ISSN 1330-3651 (Print), ISSN 1848-6339 (Online)

https://doi.org/10.17559/TV-20230508000613
Original scientific paper

Deployment with Location Knowledge by Multi Area Approach for Detecting Replica Nodes in Wireless Sensor Network

Suma Sira JACOB*, Balasubramaiam KARTHIKEYAN, Thiraviasami JOHNPETER, Rengaswamy JAYAMALA

Abstract: The Wireless Sensor Network (WSN) is important for the safety of network security. Numerous scholars have documented fundamentally fundamental attacks of various kinds in the WSN up to now. Replica nodes are identified using a range of replica node identification techniques. Although the replica is certain as a witness node, these approaches have poor detection precision and incur overhead control. This paper looks at the Multi Area Method (MAA) Replica Identification with Deployment with Location Knowledge (DLK) used. Initially, the nodes are clustered together and routed via the Low Energy Adaptive Clustering Hierarchy (LEACH) protocol. Several forms of node duplication identification protocols have now been proposed. Moreover, a single failure point located in clustered protocols, dispersed replications, is never identified by local protocols. Geographical positions are identified by the distributed protocols needed for the nodes. Deployment information utilising the position cluster detection method is suggested to avoid a node replica strike. Based on the deployment performance, the suggested model is compared to Area Based Cluster move towards (ABCD) and Fingerprint-based detection techniques. The proposed methodology offers excellent performance compared with other standard methods. Moreover, the energy consumption for RN detection was only 34 kWh.The proposed work provides optimal results for existing attacking strategies in cases of high detection higher detection percentage with a minimized Delay and increased communication overhead.

Keywords: clustering; knowledge discovery technique networking; replica detection; wireless sensor networks (WSN)

1 INTRODUCTION

WSNs play a crucial role in ensuring network security and safety. However, various fundamental attacks have been documented in WSNs, including replica node attacks, which involve the creation of cloned nodes to disrupt network operations. Existing replica node detection modus operandi often suffer from poor detection precision and high overhead control. To address these challenges, this paper proposes a multi-area approach (MAA) for replica node identification in WSNs, incorporating Deployment with Location Knowledge (DLK) [1-3].

WSNs consist of small sensing devices distributed throughout an area, capable of collecting data such as temperature, air pressure, and humidity. The collected data is transmitted to a central position for analysis. While WSNs are known for their networking capabilities, flexibility, and low power consumption, they are vulnerable to both external and internal threats, including replica node attacks. In a replica node attack, malicious nodes replicate existing nodes using their ID and main values, compromising the network's integrity. These replicated nodes, also known as clones, are distributed across the network, leading to network malfunction and security breaches [4-7].

In the context of WSNs, there are static networks where sensor nodes have fixed locations and mobile networks where nodes can change their locations over time. Detecting replica nodes is relatively straightforward in static WSNs as each node has a unique location ID. However, it becomes challenging in mobile WSNs where node IDs change with their changing locations. Therefore, several detection techniques have been proposed specifically for mobile WSNs [8-10].

The LEACH protocol is widely used for routing and data aggregation in WSNs. However, existing replica node detection methods have limitations, such as high communication overhead and the inability to detect dispersed replications in clustered protocols. Additionally, geographical position information is crucial for distributed protocols in identifying replica nodes. This paper suggests utilizing deployment information and a position cluster detection method to prevent replica node attacks [10-13].

2 RELATED WORKS

Shital Patil and Sangita Chaudhari [14] proposed a broad application in data transmission and data gathering with the aid of a wireless network. Due to the shortcomings of Wireless Sensor Networks (WSN) and the associated safety risks, the most prevalent attack scheduled on these sensor nodes is the Denial of Service (DoS) attack. Several attack prevention procedures are employed alongside DoS attacks in WSN. Various distinctive methods are utilized to avert DoS attacks in WSNs. An invulnerable framework was proposed for preventing DoS attacks on WSN, aiming to enhance attack prevention accuracy. This system recognizes different DoS attacks and reduces the false alarm rate.

The authors (BhavinRana and DhavalRana et al. 2017) [15] discussed effective routing techniques which consolidated the improved version of AOMDV and LEACH. The LEACH is utilized for the generation of clusters and offers data identified with the node's energy, but the specific node energy is superior to the LEACH selection of that node for transmitting information. The multipath routing utilizes AOMDV. Similarly in MANET, the proposed approach gives low communication overhead with low energy.

The Single Hop method was proposed by L. S. Padmavathi [16] in the year of 2015. The selection of the right witness node aids the detection of clones in the Clonal Selection algorithm. Moreover, the high throughput, minimum control overhead and maximum detection ratio are the advantages of this method. NRA is an important concept. The adversary to clone them acquires the physically insecure nodes that contain the identical individuality of the captured node. Throughout the network, the adversary organizes a random number of replicas. Based on Mobile Wireless Sensor Networks, replica node detection is a significant challenge issue.

For static WSNs, assume the boundaries of centralized detection methods. Ze Wang et al. 2017 [17] proposed a few of the distributed solutions. The author proposed global and local detection schemes for facilitating contradictory conflict identification. Being small compared to the entire area of deployment, the local area performs local detection that enhances the contradictory nodes meeting probability. Global detection effectively detects the remote nodes that are replicated in a wide area.

Parrno and his team were the first to discuss the WSN replica node attack. Randomized solve the issue. The randomized Multicast method sends signed location claims to the witness nodes that are chosen at random for consistency validation [18]. A node is found to be replicated if it claims two different locations. The enhanced line-selected method minimizes the communication overhead that occurs due to the randomized multicast scheme location claim transmission as each claim relay node participates in the detection of replicated nodes and the revocation process. Anyhow, the communication and computation overhead will be large since the multicast-based method and its variants frequently claim the locations in the entire network's lifetime. In this method, detection of replication is done based on the knowledge of group deployment where location claim is needed only from the external group node and hence this achieves optimal resource efficiency.

Zhu [19] and his team developed a method for detecting replication in which detection of replication is done by multicasting location claim to single or multiple cells and it works based on the grid cell topology. It has the main advantage of improved accuracy of detection but the communication overhead remains the same [20]. The proposed method in this paper achieves the same detection accuracy as Zhu and team's proposed method but with very minimum communication overhead [21].

Choi and group [22] presented a regionalized deployment-based local replica detection method for sensor networks. Here the entire network is considered as a subset of non-overlapping sub-regions and each sub-region has an exclusive subset. The non-empty intersection of the subsets indicates the presence of replicas. Yet still, the hacker can use other techniques to place the replicas where Choi's work fails in detection.

Ho et al. [23] designed a novel method for replica detection based on knowledge of group deployment and the idea is claimed. This method allows the sensor nodes within the home region to transmit messages ordinarily with no security protocol, whereas it needs authentication of location claim by the external zone node to transmit the message. As only external nodes are required to claim the location authentication, this method reduces the communicational, computational, and memory overheads. This method believes that every node is aware of its location through local protocols and the performance of detection is based on the local protocols' accuracy. Deployment of a localization scheme in the sensor node that has resource limitations is very expensive and it is difficult to provide accuracy in localization due to various WSN uncertainties. Also, the application of localization might bring additional threats to WSNs since the present localization methods may be vulnerable to security [24]. The proposed method in this article presents high security, and effective detection of replicas with less overhead of communication, computation and memory.

Khedim et al. [25] proposed a protocol that aims to mitigate the independence of the GPS and beacon node. MCD refers to a hybrid protocol that uses patrol robots and honeypots for detecting replicated nodes in a static sensor network, but this method needs more deployment cost as the hardware included is highly expensive. It also needs periodical examination of the nodes for the complete lifetime of the network. On the other hand, this method establishes the detection process only on demand and it is limited to local regions only.

An intrusion detection algorithm for addressing the replication attack in a clustered WSN based on N-LEACH, a novel clustering protocol [26]. The major advantage here is that the scheme could be configured according to the desired performance through the selection of the right function for encoding. Yet still, this method needs the random witness node to be chosen from the network for undertaking highly intensive computations and tasks that are energy-consuming and such witness nodes run out of energy very quickly.

Ho and team [27] proposed a deterministic QBM (Quorum-Based Multicast) and SLSM (Star-Shape Line-Selected Multicast) including a node replication detection method. But this method needs iterative claim check which leads to huge communication overhead.

Apart from all these, the Sybil attack [28] is considered a broader form of NRA (Node Replication Attack). A security protocol to resist the Sybil attack by combining trust-based algorithms exploring various techniques of reputation. This combined trust-based algorithm exhibits comparatively optimal results in opposing a Sybil Attack in a Kademlia network. A moving average exponential model for replica node assault in WSN. For a static timetable, low resource usage is accomplished and computing overhead is often reduced with this method. The recognition of multi-dimensional network replica nodes [29-32]. The analyst served mostly with the IoT networks have established a protection measure to secure the WSN from a comprehensive hybrid mechanism replica node attack. By implementing hybrid methods, QoS was strengthened, and the findings examined how the hazard was resolved in the area.

Parno and team proposed two protocols that use symmetric-key cryptography effectively for recognizing clone nodes compared to asymmetric-key cryptography. Randomized Multi-cast (RM) protocol is the first protocol, where the witnesses are chosen at random. The existence of a huge number of nodes confuses the malicious node to point out the right witness in WSN. On a node announcing its location, the witness will receive the claim from its neighbour and if the ID is from a different location then the witness floods a warning message to the entire network and revokes the D. The second protocol was Line-Selected Multicast (LSM). It minimizes the cost of communication further. Once the node announces the location claim, the randomly chosen witness receives the forwarded location claim. The location claim with the forwarding path is also stored in the buffer of each node. The replication nodes are observed at the intersection of the two straight lines shown in Fig. 1.

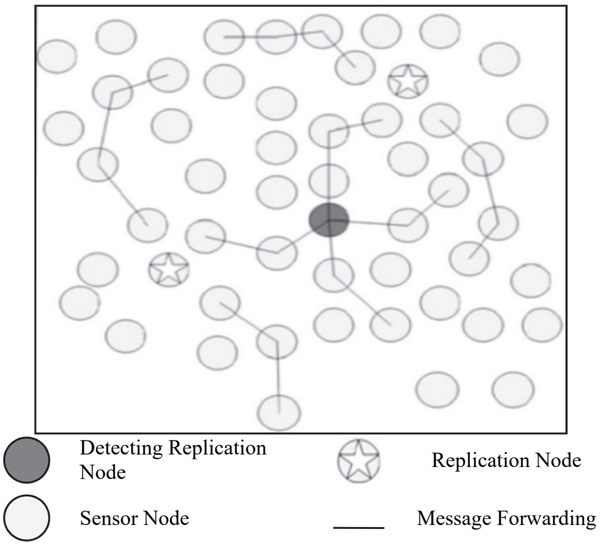

Figure 1 Representation of replica node

3 PROPOSED METHOD

A passive attacker listens in on the channel and may intercept the packet carrying the unknown data as it travels from its source to its destination. One base station, different arrangement of sensor nodes and sever is enveloped virtual topology network. The LEACH protocol utilizes the view of different portable networks and these nodes are gathered. Based on node mobility, more valuable detection protocols for mobile networks. Detection efficiency decreases with the decrease in the moving speed of the node. The proposed method aims to enhance detection accuracy by choosing the right node as a witness. As the replica nodes are detected and eliminated the wireless sensor network becomes small. If the adversary captures additional nodes with protocol must provide robust detection. Each protocol is effectively evaluated. In any operation, at least an order of magnitude is the basic requirement of communication among nodes. The principle thought in LEACH is amid the route discovery method to figure out numerous paths for contending link failure. With the help of Cluster Head Detect the strange conduct nodes, this attacker enters sensor network topology and attacks the network as an outer attacker, interior attacker or a bargained inside attacker and causes pernicious exercises like giving fantasy as the briefest way neighbours perform Denial of Service, performs interruption in routing. For the detection process Deployment with location knowledge (DLK) technique was utilized for clone node Prediction.

Network Model.

This part of the paper elaborated on the heterogeneous network model. There is N_{tot} node quantity of $X \times Y$ region in random distribution. The quantity of nodes every cluster has is N_{cls}. Every Ncls is distributed at random. The *cls* holds the value between 1 to q and now q is substituted with 4. Clusters are formed by dividing the main region into four sub-regions, and the shape of the clusters thus formed could be either square or rectangular based on the requirement of network design. This pattern of deployment is best suited for well-defined geographical locations and could be highly effective for places having great value.

The information is transmitted to BS from nodes. It is proposed in [10] that every node is nomadic within the corresponding clusters and hence change is observed in the network topology.

Depending on the energy, the network is divided into homogenous and heterogeneous networks. A homogenous network has nodes with similar energy levels. In a heterogeneous network, the nodes will be of different energy levels. This paper considers the heterogeneous network. The entire network is divided into two based on the node's energy level. Nodes having high energy levels are termed advanced nodes and nodes with low level energy are termed normal nodes where the advanced nodes are in m percentage. The energy of advanced nodes is multiplied by normal node energy. E_{cls} refers to the initial energy of every cluster. The equation for computing the energy for clusters with two levels of energy is as [6]:

$$E_{cls} = N_{cls}E_0(1-m) + N_{cls}mE_o(1+a) \tag{1}$$

Where, E_0 - Initial energy of normal node, $(1-m)$ N_{cls} is the total sum of normal nodes. N_{clsm} is the number of advanced nodes and $E_0(1+a)N_{cls}$ is the corresponding energy that shows that exists in the cluster.

Hence the energy cluster after manipulation is:

$$E_{cls} = N_{cls}E_0(1+a_m) \tag{2}$$

The initial energy of the entire region is obtained through the summation:

$$E_{Total} = \sum\nolimits_{cls=1}^{q} E_{cls} \tag{3}$$

Here, q represents the total cluster quantity.

After deployment, the typical two-dimensional static sensor network is the proposed scheme and every node handles its location. Each bidirectional link in the network communicates with all links, which is the ordinary present senior network generation. The public and private key pair based on new identity is generated and it requires BS cooperation. The adversaries never generate sensors with new identities but it never generates the key pair corresponding to the identities.

LEACH Protocol.

The protocol of LEACH is the principal progressive routing protocol that suggests data fusion. In a clustering routing protocol, it is off point of reference criticalness. Routing methodologies and safety problems are incredible research confront These days in wireless sensor networks, quantities of routing protocols are proposed; however, the protocols are hierarchical protocols such as LEACH. The protocol principle point is the enhancement of the life expectancy of WSN (Wireless Sensor Network) by bringing down the power.

For the current round, the node is selected probabilistically despite whether to close a cluster head. The level of CHs wants to know the perception of its outstanding level of energy. This reality communicates a message that is promoted at a stage heard by all.

When it is its turn to transmit by each node. The cluster heads collect the messages from send the outcome to the BS, total this information and cluster individuals.

Every node is aware and as per the existing plan, CH gathers messages from every individual cluster and sums up and sends the result to the BS.

Cluster formation for Replication Detection.

Let the assumption be that N sensor nodes are present in a circular-shaped field which has a radius of L (m) and its distribution is uniformly random and independent deployment from every node. It is also under the assumption that all nodes have similar energy at the initial stage and similar sensing ability. The data sensed are sent to the BS through the routing protocol. Generally, BS is located in the border or outside the proposed sensor region. A cluster-based routing protocol divides the timeline into rounds. Every single round commences with the phase to set up and it comprises CH selection and control message communication. In every round, at the set-up phase, a random number of CHs is elected. The quantity of CH in every round is varied and it is k. With a thumb rule, traditional algorithms estimate the k value to be 5. Rounds, $r = 0, 1, 2,$ are clubbed together so that rounds from $r = 0$ to $r = N/k - 1$ form a GOR (Group of Rounds), and rounds from $r = N/k$ to $r = 2N/k - 1$ form another GOR, and so on. G is assumed to be the node set who have never been as CH within a single GOR. Hence in round r, node i ($i = 1, 2, ..., N$) selects to be CH with the probabilistic value of:

$$T_{i,r} = \begin{cases} \dfrac{k}{n-k\left(r, mod\ N/k\right)} & i \in G \\ 0, & Otherwise \end{cases} \tag{4}$$

Eq. (3) states that every node in the network will serve a CH at least once in a GOR. Selection of CH includes three steps to transmit control messages, (i) CH for this round broadcast advertisement (ADV) message; (ii) non-CH node transmits join-request (Join-REQ) message; and (iii) CH sends Time Division Multiple Access (TDMA) scheduling message to their member nodes. Here the set-up phase ends. Next is the steady-state phase where CH gathers, aggregates, and routes the data from the sensor among the clusters. Every node which is a member of the cluster will transmit the data to its CH followed by the data aggregation by the CH. Finally, the BS receives the aggregated data.

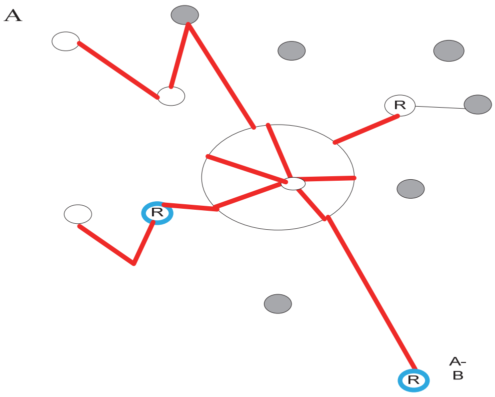

Figure 2 Replica node detection

The node replication detection is performed using a centralized approach. The node sent to the central trusted party is claimed by location. Every location claim to BS is sent with the help of the simplest solution. In the case of BS staying in a hostile atmosphere, certain claims of location might not reach it. Within its substructure, which serves as a conduit for information transfer between nodes, the cluster leader plays the role of facilitator.

At least two cluster leaders are directly next to the Gateway node. One cluster leader and another gateway node should take over once the clusters are no longer connected. The clustering technique stages that K-means use to aid data transfer are detailed below. The quantity of clusters is signified as k the input of K means clustering is considered as all nodes (n_1, n_2, ..., n_n). Some important steps involved in the cluster formation process are as follows:

Step 1: Select the number of k clusters.

Step 2: Point to the nearest cluster.

Step 3: partition the input data into k clusters by assigning each data y to the closest centroid v using any of the distance measures.

Step 4: Recompute the cluster centroids.

Step 5: Cluster head is chosen in the network. The technique of threshold is applied for the detection of malicious nodes from the network.

Proposed Multi Area Approach (MAA) RN identification.

At witness nodes, the location claims are collected in the proposed MAA method. The performance of node replication detection is enhanced using the centre node. When decreasing communication overhead, the single-point failure of a central node is avoided and the network lifetime is maintained. According to the maximum neighbour nodes method is to select the central node. The node in a network is defined using the maximum neighbour nodes model that contains the maximum amount of nodes in its range.

Deployment with Location Knowledge (DLK).

The additional knowledge and security performance are improved in this section. The group by group deploys the fundamental model that considers the sensor nodes. The deployment point that deploys each group is expected. Each group onto each sensor node, network operators load the pre-decided deployment coordinate before deployment. After deployment, the similar group with the sensor nodes are much more interested to close each other. The node replication is stopped by the proposed model. The infeasible point out to evaluate the security model that entirely removes the replicas from the network.

Detection Steps:

Set the network topology to its default values (Size between 1 and 500). With the proper threshold value in place, the base station may be permanently installed at a considerable distance from the sensors.

A Cluster contains nodes which are in the communication extent of each other. A node among sensor nodes goes about as an attacker. The attacker node has a capacity that senses data from the condition but does not transmit it to the cluster head or BS.

This attacker node may turn into a CH whenever. Cluster heads are selected by the sensor node.

At that point clusters are shaped, cluster heads are chosen and it turns into the obligation of the Base Station to recognize if any cluster head turns into an attacker. All the cluster heads are in the power of the base station.

Each Interval attacked node is checked and if the node is a Replica node the miss ratio is high contrasted with our fixed threshold value.

Check until all the nodes (up to 100) are in the network.

The Clone node attacks Several arrangements detection have been proposed every one of them is more centered around ad hoc networks that have more vitality and preparing limits. Attacks diminish the service quality of Internet administrations, hence it is imperative to apply countermeasures against Denial of Service attacks or even to just analyze them, and the primary essential advance is to identify such attacks. In this way, build up a compelling clone node attack detection framework for ensuring the network and resources of the client from the attacker.

Area Based Clustering Algorithm.

The proposed protocol makes the BS a fixed node in the middle of the playing field. All regions use a hierarchical clustering protocol in which nodes form their clusters and pick a CH to serve as the local base station. The nodes in the intermediate zone and the nodes in the advanced zone each choose themselves as CHs at a predetermined moment and then broadcast this fact to the other nodes in their respective zones. Each sensor node selects a CH depending on the amount of energy required to communicate with that CH. The CH is selected using a random weighted election probability formula based on the remaining node energy in each cluster zone. The CH provides a strategy for the communication of nodes existing in the cluster after all the clusters are organised. The node in the cluster picks up the information and sends it to the CH.

Radio components are disabled when not actively transmitting to reduce power lost to non-CHs. All the information is collected at the CH once and then sent to the BS all at once. Further, to decrease energy dissipation and extend network lifespan, CH utilises local merging of data for compressing the data being transported from CH to BS. Cluster heads are reset after each round to maximise the utilisation of all sensors. Each "round" of the protocol's operation consists of two phases: cluster setup and the steady-state phase. During the cluster setup phase, clusters are gathered together, and during the steady-state phase, data is sent from the CH to the BS. WSN performance and longevity are profoundly affected by the clustering design. The network's performance also suffers if the most distant sensor nodes die prematurely. An area-based protocol divides the sensing field into sections, where nodes are deployed in clusters and a cluster head (CH) is chosen. Separating the network's surface area improves communication and coverage for the most distant nodes.

They were made on the basic network model of area $A = X \times Y$ sq. mts, where $X = a$, $Y = b_1 + b_2 + b_3$, where $b_1 = b_3$ and $b_1 + b_2 + b_3 =$ a and the sensor nodes are placed accordingly. Every zone is separated and geographically is divided field for sensing. Exact energy-level sensor nodes are used according to the distance and purpose of the BS. Let m percentage of the total quantity of n nodes be equipped with α times of higher energy compared to normal node and termed as advanced node. Let b percentage of the total quantity of n nodes be equipped with μ times of higher energy compared to normal node and termed as intermediate node.

1. Zone$_1$ = $a \times b_1$, lying between $0 \leq Y \leq Y_1$ ¸ deployed with $n \times m/2$ static advanced nodes where 2. Zone$_2$ = $a \times b_2$, lying between $Y_1 = a \times m/2$

2. Zone$_2$ = $a \times b_2$, lying between $Y_1 < Y \leq Y_2$ ¸ deployed with b percentage of static intermediate node and $(1 - m - b) \times n$ normal node where $Y_2 = a \times Y_1$

3. Zone$_3$ = $a \times b_3$, lying between $Y_2 < Y \leq Y_3$¸ deployed with $n \times m/2$ static homogenous energy-rich advanced node where $Y_3 = a$.

The main is described as the furthest zone from the base station this guarantees the deterministic lifetime of the network and ensures the expiry of the entire node at the same period. In the homogenous zone, every node can act as CH. Even the failure of certain nodes will not have a serious effect on the operation of the scheme and hence the zone could admit such failures.

Psuedo Code for the proposed approach.

```
# Step 1: Initialization initialize network parameters, including node IDs, deployment information, and location knowledge
# Step 2: Cluster Formation
    perform clustering using the LEACH protocol
    for each node in the network:
        send a join request to the base station
        if a join request is received by a node:
            become a cluster head
            create a cluster and invite nearby nodes to join
        else:
     select the nearest cluster head and join the corresponding cluster
# Step 3: Deployment with Location Knowledge (DLK)
    for each cluster:
        determine geographical positions of the cluster head and member nodes
        calculate the distance between each member node and the cluster head
        assign location-based IDs to each member node based on its distance from the cluster head
# Step 4: Replica Node Detection
    for each cluster:
        for each member node in the cluster:
            broadcast node ID and location-based ID
            cluster head receives the broadcasted IDs and maintains a list of received IDs
        check for duplicate IDs in the received list
        if duplicate IDs are found:
            identify them as potential replica nodes
# Step 5: Replica Node Verification
    for each potential replica node:
        cluster head sends a verification request to the potential replica node
        potential replica node responds with its deployment and location information
        cluster head verifies the authenticity of the potential replica node
        if the potential replica node is verified as a replica:
   take appropriate actions such as isolation or removal from the network
```

4 RESULTS AND ANALYSIS

Parameter simulation in Network Simulator (NS2) is used to talk about the outcomes of the replica node discovery process, and IEEE 802.11b is related to the protocol. Tab. 2 displays the values used in the simulations. For this study work the maximum network size is regarded as 100 × 100 with 100 nodes. We have also tuned the network environment can dynamically increase the number of nodes.

Table 2 Simulation limits

S.No	Parameter	Value
1	size	100 × 100
2	Base station co-ordinates	x = 50 and y = 50
3	Etx and Erx	50 nJ
4	$\varepsilon f s$	100 pJ/bit/m^2
5	Number of nodes	100
6	Aggregation	5 nJ/bit/signal
7	Packet size of normal node (pn)	200 bits
8	Packet size of cluster head (pCH)	6400 bits
9	The initial energy of each node	1 J
10	Broadcast range	50

This proposed detection approach contrasted with other clustering strategies by enabling a few measures like the packet-to-delivery ratio (PDR) and Network lifetime (NLT), successful detecting replica and finally Energy consumption to be analysed.

Table 3 Packet Delivery Ratio of the projected scheme

No.of Nodes	Packet Delivery Ratio		
	DLK	ABCD	Fingerprint
100	45	56	75
200	55	58	78
300	58	59	82
400	60	62	82
500	70	75	85

The suggested model achieves the highest score across all methods (Fig. 3 for PDR and Fig. 4 for NLT), indicating that the routing protocol selects the trustworthy node.

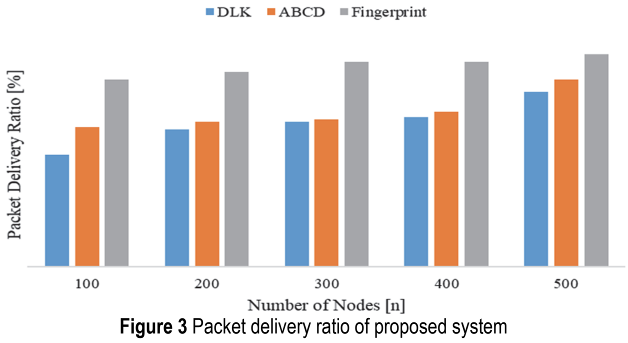

Figure 3 Packet delivery ratio of proposed system

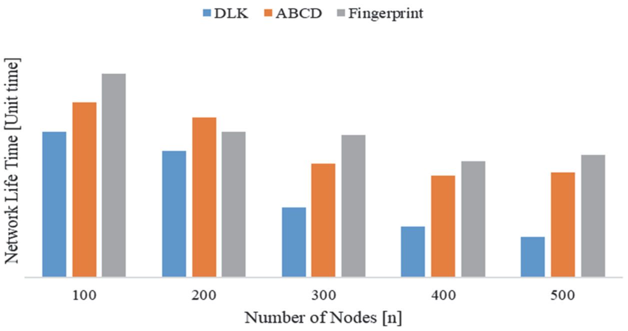

Figure 4 NLT analysis of the Proposed System

When constructing the wireless sensor network process to carry out data forwarding. While comparing all the parameters, the proposed clustering achieves 35% output and the PDR reaches 40%. Therefore, the route recovery scheme is used. When the speed increases, the consumption begins to increase in the route recovery process.

Table 4 NLT analysis of the projected system

No.of Nodes	NLT Analysis		
	DLK	ABCD	Fingerprint
100	100	120	140
200	87	110	100
300	48	78	98
400	35	70	80
500	28	72	84

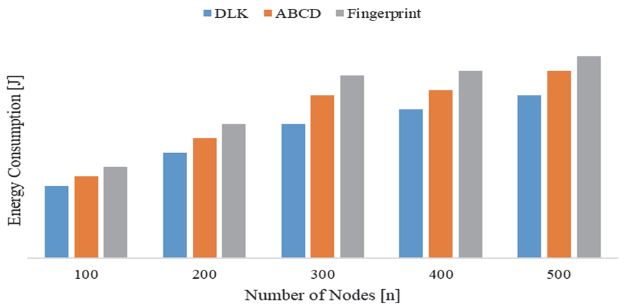

Figure 5 Energy Consumption of the Proposed System

Table 5 Energy Consumption of the Proposed System

No.of Nodes	Energy Consumption		
	DLK	ABCD	Fingerprint
100	15	17	19
200	22	25	28
300	28	34	38
400	31	35	39
500	34	39	42

Replica detection process results are shown in Fig. 6 by comparing different approaches. At the central node, the Centre and DLK technique collects entire location claims and hence the replicated node is easily detected.

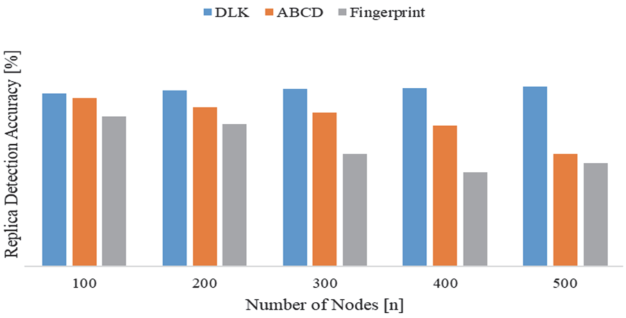

Figure 6 Replica detection accuracy of proposed system

The proposed DLK delivered better results than the ABCD approach. The relay node in the network claims the position of the distributed node. The intersection of the site claim in a relay node indicates the detection of the replicated node. A decrease in the drop of location claims by malicious nodes increases the probability of replica node detection by the central node. The presence of multiple witness nodes avoids the single-point failure of the central node. The proposed model produced a maximum detecting level of replica in DLK (92 TO 96%) compared with existing techniques.

Table 6 Detection Accuracy of the Proposed System

No.of Nodes	Replica Detection Accuracy		
	DLK	ABCD	Fingerprint
100	92.33	90.2	80.22
200	94.22	85.22	76.22
300	94.88	82.22	60.2
400	95.22	75.22	50.2
500	96.3	60.22	55.2

5 CONCLUSION

Both the LEACH procedure for detecting replicas and the MAA-based DLK method were described in this study. The fact that the DLK can identify replication assaults without location information is the major advantage of this study. Concerns regarding data security and privacy are at the heart of the issues with WSN. Managing clone node attacks in WSNs calls for creative measures to avoid them. In addition, the primary objective of this technique was to increase the sum of nodes, ensure the confidentiality of the transmission, and maximise the replica detection level on the clusters. In the case of duplicated nodes, the revocation process is never triggered. Claims messages may be corrupted on the way to their respective witness node. Other approaches provide far lower accuracy than the suggested one, which is 92.33 for 100 nodes and 94.22 for 200 nodes. Our proposed technique also outperforms the industry standard when comparing 500 nodes. The amount of power needed to detect RNs was only 34 kilowatt hours. The suggested approach gives optimal results for existing assaulting tactics in circumstances of high detection higher detection percentage with a minimised Delay and increased communication cost. Using metaheuristic algorithms, the study's scope may be broadened to encompass dynamic energy management.

6 REFERENCES

[1] Sharma, M. & Purohit, R. (2015). Node Replication Attack Detection Techniques in Wireless Sensor Network A Survey. *International Journal of Electrical, Electronics and Data Communication, 3*(8), 58-63. https://doi.org/10.18479/ijeedc/2015/v3i8/48356

[2] Dhamodharan, U. S. R. K. & Vayanaperumal, R. (2015). Detecting and preventing Sybil attacks in wireless sensor networks using message authentication and passing methods. *The Scientific World Journal*. https://doi.org/10.1155/2015/841267

[3] Arun Prakash, R., Salem Jeyaseelan, W. R., & Jayasankar, T. (2018). Detection, Prevention and Mitigation of Wormhole Attack in Wireless Ad Hoc Network by Coordinator. *Appl. Math. Inf. Sci*, *12*(1), 233-237. https://doi.org/10.18576/amis/120123

[4] Mani, G., Nivedhitha, V., Pradeep, N. S., Jayasankar, T., & Vinoth Kumar, K. (2020).Reliable Wormhole Detection System (RWDS) Based Secure Routing and Authentication for Environmental Monitoring. *Journal of Green Engineering (JGE)*, *10*(3), 734-749.

[5] Vinoth Kumar, K., Jayasankar, T., Eswaramoorthy, V., & Nivedhitha, V. (2020). SDARP: Security-based Data Aware Routing Protocol for Ad hoc Sensor Networks. *International Journal of Intelligent Networks*, *1*(2020), 36-42. https://doi.org/10.1016/j.ijin.2020.05.005

[6] Yan, J., Zhou, M., & Ding, Z. (2016). Recent advances in energy-efficient routing protocols for wireless sensor networks: A review. *IEEE Access*, *4*, 5673-5686. https://doi.org/10.1109/ACCESS.2016.2598719

[7] Leu, J. S., Chiang, T. H., Yu, M. C., & Su, K. W. (2015). Energy efficient clustering scheme for prolonging the lifetime of wireless sensor network with isolated nodes. *IEEE Communications Letters*, *19*(2), 259-262. https://doi.org/10.1109/LCOMM.2014.2379715

[8] Naruephiphat, W., Ji, Y., & Charnsripinyo, C. (2012). An area-based approach for node replica detection in wireless sensor networks. *2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications IEEE,* 745-750. https://doi.org/10.1109/TrustCom.2012.73

[9] Eswaramoorthy, V., Vinoth Kumar, K., & Gopinath, S. (2021). Fuzzy logic-based DSR trust estimation routing protocol for MANET using evolutionary algorithms. *Technical Gazette*, 28(6), 2006-2014. https://doi.org/10.17559/TV-20200612102818

[10] Byadgi, D., Prasad, A. M., & Suma, V. (2015). Network Management by Tackling Replication Attacks: A Comparative Study. *International Journal of Computer Applications*, *110*(6), 41-46. https://doi.org/10.5120/19324-1075

[11] Liu, G., Yan, Z., & Pedrycz, W. (2018). Data collection for attack detection and security measurement in Mobile Ad Hoc Networks: A survey. *Journal of Network and Computer Applications*, *150*, 105-122. https://doi.org/10.1016/j.jnca.2018.01.004

[12] Vinoth Kumar, K., Jayasankar, T., Prabhakaran M., & Srinivasan, V. (2017). Fuzzy Logic-based Efficient Multipath Routing for Mobile Adhoc Networks. *Applied Mathematics & Information Sciences*, *11*(2), 449-455. http://dx.doi.org/10.18576/amis/110213

[13] Gopinath, S., Vinoth Kumar, K., Elayaraja, P., Parameswari, A., Balakrishnan, S., & Thiruppathi, M. (2022). SCEER: Secure Cluster-Based Efficient Energy Routing Scheme for wireless sensor networks. *Material today proceedings*, *45*, 3579-3584. https://doi.org/10.1016/j.matpr.2020.12.1096

[14] Patil, S. & Chaudhari, S. (2016). DoS attack prevention technique in Wireless Sensor Networks. *Procedia Computer Science*, *79*, 715-721. https://doi.org/10.1016/j.procs.2016.03.094

[15] Vinoth Kumar, K. & Balakrishnan, S. (2023). Multi-objective Sand Piper Optimization Based Clustering with Multihop Routing Technique for IoT Assisted WSN. *Brazilian Archives of Biology and Technology*, *66*, 1-8. https://doi.org/10.1590/1678-4324-2023220866.

[16] Sindhuja, L. S. & Padmavathi, G. (2016). Replica node detection using enhanced single hop detection with clonal selection algorithm in mobile wireless sensor networks. *Journal of Computer Networks and Communications*. https://doi.org/10.1155/2016/1620343

[17] Wang, Z., Zhou, C., & Liu, Y. (2017). Efficient Hybrid Detection of Node Replication Attacks in Mobile Sensor Networks. *Mobile Information Systems*. https://doi.org/10.1155/2017/8636379

[18] Balakrishnan, S. & Vinoth Kumar, K. (2023). Hybrid Sine-Cosine Black Widow Spider Optimization-based Route Selection Protocol for Multihop Communication in IoT-Assisted WSN. *Technical Gazette*, *30*(4), 1159-1165. https://doi.org/10.17559/TV-20230201000306

[19] Zhu, B., Addada, V. G. K., Setia, S., & Jajodia, S. (2007). Roy S. Efficient Distributed Detection of Node Replication Attacks in Sensor Networks. *Proceedings of the Computer Security Applications Conference; Miami Beach, FL, USA,* 257-267. https://doi.org/10.1109/ACSAC.2007.26

[20] Conti, M., Pietro, R. D., Mancini, L. V., & Mei, A. (2007). A randomized, efficient and distributed protocol for the detection of node replication attacks in wireless sensor networks. *Proceedings of the ACM International Symposium on Mobile Ad Hoc Networking and Computing, ACM MobiHoc; Montreal, QC, Canada,* 80-89.

https://doi.org/10.1145/1288107.1288119

[21] Abinaya, P. & Geetha, C. (2014). Dynamic detection of node replication attacks using X-RED in wireless sensor networks. *Proceedings of the International Conference on Information Communication and Embedded Systems (ICICES2014); Chennai, India,* 1-4. https://doi.org/10.1109/ICICES.2014.7033957

[22] Thiruppathi, M. & Vinoth Kumar, K. (2023). Seagull Optimization-based Feature Selection with Optimal Extreme Learning Machine for Intrusion Detection in Fog-Assisted WSN. *Technical Gazette*, *30*(5), 1547-1553. https://doi.org/10.17559/TV-20230130000295

[23] Zanca, G., Zorzi, F., Zanella, A., & Zorzi, M. (2008). Experimental comparison of RSSI-based localization algorithms for indoor wireless sensor networks; *Proceedings of the Workshop on Real-World Wireless Sensor Networks; Glasgow, UK*, 1-5. https://doi.org/10.1145/1435473.1435475

[24] Farah, K. & Nabila, L. (2014). The MCD Protocol for Securing Wireless Sensor Networks against Node Replication Attacks. *Proceedings of the Proceedings of International Conference on Advanced Networking Distributed Systems and Applications, Bejaia, Algeria,* 58-63. https://doi.org/10.1109/INDS.2014.18

[25] Guo, C., Guo, S., Yang, Y., & Fei, W. (2015). Replication attack detection with monitor nodes in clustered wireless sensor networks. *Proceedings of the 2015 IEEE 34th International Performance Computing and Communications Conference (IPCCC), Nanjing, China,* 1-8. https://doi.org/10.1109/PCCC.2015.7410341

[26] Ho, Y. S., Ma, R. L., Sung, C. E., Tsai, I. C., Kang, L. W., & Yu, C. M. (2015). Deterministic detection of node replication attacks in sensor networks. *Proceedings of the 2015 IEEE International Conference on Consumer Electronics; Taipei, Taiwan,* 468-469. https://doi.org/10.1109/ICCE-TW.2015.7217002

[27] Vinoth Kumar, K. & Thiruppathi, M. (2023). Oppositional Coyote Optimization based Feature Selection with Deep Learning Model for Intrusion Detection in Fog Assisted Wireless Sensor Network. *Acta Montanistica Slovaca*, *28*(2), 496-508. https://doi.org/ 10.46544/AMS.v28i2.18

[28] Pecori, R. & Kademlia, S. (2016). A trust and reputation method to mitigate a Sybil attack in Kademlia. *Computer Networks*, *94*, 205-218. https://doi.org/10.1016/j.comnet.2015.11.010

[29] Eid, R., Muhammad, S., Syed, N., & Anwar, G. (2020). Polynomial-Based Dynamic Key Management for Secure Cluster Communication in Wireless Mobile Sensor Network. *Technical Gazette*, *27*(2), 358-367. https://doi.org/10.17559/TV-20170807075015

[30] Anitha, S., Jayanthi, P., & Thangarajan, R. (2020). Detection of Replica Node Attack Based on Exponential Moving Average Model in Wireless Sensor Networks. *Wireless Personal Communication.* https://doi.org/10.1007/s11277-020-07648-w

[31] Sunil Kumar, V. V. & Chandrasena, B. (2020). Replica Node: Detection of Node Replication in Multidimensional Networks. *International Journal of Recent Technology and Engineering (IJRTE)*, *8*(5), 2005-2008. https://doi.org/10.35940/ijrte.E5021.018520

[32] Devi, P. P. & Jaison, B. (2020). Protection of Wireless Sensor Network from Clone Attack using the SDN-Enabled Hybrid Clone Node Detection Mechanisms. *Computer Communications*, *152*, 316-322. https://doi.org/10.1016/j.comcom.2020.01.064

Contact information:

Suma Sira JACOB, Associate Professor
(Corresponding author)
Department of Information Technology,
Sri Krishna College of Technology, Coimbatore
E-mail: sumasarajacob@gmail.com

Balasubramaniam KARTHIKEYAN, Professor
Department of Information Technology,
Panimalar Engineering College, Chennai
E-mail: karthikeyan.b32@gmail.com

Thiraviasami JOHNPETER, Assistant Professor
Department of Computer Science and Engineering,
K. Ramakrishnan College of Engineering, Trichy
E-mail: johnthiraviam85@gmail.com

Rengaswamy JAYAMALA, Assistant Professor
Department of Computer Science and Engineering,
University College of Engineering (BIT Campus),
Anna University Tiruchirappalli
E-mail: jayamala_r@outlook.com