Available online at: http://www.advancedscientificjournal.com
http://www.krishmapublication.com
IJMASRI, Vol. 1, issue 1, pp. 299-303, Apr. -2025
https://doi.org/10.53633/ijmasri

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY ADVANCED SCIENTIFIC RESEARCH AND INNOVATION (IJMASRI)

ISSN: 2582-9130 **IBI IMPACTFACTOR 1.5** **DOI: 10.53633/IJMASRI**

RESEARCH ARTICLE

ENHANCED SECURITY IN WIRELESS SENSOR NETWORKS TO PREVENT CLONE ATTACKS

Mrs Prabavathi[1] N Vennila S[2] and Sathya R[3]
[1]*PG & Research Department, Department of Computer Science, St.Ann's College of Arts and Science, Tindivanam.*
Email: prabatamil18@gmail.com
[2]*Principal & Head of the Department, PG & Research Department of Computer Science, St.Ann's College of Arts and Science Tindivanam*
Email: sathiyaat@gmail.com
[3]*Assistant Professor & Head, Department of Computer Science, St.Ann's College of Arts and Science Tindivanam.*
Email: moulikrishna19@gmail.com

Abstract

The network nodes in wireless sensor networks are utilised to sense data from different kinds of inaccessible locations. Information from hostile environments has been sensed using wireless sensor nodes. Various kinds of sensors have been employed in the sends together data. Since every node has the same ID and is located at a different location at the same time, the main challenge here is identifying the node that is undergoing a clone attack.

Keywords: Clustering, WSN, Leachprotocol, Clusterheads

Introduction

WSN networks are made up of a potentially huge number of wireless sensor nodes with limited energy, memory, processing power, and communication range. [1] A wireless sensor network (WSN) is made up of several tens to thousands of sensor nodes that may store, process, and transmit the data they have sensed. A base station known as Sink is frequently included for further computing. It offers a wide range of possible uses and applications, including in the biomedical and military sectors, smart homes, remote monitoring of hazardous locations, environmental monitoring, and national defence. [2] WSN, multi-path routing technologies and key management have received increased attention. There are two types of key management: preallocation and centralised. The former is known as centralised key distribution, where each node and the base station share a pair of keys. We specifically deal with the so-called clone attack, a

basic, unique, and terrible security threat that mobile WSNs are vulnerable to. It entails duplicating and utilising the sensors that were taken in order to initiate a range of malevolent actions. Cloning the node ID and all of the cryptographic content connected to it is necessary when replicating a node [3]. Energy efficiency is a key design objective for wireless sensor networks. The rogue copy can talk with other nodes and be recognised as a genuine node thanks to the code that the tamped red no declined in to it. The attacker causes the min in a number of harmful ways when the cloned node sari is placed in the network. A clone might, for example, start a wormhole or a black hole.

Routing Protocols in WSN

Using a variety of strategies, such as data aggregation, clustering, data-centric approaches, etc., we can lower the energy consumption. The routing protocols fall into one of three categories: location-based, hierarchical, or flat.

Flat networks: This network uses equal numbers of nodes. Therefore, every node has the same function. There is no logical hierarchy in this network. Its addressing method is flat. Routing Information Protocol is an example of a flat network (RIP).

Hierarchical networks: The nodes are divided into several tiny groupings known as clusters. The coordinator of other nodes is the cluster head (CH) of each cluster. In order to lessen energy inefficiency, these CHs aggregate data. Cluster leaders are subject to change. The CH is the node with the maximum energy. One effective technique to reduce energy usage in a cluster is through hierarchical routing. Scalability, energy economy, effective bandwidth utilisation, and a decrease in packet collisions and channel contention are some of its main benefits. Hierarchical networks include Low were Adaptive Clustering Hierarchy (LEACH), Hybrid, Energy-Efficient Distributed Clustering (HEED) and others (20).

Location – based net works: The position of the sensor nodes is crucial in location-based clustering. Data is sent to a specific location using a base station. Understanding the location of the sensor nodes is crucial for these protocols in order to send data to the appropriate locations. The incoming signal strengths can be used to estimate the distance between nearby nodes. According to location- based protocols, nodes should shutdown to conserve energy if there is no activity. Location – Based Protocol Distance Routing Effect Algorithm for Mobility (DREAM) and Location – Aided Routing (LAR) are two examples. [10] The entire sensor net work is divided into clusters, which are groups of sensor nodes, with the cluster head being a high-energy node inside the cluster. The leader first strategy and the cluster first approach are the two methods employed in this procedure. The cluster head is chosen initially under the leader - first technique, and the cluster is there after established. The cluster head is chosen after the cluster has been formed, according to the cluster first approach.

LEACH Protocol

[4] The first notable advancements to traditional clustering techniques in WSN include the creation of the Low Energy Adaptive Clustering Hierarchy, or LEACH. LEACH aims to increase the lifespan of a wireless sensor network by reducing the energy needed to establish and sustain clusters. In the hierarchical LEACH protocol, the majority of nodes send data to cluster heads, which then compile and compress it before sending it to the base station (sink). Every round, a stochastic process is used by each node to decide if it will become the cluster head. [9] LEACH proposes that each node probabilistically become a cluster head in order to maintain balanced energy consumption and prevent collisions by using the time division multiple access (TDMA) principle. The remaining energy and other characteristics of the sensor nodes are not taken into account when choosing the cluster heads. For prounds, where P is the desired percentage of cluster heads, nodes that have previously served as cluster heads are not eligible to serve as cluster heads again. Every node thereafter has a 1/P chance of becoming the cluster head in every round. Every node that isn't a cluster head chooses the nearest cluster head at the conclusion of each round and joins that cluster. The two stages of the leach protocol's cluster formation are depicted in Figure 1.2.

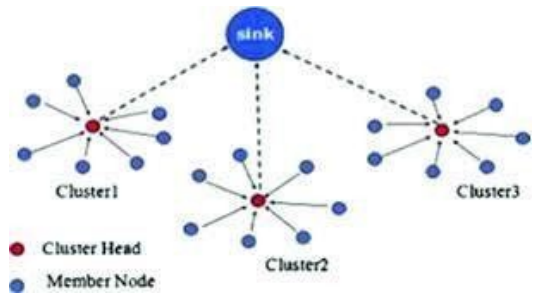

Figure1.2:Leachprotocol

1. **Phase of Setup:** [10] Cluster formation and cluster head selection comprise the setup step.

a. **Cluster formation:** After the sensor nodes are placed on a level surface, the entire region is split up into sectors, which resemble a rectangular grid. Sensor nodes are positioned so that there are an adequate number of high- energy nodes in each sector. A cluster of sensor nodes is formed by each sector.

b. **Cluster head selection:** The base station will connect to every sensor node and as certain its location and battery life. High- energy sensor nodes will be chosen by the base station to serve as cluster heads, and within each cluster, a cluster of cluster heads will develop. The cluster head with the highest energy level will be selected as the master. There will only be one master in the cluster at any given moment.

2. **Phase of Steady-state:** [9] Each non-CH node transmits data to its corresponding CH during this phase using its TDMA schedule. Upon receiving this data, a CH forwards it to the BS via its subsequent relay node. A non- CH node saves energy by going into sleep mode when its data transmission slot is over.

LiteratureReview

"Research on hierarchical mobile wireless sensor network architecture with mobile sensor nodes" was published in 2010 by Xuhui - Chen et al. [1]. The nodes in a standard wireless sensor network, such as users, sink nodes, and sensor nodes, are thought to be static. The network is set up using a single layer planner, which is unable to adjust to the application of mobile sensor nodes. The network architecture is covered first in this article, followed by an introduction to the typical wireless sensor network architecture and an analysis of the mobile sensor node application scenario.

The author suggested a wireless sensor network architecture that includes mobile sensor nodes.

"A secure routing with intrusion detection for clustering wireless sensor networks" was published in 2010 by Xiao Zhenghong et al. [2].

In order to identify potential clone as saults that could be launched to interfere with the system's regular operations, the authors of this research suggest a social proximity - based approach for a mobile health care disease control system. Our approach, which is based on social closeness, uses user relationships to detect clones. In particular, the author established novel metric know as community between that takes into account the community data of mobile users. "An approach to increase the wireless sensor network life time" was published in 2012 by N. Marriwala etal. [3]. Small devices known as sensor nodes, which are outfitted with sensors to track environmental and physical parameters including motion, speed, temperature, humidity and pressure, makeup a wireless sensor network. Since the wireless sensor network's nodes were battery-operated, one of the major problems with wireless sensor networks is that network sensor nodes have inherently limited battery power.

Reducing the energy consumption and restricted power sources of the sensor nodes is the primary challenge of wireless sensor networks, according to Md. Azharuddin et al.'s 2013 paper " A Distributed Fault tolerant Clustering Algorithm for Wireless Sensor Networks "[5]. Clustering is the primary technique to save energy usage and boost scalability. Because of the additional workload from data collecting, data aggregation, and communication to the base station, cluster heads (CHs) in a cluster - based WSN use more energy. Therefore, taking into account the energy consumption of the CHs, efficient cluster formation is quite difficult. After CH is destroyed, it ceases to function and all of the cluster's common nodes are unable to communicate.

"Wireless sensor networks for monitoring the environmental activities" was published in 2010 by Ruchi Mittal et al. [7]. Sensor networks have a long history, and a wide variety of sensor devices are employed in many real-world applications.

Methodology

The clone attack is the foundation of the suggested work. In a clone attack, the node duplicates the other node's ID and displays its predictions at various points. An enemy can employ a clone node in a variety of ways, including launching a wormhole or black hole attack. All valid nodes may receive erroneous information from this attack. The clone attack is ideal for the enemy. The attacker must not compromise the number of nodes in order to launch this assault. One node can be cloned by the attacker, who can then use it to anticipate additional nodes. At various times and places, it fabricates its positions. Since every node has the same ID and locations at different times, them a in challenge here is identifying the node undergoing a clone attack. Clusters that replicate have also been experiencing this issue, with the primary issue occurring during cluster head replication. The suggested algorithm's flow is shown in Figure 3.1.

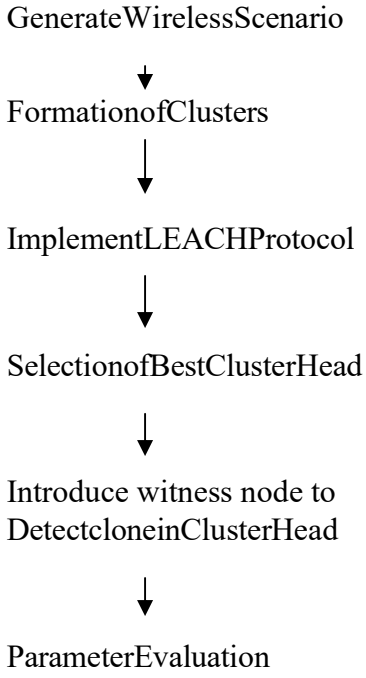

Figure3.1: Flow diagram for proposed work

Conclusion & Future Scope:

The current LEACH protocol extends the network's life span. The primary determinants of wireless sensor networks are fault tolerance, routing and energy consumption. The current work can determine the shortest way and boost node efficiency. However, because the clone node copies the transmitted node's ID and sends it to a different predicted location, the node is not secure during transmission. The suggested approach creates a witness node that can introduce and detect the clone node using a modified LEACH protocol. As a result, it is simple to locate the clone node, which raises each node's energy level throughout transmission. Due to the fact that the LEACH protocol operates on extra parameters, such as clone node detection, node energy consumption, node-to-node communication and network overhead during node transmission.

Future scope:

WSN has been incorporated into the proposed work. In the future, RSNs (Random Sensor Networks) can have any topology. This study can be applied in the actual world for wireless sensor network sensing and data transmission inthefuture.NS-2simulationtool, however in the future, simulations such as QUALNET, MATLAB, and others could be used to model this work.

References

1. Xuhui Chen, “Research on Hierarchical Mobile Wireless Sensor Network Architecture with Mobile Sensor Nodes”, International Conference on Biomedical Engineering and Informatics (BMEI), IEEE, ISSN 978-1-4244- 6498-2, Vol.56, IssueNo.14, pp.:2863–2867, China,2010.
2. Xiao Zhenghong, Chen Zhigang, “ASecure Routing Protocol with Intrusion Detection for Clustering Wireless Sensor Network”, International Forum on Information Technology and Application (IFITA), IEEE, ISSN 978-0- 7695- 4115-0,Vol.8,IssueNo.12,pp.:1253– 1258,China, 2010.
3. Marriwala, N. Rathee, P, “An Approach to Increase the Wireless Sensor Network Life time”, World Congress on Information and Communication Technologies (WCICT), IEEE,

ISSN 978-1-4673-4806-5, Vol.3, Issue No.6, pp.:495–499, India, July, 2012.

4. Md. Azharuddin et al [1] "A Distributed Fault-tolerant Clustering Algorithm for Wireless Sensor Networks", International Conference on Advance in Computing, Communication and Informatics (ICACCI), IEEE, ISSN 978-1-4673-6217-7, Vol.4, Issue No.12, pp.:23-33, India,2013.
5. Thander The in, "Increasing Availability and Survivability of Cluster Head in WSN", International Conference on Grid and Pervasive Computing Workshops (ICGPCW), IEEE, 2008, ISSN 978-0-7695-3177-9, Vol.45, Issue No.21, pp.:281–285, Korea, 2008.
6. Ruchi Mittal, "Wireless Sensor Networks for Monitoring the Environmental Activities" IEEE, ISSN 9781-4244-5967-4,Vol.5, Issue No.12, pp.:1–5,India,2010.

******