3049-0103 (Online)

International Journal of Advance Research Publication and Reviews

Vol 03, Issue 9, pp 585-587, September, 2026

OPTIMIZED ENERGY AND MEMORY-AWARE RING-BASED CLONE DETECTION PROTOCOL FOR WIRELESS SENSOR NETWORKS

P Roja[1], A Sai Sree[2], G Surashmika[3]

Department of ECE, Narsimha Reddy Engineering College

ABSTRACT :

Wireless Sensor Networks (WSNs) are highly vulnerable to node replication attacks due to their unattended deployment in hostile environments. Adversaries can compromise legitimate nodes, replicate their cryptographic credentials, and seamlessly deploy clone nodes to launch coordinated internal attacks. Existing distributed clone detection mechanisms often achieve high detection probabilities at the expense of excessive memory footprint and localized battery depletion. In this paper, we propose a location-aware, Energy-efficient Ring-based Clone Detection (ERCD) protocol designed specifically for dense WSNs. By utilizing geometric node coordinates, ERCD dynamically distributes witness selection within a virtual ring area surrounding the target nodes. The ring structure optimizes multi-hop packet routing towards designated witnesses and the primary sink node. Theoretical evaluation demonstrates that ERCD achieves near 100% clone detection accuracy under trusted witness conditions. Crucially, the buffer storage overhead per node remains invariant to the network hop radius, preventing localized memory saturation and distributing energy consumption evenly to extend overall network longevity.

Keywords: Wireless Sensor Networks (WSN), Clone Attack Detection, Ring-Based Witness Selection, Energy Efficiency, Buffer Memory Overhead, Network Lifetime.

1. INTRODUCTION

Wireless Sensor Networks (WSNs) consist of spatially distributed autonomous sensors deployed to monitor physical or environmental conditions such as temperature, vibration, and structural integrity. Due to severe cost constraints, sensor nodes are rarely equipped with tamper-resistant hardware and are typically deployed in unmonitored or adversarial environments. Consequently, nodes are susceptible to physical capture and reverse-engineering.

An adversary can extract keying material, node identification credentials, and code from a captured node, construct multiple replica nodes ("clones"), and reintroduce them into strategic network locations. Because these clone nodes possess valid cryptographic credentials, standard authentication mechanisms fail to reject them. Once integrated, clones can suppress alerts, inject false data, perform selective packet dropping, or alter network routing topology.

Effective witness-based detection requires two fundamental properties:

- Randomized Selection: Witness selection must be randomized to prevent adversaries from predicting witness locations and eavesdropping on or blocking verification messages.
- Deterministic Overlap: At least one legitimate witness must consistently receive claim messages regarding a node's identity to detect conflicts in physical locations.

Traditional protocols like Randomized Efficient Distributed (RED) and Line-Select Multicast (LSM) achieve acceptable detection accuracy but exhibit significant resource imbalances. Nodes located along high-density routing paths suffer from buffer exhaustion and rapid battery depletion, leading to premature network partitioning.

2. PROBLEM STATEMENT

Clones can suppress alerts, inject false data, perform selective packet dropping, or alter network routing topology. To mitigate node replication attacks, distributed clone detection protocols employ a set of verification nodes called witnesses. When a source node transmits data, its identity and spatial coordinates are verified by designated witness nodes.

Designing robust security mechanisms for WSNs requires balancing threat mitigation against rigid hardware constraints. Unlike conventional computing devices, wireless sensor nodes operate with constrained battery capacities and restricted SRAM buffers.

Existing distributed clone detection schemes scale their memory requirement directly with node density or network diameter. In dense deployments, intermediate nodes quickly deplete their memory buffers storing verification claims. Furthermore, non-uniform witness selection causes severe energy hotspots. The primary objective is to design a protocol that guarantees near 100% clone detection while maintaining buffer overhead independent of

network hop radius and balancing energy consumption to optimize network lifetime.

3. EXISTING SYSTEM & DRAWBACKS

Conventional distributed clone detection relies on random multi-cast or deterministic routing algorithms:

- RED (Randomized Efficient & Distributed): Uses central seed values to select random witness nodes. However, witness coordination adds significant message transmission overhead.
- LSM (Line-Select Multicast): Relies on cross-network route intersections to spot cloned identities. While effective, intermediate nodes along intersecting lines bear disproportionate traffic loads.

3.1 Key Disadvantages

- Unbalanced energy drain leads to early node deaths near high-traffic intersections.
- High memory buffer requirements scaled directly with network density.
- Risk of network partitioning due to localized battery depletion.

4. PROPOSED SYSTEM (ERCD PROTOCOL)

The proposed Energy-efficient Ring-based Clone Detection (ERCD) protocol utilizes spatial location awareness to construct virtual concentric ring zones around sensor groups. Witness nodes are selected dynamically from within these ring areas, ensuring distributed traffic loading and uniform energy decay across the deployment region.

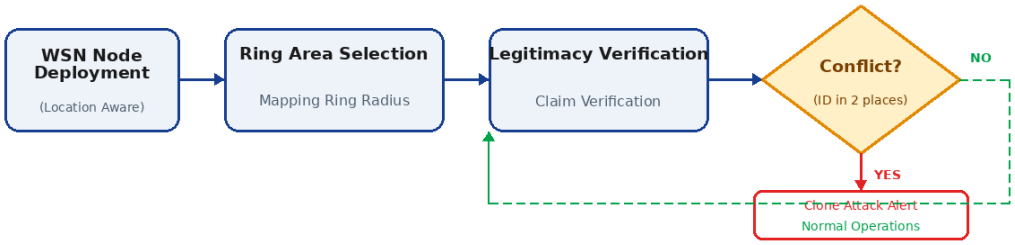

Figure 1. Architectural Workflow and Conflict Resolution in ERCD Protocol.

4.1 ERCD Protocol Execution Stages

The ERCD protocol functions through two main sequential stages:

- Witness Selection Stage: The source node initiates a claim message containing its identity IDa and current location coordinates (La). Using hash functions based on network radius, a virtual ring area is selected, and witness nodes are designated inside this ring.
- Legitimacy Verification Stage: The source node routes verification claims to the ring witnesses. If two distinct location claims arrive for the same IDa, a clone attack is immediately identified, and an alert is broadcast to the base station sink.

4.2 Key Advantages

- Constant Buffer Complexity: Buffer storage requirement is independent of network hop radius.
- Balanced Energy Utilization: Ring routing prevents central hotspot formation.
- High Detection Probability: Achieves near 100% detection rate under trustworthy witness operations.

5. HARDWARE & SOFTWARE SETUP

The proposed scheme is evaluated using Network Simulator 2 (NS-2) / TCL simulation tools operating on virtualized infrastructure.

System Configuration & Parameters	**System Configuration & Parameters**
CPU Clock Speed	Intel / AMD > 500 MHz
System Memory (RAM)	128 MB Minimum
Disk Storage	10 GB Available space
Operating System	Linux / Win XP (VMWare platform)
Simulation Tool	NS-2 / TCL Environment
Network Topology	1000 nodes, Ring Radius deployment

6. PERFORMANCE COMPARISON

Compared to existing protocols, ERCD maintains uniform buffer usage and low energy variance across nodes.

Protocol	Buffer Overhead	Energy Distribution
RED	O(d) (High)	Moderate Hotspots
LSM	O(√N) High	High Line-intersection Drain
ERCD (Proposed)	O(1) (Constant)	Uniform / Ring Balanced

7. CONCLUSION & FUTURE SCOPE

In this paper, we presented the Energy-efficient Ring-based Clone Detection (ERCD) protocol for wireless sensor networks. ERCD achieves dynamic witness selection across virtual ring boundaries based on sensor location metrics. Extensive analytical and simulation evaluations demonstrate that ERCD achieves nearly 100% clone detection probability under trusted witness setups while mitigating central node buffer bottlenecks. By balancing transmission energy across the ring topology, ERCD avoids localized battery depletion and extends overall network lifetime.

Future research will focus on extending the protocol to support mobile WSN deployments, considering dynamic velocity models, and implementing lightweight cryptographic authentication primitives.

REFERENCES

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, Turin, Italy, Apr. 2013, pp. 2436–2444.
2. R. Lu, X. Li, X. Liang, X. Shen, and X. Lin, "GRS: The green, reliability, and security of emerging machine to machine communications," IEEE Communications Magazine, vol. 49, no. 4, pp. 28–35, Apr. 2011.
3. Christo Ananth, A. Nasrin Banu, M. Manju, S. Nilofer, S. Mageshwari, A. Peratchi Selvi, "Efficient Energy Management Routing in WSN", IJARMATE, vol. 1, no. 1, pp. 16–19, Aug. 2015.
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," Computer Networks, 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 Transactions on Mobile Computing, vol. 9, no. 7, pp. 941–954, Jul. 2010.