Detecting Security Attacks and Energy Efficient Load-Balanced Clustering Techniques for Wireless Sensor Networks

[1] Ms.T.Sreedevi, [2] Mrs. Meenakshi Bhrugubanda
[1] PG Scholar, M.Tech in CNIS, Dept of IT, Mahatma Gandhi Institute of Technology, Gandipet, Hyderabad, India.
sreedevitripuraneni@gmail.com
[2] Assitant Professor , Dept of IT, Mahatma Gandhi Institute of Technology, Gandipet, Hyderabad, India.

Abstract— Heaps of real-time utilizations of wireless sensor network requires boost of network lifetime. Many clustering approaches have been proposed however they experience the ill effects of lopsided groups which in the end make the network load unbalanced. In this work, we have recommended a two-stage energy proficient balanced clustering method which will balance the network load. We thought about the boundaries leftover energy, intra-bunch cost, entomb group cost, correspondence separation. We contrasted our proposed protocol and an ongoing clustering protocol CH-leach. Reproduction results show that the proposed calculation achieves better burden balance, increment the network lifetime with energy balance groups and lower hub demise rate. WSN routing in order to balance the energy consumption and improve the network lifetime. Three one security analysis suggests that a distributed WSN architecture that supports fault tolerance and consistency checks is important for WSN control plane security. Our analysis methodology may be of independent interest for future security analysis of WSN and conventional networks. Provides a new evaluation framework to objectively compare the security of both network paradigms, using threat models defining the attacker's position in the network.

1. INTRODUCTION

Presently wireless sensor networks (WSNs) have been seen as a fundamental technology. A typical WSN composed of a broad number, insignificant cost sensor hub which work on restricted battery power and are occupied with the unreachable and unsafe condition. Sensor nodes can detect fringe occasions, combine the sense statistics and communicate it. WSNs are used with a wide scope of applications such as ecological disorder monitoring, military surveillance, ocean monitoring, the inward natural life of ocean monitoring, submerged mineral mining, persistent monitoring etc. As referenced before sensor hub works with restricted battery power and is occupied with an unreachable and risky condition. That is the reason they are exceptionally difficult to replace or recharged. Therefore, energy efficiency to expanding the network life expectancy is one of the basic challenges [1,2,3].

For augmenting the existence time of WSNs an a lot of hierarchy based clustering protocol has been proposed by the researchers. Each of them utilizes various protocols for cluster formation and information transmission [4]. These protocols segment the WSN into various logical gatherings which named clusters.

In each cluster a hub act like a pioneer which called cluster head (CH). CH is mindful towards communicate through the base station (BS). Therefore, steering overhead of normal nodes are reduced because they just communicate their information to CH. In [5] Heni Zelman initially proposed LEACH protocol for WSN. The key thought of LEACH was rotating the CH over the entire network for efficient burden dispersal. This protocol selects CH haphazardly with probabilistic way.

Subsequent to completing a couple of rounds low energy sensor hub may become CH. On the off chance that the low energy sensor hub is named for CH, at that point it will lapse quickly. Consequently, network heaviness will affect and network lifetime decrease. [6].

LEACH-C or LEACH-Centralized is another approach [7] to increase the performance of LEACH. In LEACH-C the BS make all decisions like CH selection, cluster formation and circulation of information into the network. CH choice relies upon energy and location information.

In EESCA [8], CH selection is made by cross breed way relies upon location and remaining energy. The author claims that the proposed method is decent for load balancing and increase the network lifetime. This protocol partitions the entire network into a static number of cluster (four). Select a hub as a CH which is central situation of the cluster and low normal communication distance. CH jelly the successive gathers together to lose its half of the total energy allotted in the initial time frame. A while later another hub is selected with low normal communication distance. At the point when all hub of the cluster loses their half energy, at that point the CH selection is relying upon outstanding energy. On the off chance that a hub from the edge of the network is selected as CH. The nodes in the cluster need to communicate their statistics over a protracted distance. Hence more imperativeness will consume.

In [9] proposed another method advanced leach, OLEACH principle reason for this algorithm is to improve winning LEACH just as LEACH-C protocols. The key thought of the method is select a hub as a CH which energy level is more prominent than 10% of the remaining energy level of each sensor. At the point when the energy is not as much as its level in second stage customary LEACH protocol will be run. In EBCAG [10], the key point behind formation of cluster is to calibrate cluster size indicated by the partition between the BS and CH. In this method each sensor hub protects an incline regard which describe its most

minimal advance count to the BS. Nonetheless, safeguarding a slope an incentive for each sensor hub produce extra energy overhead inside the network. In this protocol, for formation and maintenance of various size of cluster required enormous measure of energy.

In ECPF [11], CH selection is finished by non-probabilistic way. It selects CH according to postpone times which is conversely comparative with the rest of the energy. ECPF method additionally practices fluffy logic rules for choosing last CH from a provisional arrangement of CH. In this method CH selection technique basically relies upon the defer time. However, remaining energy of hub is less in upper rounds. Therefore, postpone time will be extremely short. Selection of CH from provisional arrangement of CH utilizing fluffy logic will require more time and energy. Recently different protocol proposed based on LEACH. CH-Leach [12] based on k-means procedure. Notwithstanding, according to [16] kmeans procedure experiences void cluster and inconsistent cluster size issue. In [13] use k-means algorithm for clustering. CH selection is made by Gauss disposal algorithm. This approach likewise experiences inconsistent cluster size. Because of inconsistent cluster size, lopsided burden conveyance occurs in the network. Because a CH holds more member nodes (MNs) will chomp more energy, and passes on quicker in compare to another CH holding less MNs [14]. The identified properties are critical for successful operation of networks in practice, as they enable networks to function efficiently, scale, and ensure the networks' high availability. The two threat models provide varying degrees of adversarial capabilities, enabling the analysis of differences and similarities in the attack surface of protocols implementing each of the five properties in both network paradigms. To the best of our knowledge, this is the first framework that allows for such an apples-to-apples comparison of both paradigms, exploring both attacks and defenses. In our proposed protocol we give arrangement of these issues.

Here we offered a new approach for energy efficient load balancing for WSNs. Proposed method contain two stages. First stage composed of cluster formation and the second stage is load balancing algorithm. For load balancing we consider intra, inter cluster cost, communication distance among CH and the BS. We have described briefly about the protocol in section II, Methodology III, result in section IV and conclusion in section V.

.

II. PROPOSED PROTOCOL

A. Assumptions

In our proposed protocol we expect that all nodes are haphazardly organized over the network. All the nodes are homogeneous for example all hub have equivalent communication capacities and equivalent beginning energy. Nodes energy can vary according to communication distance. The BS is fixed with enough computational force. We intentional two circumstances for the location of BS, one is the center of the network and the other is the edge of the network.

B. Radio Model

We use first order radio model [7] for energy consumption

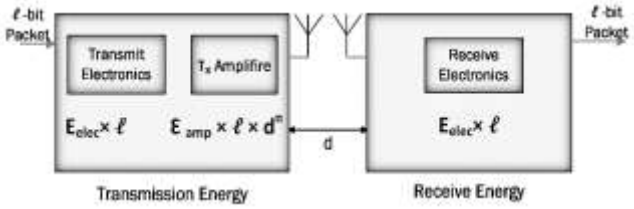

Figure. 1 Radio energy degeneracy model

analysis which is illustrated in Fig. 1. For transmitting bit message over distance d, the energy consumption can be defined by the following equation:

$$E_{TX(l,d)} = \begin{cases} E_{elec} \times l + \epsilon f_s \times l \times d^2, for\ d < d_0 \\ E_{elec} \times l + \epsilon_{mp} \times l \times d^4, for\ d \geq d_0 \end{cases} \quad (1)$$

Where E_{elec} is energy for processing per bit, and ϵf_s and ϵ_{mp} energy consume for transmitting one bit to accomplish a tolerable bit error rate in free space and multipath model respectively.

Where threshold d_0 can be defined by the following equation:

$$d_0 = \sqrt{\frac{\epsilon f_s}{\epsilon_{mp}}} \quad (2)$$

And for receiving bit, the consumption is given by the following equation:

$$E_{RX} = E_{elec} \times l \quad (3)$$

C. Protocol Description

Our proposed protocol composed of two stages. One is the cluster formation and the other is load balancing based on a centralized system. All computation will be done by the BS [15]. In the cluster formation stage, cluster formation and CH selection will be done by the k-means algorithm [12].

However, the k-means algorithm creates an empty cluster and unequal size of clusters [16]. In the load balancing stage first, we remove the empty cluster where the number of nodes equals zero. We define maximum node threshold Thnode. Which can be defined as follows: Thnode= No. of alive node/No. of cluster, minimum node threshold Thmin. Where Thmin.= m percent of Thnode and communication distance threshold Dth. We assume in our work that Dth=80 percent of the network size. where Dth is the communication distance threshold from BS to corresponding CH of a cluster.

For fine tuning the load balance, we considering the parameters intra cluster cost, inter cluster cost and communication distance. Intra cluster cost means energy needed for communication among member nodes with its

CH in a cluster. Inter cluster cost means energy needed for communication between CH and the BS. Communication distance means the distance between CH and the BS. The CH of a corresponding cluster which is farthest from the BS, spend more energy for sending its data to BS. So proposed algorithm checks with the communication distance threshold Dth for every CH. If the Dth is greater than Dch, where Dch is the distance from BS to CH then the node threshold Thnode for that cluster will be 10 percent less than the original node threshold Thnode. Then find the cluster which the number of nodes less than Thmin. Remove these nodes from that cluster and join them to their nearest cluster. The cluster becomes empty, again remove the empty cluster.

Now find the heavy loaded cluster where number of node is greater than Thnode. Load balance is done by removing those extra nodes which are furthest from its CH and join those nodes to their nearest cluster. For the lightly loaded cluster where number of node is less than Thnode, will receive nodes removes from the heavy loaded cluster. After that, some cluster might be heavy or lightly loaded. For this reason, we didn't apply any condition. After several iterations of the process, all cluster of the network will be well balance. i.e. not too heavily and lightly loaded. Since this protocol consider for one hop communication network the pseudo code of proposed algorithm is outline bellow:

- **Step 1:** Cluster formation will be done by k-means algorithm.
- **Step 2:** Select CH according to residual energy of each cluster.
- **Step 3:** Set node threshold Thnode = No. of alive node/No. of cluster
- **Step 4:** Set Dth= Network size*.80 // Where Dth is the communication distance threshold from BS to CH
- **Step 5:** Set Thmin. = m percent of Thnode // where m is variable.
- **Step 6:** Find all empty cluster and remove those cluster.
- **Step 7:** if number of nodes of any cluster is < Thmin.
- Then join those nodes to the nearest cluster and remove that empty cluster.
- **Step 8:** Find all heavy loaded and lightly loaded cluster according to node threshold level. Execute step 9 and 10 for n time.
- **Step 9:** for each heavy loaded cluster Thnode = No. of alive node/No. of cluster If (Dth>Dch) Set NewThnode= Thnode*0.9
  Else Set Thnode =NewThnode
  End if
  Find adjustable node from this cluster which is furthest from its CH
  Adjustable node= number of node of the cluster- Thnode.
  For each adjustable nodes
  Join this node to its nearest CH other than self CH
  End for
  End for
- **Step 10:** for each lightly loaded cluster
  Thnode = No. of alive node/No. of cluster
  If (Dth>Dch)
  Set NewThnode= Thnode*0.9
  Else Set Thnode =NewThnode
  End if
  Select adjustable nodes which are nearest to the CH but not member of this cluster.
  Adjustable node= Thnode- number of node of the cluster
  For each adjustable nodes
  Join the node to this cluster
  End for
  End for.

III. METHODOLOGY

- **WSN Node Creation**

This is the first module of our project. It will provide a good security for our project. So server contain server also check the authentication of the user. It well improves the security and preventing from unauthorized data owner enters into the network. In our project we are using SWING for creating design. Here we validate the login user and server authentication. WSN involves one or more WSN controllers, each controlling a number of network elements within its domain via standard protocols. Each controller may run in multiple instances, each further managing a subset of network elements and backing-up other instances to provide both scalability and high availability An WSN controller is an entity that does not exist in a CN, thus its security requires special attention. As noted earlier, we focus on control plane security here.

- **Basic & Loop Free Forwarding**

This is the second module of our project. In this, the Sender sends files to the destinations with the help of the nodes which are available in the network. For that purpose, first select the file then initialize the nodes which are available in the network and then selects the destination node for sending the file successfully and have to choose the nodes dynamically for providing security. When data is transferred from one node to another it will be transferred with Basic Forwarding and without any loops.

- **Link Redundancy**

This is the third module of our project. I n this module, the information regarding to nodes selection can be determined. The Sender can choose the file for sending it to the destination. For sending purpose we have to choose the

routing path dynamically based on the available nodes in the network and have to choose the destination node (receiver) all this will be done without any link redundancy. It can be done by grouping multiple links into one virtual link, A Link Aggregation Group (or LAG), viewed as a single link

- **Energy Efficient Load Balancing**

This is the fourth module of our project. In this module, for sending purpose we have to choose the routing path dynamically based on the available nodes in the network and have to choose the destination node(receiver) all this will be done without any link redundancy, Energy Efficient & Load Balancing. We determined & analyze the traffic load and energy consumption of the sensor nodes, which is complicated because network routing paths change dynamically.

- **Attack Detection**

This is the fifth module of our project. In this module, the Attackers can abuse or corrupt the files sanded by the service provider before reaching it to the destination node. So, for corrupting the file, the attacker selects the node which is involved in the routing (The nodes selecting for the routing must be active nodes in the network and having sufficient energy) and then he injects the corrupted data.

- **Scalability**

This is the six modules of our project. Scalability is an important issue in our paper, while easy in small networks, challenges arise in larger networks such as a large enterprise data centre with many physical servers and virtual machines, each with several MAC addresses. We will show the scalability of our WSN in a tabular format in project.

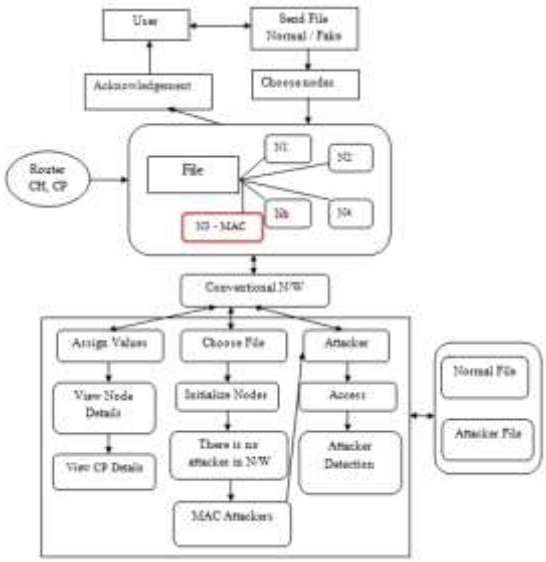

Fig: 1. System Model

IV. RESULT

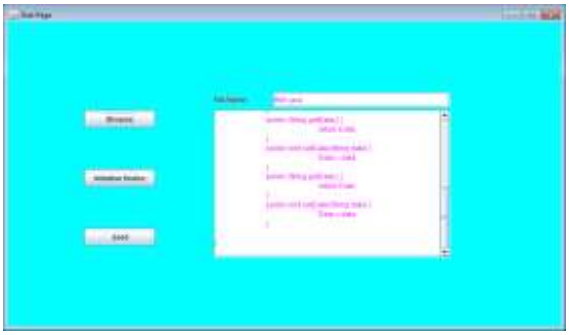

Fig: 2. Send Page

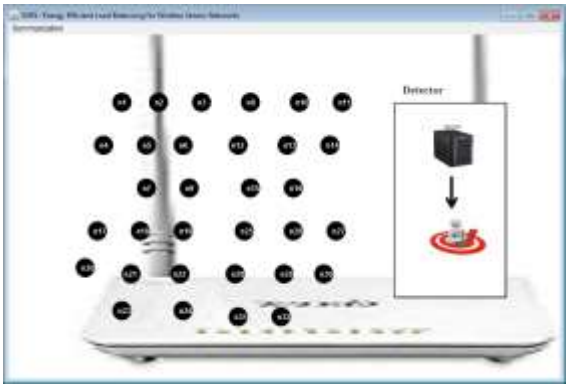

Fig: 3. Router Nodes

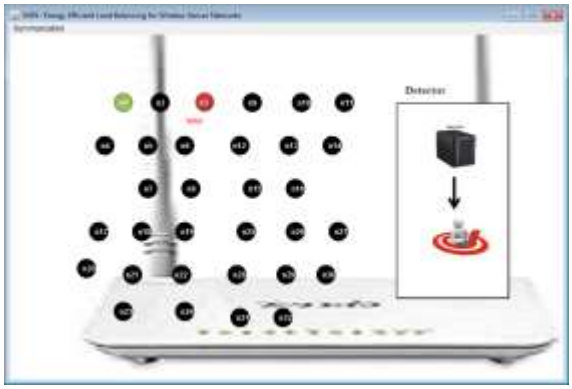

Fig: 4. Data Transforming

V. CONCLUSION

Vitality effectiveness is the key issue fir the usage of different wireless sensor network applications. In this work we have offered a two-arrange vitality capable burden balance calculation to make even load appropriation inside the network. We have actualized and tried the proposed convention on two circumstances of the BS location and contrasted and a current convention. The reproduction results show that offered convention accomplishes great burden

adjusting inside the network. Accordingly, network life time improves fundamentally.

The identified properties are critical for successful operation of networks in practice, as they enable networks to function efficiently, scale, and ensure the networks' high availability. The two threat models provide varying degrees of adversarial capabilities, enabling the analysis of differences and similarities in the attack surface of protocols implementing each of the five properties in both network paradigms. To the best of our knowledge, this is the first framework that allows for such an apples-to-apples comparison of both paradigms, exploring both attacks and defenses.

The framework is useful to both network administrators and security researchers; we thus believe this work will help guide further WSN research, and aid practitioners in the design, development, and deployment of WSN's with stronger robustness and security properties. Scalability is an important issue in our paper, While easy in small networks, challenges arise in larger networks such as a large enterprise data centre with many physical servers and virtual machines, each with several MAC addresses. We will show the scalability of our WSN in a tabular format in project.

REFERENCES

[1] Md. Nurul Islam Khan, Md. Saiful Islam "A New Approach of Energy Efficient Load Balancing for Wireless Sensor Networks" 2019 International Conference on Robotics, Electrical and Signal Processing Techniques (ICREST), IEEE, February 2019.

[2]A. More, V. Raisinghani, "A survey on energy efficient coverage protocol in wireless sensor networks," Journal of King Saud University-Computer and Information Science, vol. 29, pp. 428-448, Oct. 2017.

[3] R. Sruthi, "Medium Access Control Protocols for Wireless Body Area Networks: A Survey," Global Colloquium in Recent Advancement Effectual Researches in Engineering, Science and Technology, pp. 621-628, 2016.

[4] M. Ahmed, M. Salleh, M. I. Channa, "Routing protocols based on protocol operations for underwater wireless sensor network: A survey," Egyptian Informatics Journal, vol. 9, pp. 57-62, Mar. 2018.

[5] T. Firdaus, M. Hasan, "A Survey on Clustering Algorithm for Energy Efficiency on Wireless Sensor Networks," International Conference on Computing for Sustainable Global Development, pp. 759-763, 2016.

[6] W. R. Heinzelman, A. Chandrakasan and H. Balakrishnan, "Energy Efficient Communication Protocol for Wireless Microsensor Networks," 33rd Hawaii International Conference on System Science, pp. 1-10, 2000.

[7] S. K. Singh, P. Kumar and J. P. Singh, "A Survey on Successors of LEACH Protocol," IEEE Access, vol. 5, pp. 4298-4328, Feb. 2016.

[8] W. B. Heinzelman, A. P. Chandrakasan, and H. Balakrishnan," An Application-Specific Protocol Architecture for Wireless Microsensor-Networks," IEEE Transactions on Wireless Communications, vol.1, pp. 660-670, Oct. 2002.

[9] P. Yuvaraj, K. V. L. Narayan, "Energy Efficient Structured Clustering Algorithm for Wireless Sensor Networks," International Conference on Computing, Analytics and Security Trends, pp. 523-527, 2016.

[10] S. E. Khediri, N. Nasri, A. Wei, A. Kachouri, "A New Approach for Clustering in Wireless Sensor Networks Based on LEACH," International workshop on Wireless Networks and Energy Saving Techniques, pp. 1180-1185, 2014.

[11] T. Liu, Q. Li, P. Liang, "An energy-balancing clustering approach for gradient-based routing in wireless sensor networks," Computer Communications, vol. 35, pp. 2150-2161, Oct. 2012.

[12] H. Taheri, P. Neamatollahi, O. M. Younis, S. Naghibzadeh, M. H. Yaghmaee, "An energy-aware distributed clustering protocol in wireless sensor networks using fuzzy logic," Ad Hoc Networks, vol. 10, pp. 1469-1481, Sep. 2012.

[13] W. Aabushiba, P. Johnson, S. Alharthi, C. Wright, "An Energy Efficient and Adaptive Clustering for Wireless Sensor Network (CHleach) using Leach Protocol," International Computer Engineering Conference, pp. 50-54, 2017.

[14] E. Rabiaa, B. Noura, C. Adnene, "Improvements in LEACH based on K-means and Gauss algorithm," The International Conference on Advancement Wireless, Information and Communication Technologies, pp. 460-467, 2015.

[15] A. Sharma, P.Kansal, "Energy Efficient Load-Balanced Clustering Algorithm for Wireless Sensor Networks," Annual IEEE India Conference, pp. 1-6, 2015.

[16] Mst. J. Ferdous, J. Ferdous, T. Dey, "Central Base-Station Controlled Density Aware Clustering Protocol for Wireless Sensor Networks," International Conference on Computer and Information Technology, pp. 37-43, 2009.

[17] V. S. Chandrawanshi, R. K. Tripathi, N. U. Khan, "A Comprehensive Study on K-means Initialization Techniques for Wireless Sensor Networks," International Conference on Signal Processing and Communication, pp. 154-159, 2016.