Volume 5, Issue 5, May 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Review of To Avoid Replication Attack in Clusters through Witness Node

Parveer Kaur
Dept of Computer Science Engg.,
Mtech Full Time RIMT IET, Punjab India

Abhilash Sharma
Assistant Professor of Dept of Computer Science Engg., RIMT IET, Punjab, India

Abstract - A wireless sensor network is a gathering of specific transducers with a correspondences foundation for observing and recording conditions at diverse areas. In this work we used LEACH Protocol to find the cluster heads & Sub cluster Heads. Low Energy Adaptive Clustering Hierarchy ("LEACH") is a TDMA-based MAC convention which is incorporated with bunching and a straightforward directing convention in remote sensor systems (WSNs). Problem of Energy consumption is occurred in the network, Which is reduce by using Leach Protocol.

Keywords: WSN, LEACH Protocol, TDMA, MAC.

I. INTRODUCTION

1.1WSN (Wireless Sensor Network)

A wireless sensor network is a gathering of specific transducers with a correspondences foundation for observing and recording conditions at diverse areas. Generally checked parameters are temperature, humidity, weight, wind direction and velocity, enlightenment force, vibration power, sound force, force line voltage, substance focuses, pollutant and basic body capacities. A sensor system comprises of various detection stations called sensor hubs, each of which is little, lightweight and versatile. Each sensor hub is outfitted with a transducer, microcomputer, handset and force source. The transducer produces electrical signs focused around sensed physical impacts and phenomena. The microcomputer courses of action and stores the sensor yield. The handset gets charges from a focal PC and transmits information to that PC. The power for every sensor hub is gotten from a battery.

1.2 Main terms in WSN

- **Sensor Node:** A sensor node is the core component of a WSN. Sensor nodes can take on multiple roles in a network, such as simple sensing; data storage; routing; and data processing.
- **Clusters:** Clusters are the organizational unit for WSNs. The dense nature of these net- works requires the need for them to be broken down into clusters to simplify tasks such a Communication.
- **Cluster heads:** Cluster heads are the organization leader of a cluster. They often are required to organize activities in the cluster. These tasks include but are not limited to data-aggregation and organizing the communication schedule of a cluster.
- **Base Station:** Base station is at the upper level of the hierarchical WSN. It provides the communication link between the sensor network and the end-user.
- **End User:** The data in a sensor network can be used for a wide-range of applications. Therefore, a particular application may make use of the network data over the internet, using a PDA, or even a desktop computer.

1.3 Routing Protocols in WSN

- **Location-based Protocols:** In area based conventions, sensor hubs are tended to by method for their areas. Area data for sensor hubs is needed for sensor organizes by the greater part of the steering conventions to compute the separation between two specific hubs so that vitality utilization can be evaluated. In this segment, we display a specimen of area mindful routing protocols proposed for WSNs.
- **Data Centric Protocols:** Data-centric protocols contrast from traditional address-centric protocols in the way that the information is sent from source sensors to the sink. In address-centric protocol each one source sensor that has the proper information reacts by sending its information to the sink freely of all different sensors. Be that as it may, in data-centric protocols, when the source sensors send their information to the sink, halfway sensors can perform some manifestation of collection on the information starting from different source sensors and send the totaled information around the sink. This procedure can bring about vitality funds due to less transmission needed to send the information from the sources to the sink.
- **Mobility-based Protocols:** Mobility brings new difficulties to routing protocols in WSNs. Sink versatility requires energy efficient protocols to ensure information conveyance started from source sensors to portable sinks.

- **Multipath-based Protocols:** Considering information transmission between source sensors and the sink, there are two routing paradigms: single-way routing and multipath routing. In single-way routing, each one source sensor sends its information to the sink by means of the briefest way. In multipath routing, each one source sensor finds to start with k shortest ways to the sink and partitions its heap evenly among these ways.

1.4 Clustering

Clustering is the task of grouping a set of objects in such a way that objects in the same group (called a cluster) are more similar (in some sense or another) to each other than to those in other groups (clusters). It is a main task of exploratory data mining, and a common technique for statistical data analysis, used in many fields, including machine learning, pattern recognition, image analysis, information retrieval, and bioinformatics. Cluster analysis itself is not one specific algorithm, but the general task to be solved. It can be achieved by various algorithms that differ significantly in their notion of what constitutes a cluster and how to efficiently find them. Popular notions of clusters include groups with small distances among the cluster members, dense areas of the data space, intervals or particular statistical distributions. Clustering can therefore be formulated as a multi-objective optimization problem. The appropriate clustering algorithm and parameter settings (including values such as the distance function to use, a density threshold or the number of expected clusters) depend on the individual data set and intended use of the results.

- **Static and Dynamic Clustering:** A common examination for a distribution strategy that makes utilization of element bunching is to utilize a static grouping system. A case of the utilization of static grouping is the division orders made by expansive file firms. Ordinarily bunches are structured focused around the sort of business or industry connected with an organization (ie utilities, vitality and so on). The Dow Jones Industrial Average contains 30 substantial top stocks that have a long exchanging history. Besides, each one stock can be effectively grouped by their particular S &p segment. This static grouping can likewise structure as the premise for fusing danger equality strategies for portfolio assignment. Element grouping holds a little yet steady focal point over static bunching. The element strategy produces higher returns and danger balanced returns over a long back test period. At the end of the day, Cluster Risk Parity (element grouping with danger equality or danger equality etc) does better than some other danger equality variation. Besides, element bunching likewise delivers better returns and danger balanced returns than non-grouping strategies. Interestingly, static bunching was not as successful as disregarding groups inside and out. This proposes that the changing instability and relationship contain data that is exploitable on an element premise.

1.5 LEACH Protocol

Low Energy Adaptive Clustering Hierarchy ("LEACH") is a TDMA-based MAC convention which is incorporated with bunching and a straightforward directing convention in remote sensor systems (WSN's). The objective of LEACH is to bring down the vitality utilization needed to make and keep up groups keeping in mind the end goal to enhance the life time of a remote sensor system. Drain is a progressive convention in which most hubs transmit to bunch heads, and the group heads total and clamp the information and forward it to the base station (sink). Every hub utilizes a stochastic calculation at each round to figure out if it will turn into a group head in this round. Drain expect that every hub has a radio sufficiently capable to specifically achieve the base station or the closest group head, yet that utilizing this radio at full power all the time would squander vitality. Hubs that have been bunch heads can't get to be group sets out again toward P rounds, where P is the fancied rate of group heads. From there on, every hub has a 1/P likelihood of turning into a bunch head in each round. Toward the end of each round, each one hub that is not a group head chooses the closest bunch head and joins that bunch. The group head then makes a timetable for every hub in its bunch to transmit its information. All hubs that are not bunch heads just correspond with the group head in a TDMA design, as indicated by the timetable made by the bunch head. They do so utilizing the base vitality expected to achieve the group head, and just need to keep their radios on amid their time opening. Drain likewise utilizes CDMA so each one group utilizes an alternate set of CDMA codes, to minimize impedance between bunches. Drain is focused around a various leveled grouping structure model and vitality proficient group based directing conventions for sensor systems. In this directing convention, hubs self-sort out themselves into a few neighborhood bunches, each of which has one hub serving as the group head.

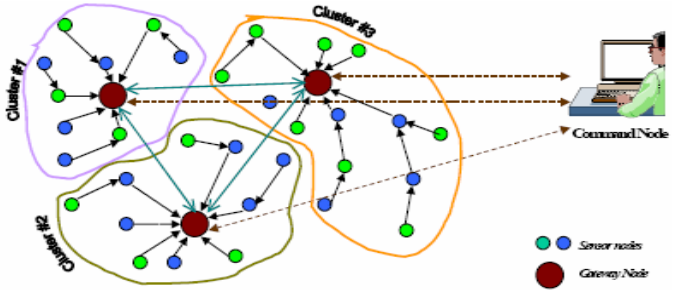

Fig 1.1: Leach Protocol

1.6 Node Replication

Wireless sensor network, an adversary first physically captures only one or few of legitimate nodes, then clones or replicates them fabricating those replicas having the same identity (ID) with the captured node, and finally deploys a capricious number of clones throughout the network. Causes of node replication attack are as follows:

- It creates an extensive harm to the network because the replicated node also has the same identity as the legitimate member.
- It creates various attacks by extracting all the secret credentials of the captured node.
- It corrupts the monitoring operations by injecting false data.
- It can cause jamming in the network, disrupts the operations in the network and also initiates the Denial of Service (D o S) attacks too.
- It is difficult to detect replicated node and hence authentication is difficult.

A WSN can be either stationary or mobile. In static wireless sensor networks (SWSNs), the sensor nodes are stationary or static; that is, the sensor nodes are deployed randomly, and after deployment their positions do not change. On the other hand, in mobile wireless sensor networks (MWSNs), the sensor nodes can move on their own, and after deployment, appearing at different locations at different times. The advantages of our proposed include

1) Localized detection
2) Efficiency and effectiveness
3) network-wide synchronization avoidance
4) network-wide revocation avoidance.

1.7 Detection Techniques

Based on the detection methodologies, classify the clone attack detection.

- Detection Techniques for Stationary WSNs
- Detection Techniques for Mobile WSNs

Witness-Finding Strategy: Node broadcast its location claim to its neighbors, shares a nodes location claims with a limited subset of chosen witness nodes. Checking whether there are the same ID's used at different location to detect the replicas. Static networks trust on the witness-finding strategy, which cannot be applied to mobile networks.

II. LITERATURE SURVEY

Abinaya, P. et al [1] "Dynamic detection of node replication attacks using X-RED in wireless sensor networks":Wireless Sensor Networks often deployed in hostile environments, where an attacker can also capture some nodes. Once a node is captured, the attacker can re-program it and start replicating the node. These replicas can then be deployed in all the network area to render malicious attacks. For any node replication detection protocol, the three most important design issues are memory usage, detection probability and energy consumption. Previous node replication detection schemes either incur more traffic in the network or large memory overhead. We propose a novel dynamic technique for detecting replication attacks using X-RED. X-RED achieves high detection probability and reduces memory overhead than the previously distributed schemes.

Wen Tao Zhu et al [2] "Node Replication Attacks in Wireless Sensor Networks: Bypassing the Neighbor-Based Detection Scheme" We consider the node replication attack, which is an application-independent attack unique to wireless sensor networks. The attack makes it possible for an adversary to prepare her own low-cost sensor nodes and induce the network to accept them as legitimate ones. To do so, the adversary only needs to physically capture one node, reveal its secret credentials, replicate the node in large quantity, and deploy these malicious nodes back into the network so as to subvert the network with little effort. Recently, Ko et al. proposed a neighbor-based detection scheme to cope with replication attacks. The scheme features distributed detection and takes node mobility into account. It harnesses the dynamic observations of the neighbors of a claimer node and avoids the protocol iterations typically found in distributed detections. Unfortunately, we show that their proposal is subject to various replication attacks that can circumvent the detection. Moreover, it is even possible for a sophisticated adversary to exploit the protocol to revoke legitimate nodes.

Ashlyn antoo et al [3] "EEM-LEACH: Energy Efficient Multi-hop LEACH routing protocol for clustered WSN": All technologies in communication sector are trying for the development and improvement of low cost, Low power and smaller multi functional sensor nodes in wireless networking field. One of the major issues in wireless sensor network is limited battery life of sensor nodes. Energy loss for data transfer from nodes to base station is the main cause of energy depletion. A number of routing protocols were introduced to increase the lifetime of the sensor nodes. The most efficient scheme is based on the principle of divide and conquer and data aggregation i.e clustering. EEM-LEACH found a multiple paths with minimum communication cost to send a data from each node to base station. If the communication cost for direct data transfer is less then sensor nodes can directly send their data to base station. It prevents them from dying soon.

Harneet Kaur et al [4] "Hybrid energy efficient distributed protocol for heterogeneous wireless sensor network": The main requirements in the wireless sensor networks are to increase the lifetime of sensor nodes and energy efficiency. In this paper Heterogeneous – hybrid energy efficient distributed protocol was proposed to increase the network lifetime. In wireless sensor network, the impact of heterogeneity has shown in term of energy of nodes. The simulation results shows that the H-HEED increases the lifetime of sensor nodes and more effective data packets in comparison with HEED protocol.

Modares, H et al [5] "Overview of Security Issues in Wireless Sensor Networks": Wireless sensor networks (WSN) are for the most part set up for social affair records from insecure environment. Almost all security protocols for WSN accept that the adversary can attain to completely control over a sensor hub by method for direct physical access. The presence

of sensor systems as one of the primary innovation later on has postured different difficulties to specialists. Remote sensor systems are made out of expansive number of small sensor hubs, running independently, and in different cases, with none get to renewable vitality assets. Likewise, security being major to the acknowledgement and utilize of sensor systems for various applications, additionally diverse set of difficulties in sensor systems are existed. In this paper we will concentrate on security of Wireless Sensor Network.

III. APPROACHES USED

Low Energy Adaptive Clustering Hierarchy (LEACH)-

Low Energy Adaptive Clustering Hierarchy ("LEACH") is a TDMA-based MAC convention which is incorporated with bunching and a straightforward directing convention in remote sensor systems (WSNs). The objective of LEACH is to bring down the vitality utilization needed to make and keep up groups keeping in mind the end goal to enhance the life time of a remote sensor system. Drain is a progressive convention in which most hubs transmit to bunch heads, and the group heads total and clamp the information and forward it to the base station (sink). Every hub utilizes a stochastic calculation at each round to figure out if it will turn into a group head in this round. Drain expect that every hub has a radio sufficiently capable to specifically achieve the base station or the closest group head, yet that utilizing this radio at full power all the time would squander vitality. Hubs that have been bunch heads can't get to be group sets out again toward P rounds, where P is the fancied rate of group heads. From there on, every hub has a 1/P likelihood of turning into a bunch head in each round. Toward the end of each round, each one hub that is not a group head chooses the closest bunch head and joins that bunch.

Power-Efficient Gathering in Sensor Information Systems (PEGASIS)-

PEGASIS is an extension of the LEACH protocol. It forms chains from sensor nodes so that each node transmits and receives their data from a neighbor and a single node is selected from that chain to transmit to the base station (sink). The data is gathered and moves from one node to next node in the form of chain, aggregated and sent to the base station. The chain construction is performed in a greedy way. PEGASIS does not form cluster like LEACH and uses a single node in a chain to transmit data to the BS (sink) instead of using multiple nodes. A sensor transmits data to its local neighbors in the data fusion phase instead of sending directly to its CH as in the case of LEACH. In PEGASIS routing protocol, the construction phase assumes that all the sensor nodes have full knowledge about the network, about the positions of the sensors, and use a greedy approach. When a sensor fails or dies due to low battery power, the chain is constructed using the same greedy approach by bypassing the failed sensor. In each round, a sensor node is randomly chosen from the chain that will transmit the aggregated data to the BS.

Hybrid, Energy-Efficient Distributed Clustering (HEED)-

HEED also extends the basic scheme of LEACH by using residual energy and node degree as a metric for cluster formation to achieve power balancing. This protocol operates in multi-hop networks, using an adaptive transmission power in the inter-clustering communication. HEED was proposed with four primary goals, which are (i) prolonging network lifetime by distributing energy consumption, (ii) terminating the clustering process within a constant number of iterations, (iii) minimizing control overhead (iv) producing well-distributed CHs and compact clusters. In HEED, the proposed algorithm, selects CHs by the combination of two clustering parameters. The primary parameter is their residual energy of each sensor node and the secondary parameter is the intra-cluster communication cost as a function of node degree (i.e. number of neighbors). The primary parameter is used to select an initial set of CHs while the secondary parameter is used for breaking ties. Thus the network lifetime of HEED is better than LEACH because LEACH randomly selects CHs, which may result in faster death of some nodes. The final CHs selected in HEED are well distributed across the network and the communication cost is minimized. This method is suitable for prolonging the network lifetime of wireless sensor networks.

Dynamic Source Routing (DSR)-

The Dynamic Source Routing (DSR) is a routing protocol for wireless mesh networks. It forms a route on-demand like AODV, when a transmitting node requests one. However, it uses source routing instead of relying on the routing table at each intermediate device. This protocol is truly based on source routing whereby all the routing information is maintained at mobile nodes. It has only two major phases, which are Route Discovery and Route Maintenance. Route Reply would only be generated if the message has reached the intended destination node (route record which is initially contained in Route Request would be inserted into the Route Reply).

Table 1.1: comparison between Protocols

Type/Characteristics	**LEACH**	**PEGASIS**	**HEED**	**DSR**
Advantage	LEACH is use to bring down the vitality utilization needed to make and keep up groups keeping in mind the	It is able to increase the lifetime of a each node by using collaborative techniques. Bandwidth consumption in communication is less due	This method is suitable for prolonging the network lifetime of wireless sensor networks.	This protocol uses a reactive approach which eliminates the need to periodically flood the network with table update messages

	end goal to enhance the life time of a remote sensor system.	to local coordination between nodes.		which are required in a table-driven approach. In a reactive (on-demand) approach.
Disadvantage	The disadvantages of this are Every hub utilizes a stochastic alculation at each round to figure out if it will turn into a group head in this round.	Excessive data delay. All sensor nodes have same level of energy and can die at the same time.	The andom selection of the cluster heads may cause higher communication overhead. The periodic cluster head rotation need extra energy to rebuild cluster.	The disadvantage of this protocol is that the route maintenance mechanism does not locally repair a broken link.
Energy	High	High	Low	Medium
Packet Delivery Ratio	High	Medium	High	Low
Throughput	Medium	Low	Medium	Low
Delay	Low	Medium	Low	Low
Lifetime	High	Medium	High	Low

IV. CONCLUSION

In this we have four protocols i.e LEACH, PEGASIS, HEED, DSR & Five parameters Energy, PDR, Throughput, and Delay & Lifetime. From above study it is analyzed that the Performance of LEACH is Excellent. Performance of the HEED is best but less good than Leach. Performance of the PEGASIS is better but less good than Leach & Heed. Performance of the DSR protocol is very poor.

REFERENCES

[1] Abinaya, P. "Dynamic detection of node replication attacks using X-RED in wireless sensor networks", *IEEE Conf on Information Communication and Embedded Systems (ICICES)*, 2014, pp 1 – 4.

[2] "Wen Tao Zhu "Node Replication Attacks in Wireless Sensor Networks: Bypassing the Neighbor-Based Detection Scheme", *Network Computing and Information Security (NCIS)*, 2011, pp 156 – 160.

[3] Yan Liang, Rui Wang "A Biologically Inspired Sensor Wakeup Control Method for Wireless Sensor Networks" *IEEE Transactions on Systems, Man and Cybernetics*, pp. 525-538, 2010.

[4] Ashlyn Antoo "EEM-LEACH: Energy Efficient Multihop LEACH Routing Protocol for Clustered WSNs" *International conference on control, Instrumentation, communication and computational technology (ICCICCT)*, 2014.

[5] Modares, H, Moravejosharieh, A. "Overview of Security Issues in Wireless Sensor Networks" *IEEE Third International Conference on Computational Intelligence, Modelling and Simulation*, pp. 308-311, 2011.

[6] Marriwala, N, Rathee, P. "An approach to increase the wireless sensor network lifetime" *IEEE World Congress on Information and Communication Technologies*, pp. 495-499, 2012.

[7] Mittal, R, Bhatia, M.P.S. "Wireless sensor networks for monitoring the environmental activities" *IEEE International Conference on Computational Intelligence and Computing Research*, pp. 1-5, 2010.

[8] Harneet Kour "Hybrid Energy Efficient Distributed Protocol for Heterogeneous Wireless Sensor Network" *International journal of Computer Applications*, Volume 4- No.6 , 2010.

[8] U. Ahmed and F.B. Hussain, "Energy efficient routing protocol for zone based mobile sensor networks", *in proceedings of the 7th international Wireless Communications and Mobile Computing conference (IWCMC)*, pp. 1081-1086.

[9] Y. Han and Z. Lin. "A geographically opportunistic routing protocol used in mobile wireless sensor networks", *in proceedings of the 9th IEEE international conference on Networking, Sensing and Control (ICNSC)*, pp. 216-221.

