International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 07 | July-2016 www.irjet.net p-ISSN: 2395-0072

Energy Efficient Hierarchical Clustering (EEHC) Protocol using Apply Trust Based Concept for Securing Cluster-Based Sensor Networks

Dr. M. Kezia Joseph[1], Shafia Tasneem[2]

[1]Professor, Dept. of Electronic and Communication Engineering, Stanley College of Engineering and Technology for Women's, Hyderabad, India
[2]ME Student, Dept. of Electronic and Communication Engineering, Stanley College of Engineering and Technology for Women's, Hyderabad, India

---

Abstract - *A wireless network consisting of a large number of small sensors with low-power transceivers can be an effective tool for gathering data in a variety of environments. The data collected by each sensor is communicated through the network to a single processing Centre that uses all reported data to determine characteristics of the environment or detect an event. The communication or message passing process must be designed to conserve the limited energy resources of the sensors. Clustering sensors into groups, so that sensors communicate information only to cluster heads and then the cluster heads communicate the aggregated information to the processing Centre, may save energy. In this work a new scheme EEHC is proposed. In this study energy consumption, performance on delay, performance on dropping, packet delivery ratio and network output are being calculated for the proposed and existing systems to estimate the performance of the proposed method.*

Key Words: Clustering methods, sensor networks, algorithms, network security and wireless communication.

1. INTRODUCTION

Proficient outline and execution of remote sensor systems has turned into a hot range of examination as of late, because of the immense capability of sensor systems to empower applications that associate the physical world to the virtual world. By systems administration expansive number of little sensor hubs, it is conceivable to acquire information about physical marvels that was troublesome or difficult to get in more traditional ways. In the coming years, as advances in small scale creation innovation permit the expense of assembling sensor hubs to keep on dropping, expanding organizations of wireless sensor networks (WSN) are normal, with the systems in the long run developing to vast number of hubs (e.g., thousands).

Because of the extensive variety of utilization, remote sensor systems have increased overall consideration as of late. The system is constructed utilizing sensor hubs which are small, with restricted preparing and figuring assets, and they are modest contrasted with conventional sensors. These sensor hubs can sense, assemble, and measure data from the earth and in view of some neighborhood choice procedure or utilization of the system conveyed in the territory, they can transmit gathered information to the client or sink hub.

WSNs have substantial zone of uses however they are constrained because of its engineering like restricted vitality, preparing power, adaptability issues, stockpiling limit, data transfer capacity, range and so on. So when it comes to different mechanisms like key management, routing, data aggregation or tracking or other area, development of techniques for better efficiency is needed [10].

As sensor hubs are sent in antagonistic or remote environment and unattended by human, they are inclined to various sort of assaults. So information must be exchanged between hubs utilizing encryption strategies and for that adjustment of key administration is critical for WSNs. Key administration is a center component to guarantee security in system and one of the significant utilizations of remote sensor system. Key administration can be characterized as an arrangement of procedures and system that bolster key foundation and the support of progressing keying connections between legitimate gatherings as indicated by a security approach. The objective of key administration in WSNs is to take care of the issue of making, dispersing and maintaining those secret keys [10].

Thus strategies for key administration of encryption keys are of indispensable significance for security in WSNs. Because of the impediments of assets for sensor hubs, conventional key administration plans can't be utilized for encryption reason as a part of WSN. So lots of examination work has been done and as yet going ahead in WSN for creating key administration conspires that can satisfy the whole necessities.

The paper is composed of six sections. In section 2 writing review is talked about. In section 3 framework engineering of proposed technique is presented. In section 4 methodologies is depicted. In section 5 results are shown. In section 6 conclusions and future extension is given.

2. LITERATURE SURVEY

Since both device and battery innovations have just as of late developed to the point where smaller scale sensor hubs are achievable, this is a genuinely new field of study. Scientists have started examining not just the utilizations and difficulties confronting sensor systems however have likewise been creating preparatory thoughts with respect to how these systems ought to work and additionally the proper low-vitality design for the sensor hubs themselves [9].

There have been some application-particular conventions produced for smaller scale sensor systems. Clare et al. built up a time division multiple access (TDMA) media access control (MAC) convention for low-vitality operation. Utilizing a TDMA approach spares vitality by permitting the hubs to stay in the rest state, with radios shut down, for quite a while. Intanagonwiwat et al. developed directed diffusion, a protocol that employs a data-driven model to achieve low-energy routing [8].

A security hub based key administration convention is proposed for group based sensor systems. Part hubs and cluster heads are in charge of information gathering and transmission. Security hubs are in charge of key administration. Security hubs control key administration capacity of cluster heads, and decrease harm of caught cluster heads. Era of security hubs and various types of keys is portrayed. Execution examination and reenactment demonstrate that the proposed key administration convention devours less vitality, and its postponement time of key era is short. In the meantime, the convention can give more community verification security to keys. It has solid strength against hub catch, and can bolster expansive scale system [1].

The principle objective of Cluster-based sensor systems is to decrease system delay and reduce energy consumption. LEACH is a cluster based convention for small scale sensor systems which accomplishes vitality productive adaptable steering and reasonable media access for sensor hubs. Notwithstanding, the race of a vindictive or traded off sensor hub as the cluster head is one the most critical breaks in cluster based remote sensor systems. The drawbacks of existing method are more energy consumption, authentication is not provided properly and distance calculation from node to node is not maintained. A deterministic key administration plan, called DKS-LEACH [6] to secure LEACH convention against pernicious assaults is proposed.

3. SYSTEM ARCHITECTURE

The WSN consists of bunches. Every bunch has a cluster head (CH). The hubs in a bunch share a key known as cluster key which is implied for broadcasting messages safely. This key can be overhauled by cluster head when new sensor joins the bunch or a current hub leaves the bunch. Cluster heads forward information to base station. The cluster keys are conveyed to base station through system controller. In view of the messages traded with base station, the cluster keys are overhauled. Each node in the network shares different pair wise key with neighbors for secure authentication and communication in the network. Nodes can dynamically establish pair wise key between other nodes in the network using public key cryptography.

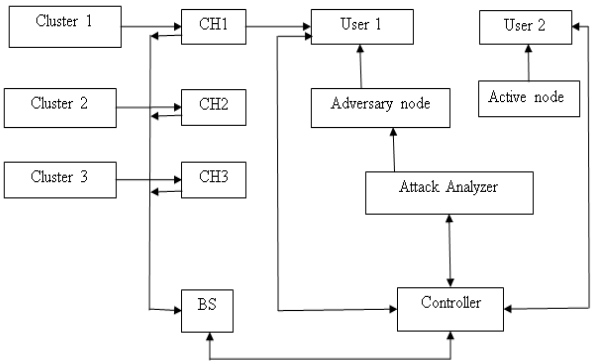

Fig -1 Architectural diagram of proposed method

The BS is the primary layer which controls the system furthermore causes in interfacing WSN to outer systems like Internet. The second layer is known as CH layer. The CH coordinates all other nodes in the cluster in terms of information exchange and different operations. The third layer is implied for gathering information from encompassing environment and sends that to cluster head. The sensor node (SN) layer is isolated into numerous bits known as clusters. Every cluster has a CH which organizes all SNs in the group. SNs can communicate with different SNs in the same cluster furthermore the CH. All CHs of all clusters can transfer data with each other furthermore the BS. The proposed plan makes utilization of two sorts of keys for encryption. Out of them, the first is a shared key amongst CH and SNs while the second one is the master key shared amongst BS and CHs. The master key is separated into numerous sub keys which are circulated among the CHs progressively. CH has more vitality utilization because of its substantial obligations.

4. METHODOLOGY

Every sensor in the system turns into a cluster head (CH) with likelihood p and publicizes itself as a cluster head to the sensors inside its radio extent. These cluster heads are called as volunteer cluster heads. This ad is sent to every one of the sensors that are close to "k" jumps far from the cluster head. Any sensor that gets such promotions and is not itself a cluster head joins the group of the nearest cluster head. Any sensor that is neither a cluster head nor has joined any group itself turns into a cluster head; these cluster heads are called as constrained cluster heads. Since the commercial sending to "k" bounces is constrained, if a sensor does not get a CH notice inside time length "t" it can induce that it is not inside "k" jumps of any volunteer cluster head and henceforth turn into a constrained cluster head. Additionally, since each one of the sensors inside a cluster are at most k bounces far from

the cluster head, the cluster head can transmit the amassed data to the handling focus after each t units of time. This point of confinement on the quantity of jumps subsequently permits the cluster heads to plan their transmissions. Note this is a circulated calculation and does not request clock synchronization between the sensors.

The vitality utilized as a part of the system for the data assembled by the sensors to achieve the preparing focus will rely upon the parameters p and k of our calculation. Since the goal of the work, is to sort out the sensors in groups to minimize this vitality utilization, finding the estimations of the parameters p and k of the calculation is expected to guarantee minimization of vitality utilization. Expressions for ideal estimations of p and k in the following subsection are determined. Cluster head formation based on levels is only possible by the support of EEHC. Energy is calculated for all nodes but particularly needed for cluster heads. In this probability values are calculated using RSA mechanism and set them into level of processing and compare the levels. Individual calculations are required for cluster head communication and look at the lifetime network.

4.1 Algorithm

Step1: First choose level-1 cluster heads and level-2 cluster heads.
Step2: Each sensor node decides to become level-1 cluster head with certain probability p1.
Step3: Prolong the information as cluster head to sensor nodes within range.
Step4: This information forwarded to all sensor nodes within the k1 hops of the advertising CH.
Step5: Each sensor receives an advertisement joins the cluster of the closest level-1 CH.
Step6: The remaining sensor nodes become forced level-1 CHs.
Step7: Level-1 CHs then elect themselves as level-2 CHs with a certain probability p2.
Step8: Broadcast their decision of becoming a level-2 CH.
Step9: This decision forwarded to all sensor nodes with k2 hops.
Step10: The level-1 CHs that receive the advertisements from level-2 CHs joins the cluster of the closest level-2 CH.
Step11: All other level-1 CHs become forced level-2 CHs. Cluster heads at 3, 4…..are chosen in similar way…with probability of p3, p4…respectively to generate a hierarchy of CHs.

4.2 Optimal parameters for the algorithm

a) The sensors in the remote sensor system are conveyed according to a homogeneous spatial Poisson procedure of power ' λ' in 2-dimensional space.
b) All sensors transmit at the same force level and subsequently have the same radio extent r.
c) Data traded between two conveying sensors not inside each other's radio extent is sent by different sensors.
d) A separation of "d" between any sensor and its cluster head is proportional to (d/r) bounces.
e) Each sensor utilizes 1 unit of vitality to transmit or get 1 unit of information.
f) A directing foundation is set up; thus, when a sensor imparts information to another sensor, just the sensors on the steering way ahead the information.
g) The correspondence environment is contention and error free; thus, sensors don't need to re transmit any information.

4.3 Traffic control

Consistent Bit Rate (CBR) is a term utilized as a part of information transfers, identifying with the nature of administration. At the point when alluding to codecs, steady bit rate encoding implies that the rate at which a codec's yield information ought to be devoured is consistent. CBR is helpful for gushing sight and sound substance on restricted limit channels since it is the greatest bit rate that matters, not the normal, so CBR would be utilized to exploit the majority of the limit. CBR would not be the ideal decision for capacity as it would not assign enough information for complex areas (bringing about corrupted quality) while squandering information on basic segment.

The issue of not dispensing enough information for complex areas could be understood by picking a high bitrate to guarantee that there will be sufficient bits for the whole encoding process; however the span of the document toward the end would be relatively bigger. Most coding plans, for example, Huffman coding or run-length- encoding produce variable-length codes, making immaculate CBR, hard to accomplish. This is incompletely unraveled by differing with the quantization (quality) and completely explained by the utilization of padding. (Be that as it may, CBR is inferred in a basic plan like decreasing every one of the 16-bit sound specimens to 8 bits.) For the situation of spilling video as a CBR, the source could be under the CBR information rate target. So as to finish the stream, it's important to include stuffing parcels in the stream to achieve the information rate needed. These bundles are absolutely nonpartisan and don't influence the stream.

4.4 Adhoc on demand distance vector (AODV)

In AODV telecasts each adjustment in the system to each hub are not necessary. On the off chance that a connection breakage does not influence on going transmission, no worldwide telecast happens. Just influenced hubs are educated. Neighborhood developments of hubs have nearby impacts. AODV reduces the system wide broadcasts to the extent possible, significant reduction in control overhead when compared with DSDV.

AODV finds routes as and when essential. It maintains the routes as long as necessary. Every node maintains its monotonically increasing sequence number. Increases every time, the hub sees change in the area topology. AODV uses directing tables to store steering data. Directing table in AODV is for unicast routes and multicast routes. At the point when a hub wishes to send a packet to some destination, it checks its directing table to figure out whether it has a present route to the destination. If yes, forwards the packet to next hop node. Else it initiates a route discovery process.

4.5 Advantages of proposed method

The advantages of proposed method are energy consumption is low, distance calculation is easy, network performance is more, routes are maintained properly for communication and fake messages are stopped to base station.

5. SIMULATION AND RESULTS

In this study, operating system ubuntu 14.04 and ns2-2.35 tool is used. It has platform like Linux. Installation of languages is completed and program is written in text document and it is saved as .tcl. System is made for information transmission and gathering with the support of controller.

Table 1 is summarized with the different configuration values that were used in the performed simulations.

PARAMETER	SPECIFICATION
Simulation tools used	Network Simulator 2.35 (NS2)
Simulation time	10 sec, 20 sec, 30 sec, and 50sec
Number of nodes	10,20,30,40,50,60,70,80,90,100
Transmission range	250m
Maximum speed	0-20 m/sec
Application traffic	constant bit rate (CBR) [20]
Packet size	512bytes
Node mobility model	8 packets/sec
Protocol	AODV
No. of runs	450

Table -1 Simulation parameters

Figure 2 is network output graph in this number of hubs are shown on x-axis and throughput is shown on y-axis. Throughput is measured regarding megabits every second. For 50 nodes throughput is around 87 megabits per second in case of existing method whereas throughput of proposed method is around 96 megabits per second.

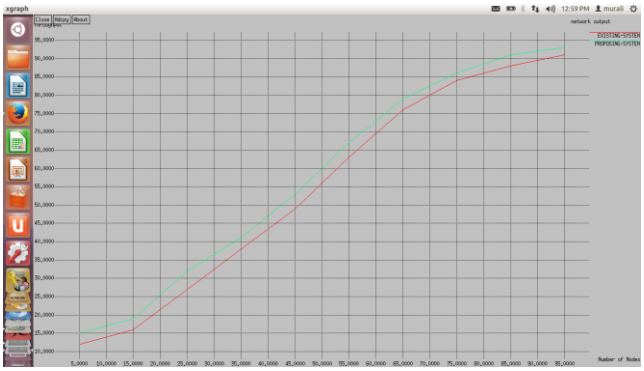

Fig -2 Network output

Figure 3 is Performance on dropping of packets graph in this time is shown on x-axis and number of packets is shown on y-axis. For 95 seconds of time 10 packets fall in existing method and 7 packets fall in proposed method.

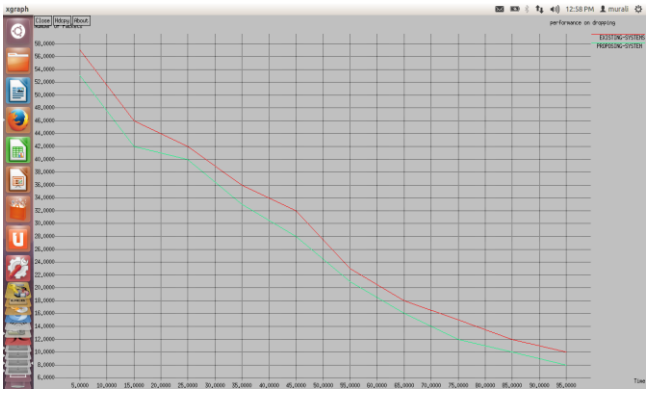

Fig -3 Packet dropping performance

Figure 4 is Energy consumption graph in this time is shown on x-axis and network size is shown on y-axis. Time is measured in terms of seconds. For 95 seconds of time, energy consumption is 45 joules for existing method and 36 joules for proposed method.

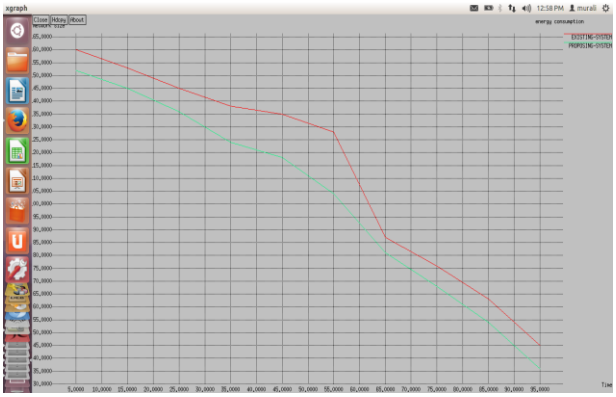

Fig -4 Energy consumption

Figure 5 is Performance analysis on delay of packets graph in this time is shown on x-axis and number of packets is shown on y-axis. For 95 seconds of time 4 packets are deferred in existing method and 3 packets are deferred in proposed method.

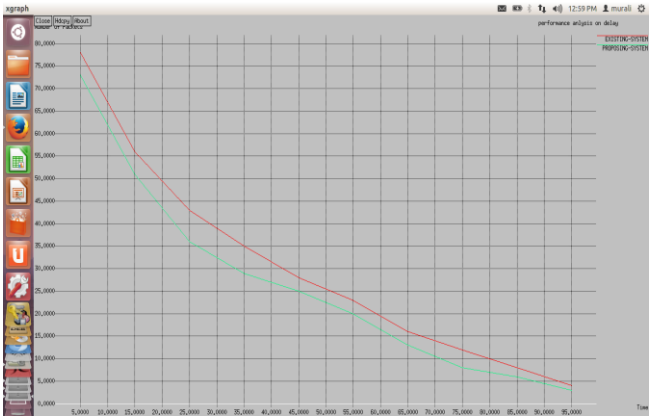

Fig -5 Performance of delay analysis

Figure 6 is Packet delivery ratio graph in this time is shown on x-axis and % of data packet delivered is shown on y-axis. For 95 seconds of time 74 % of data is delivered in existing method and 90% of data is delivered in proposed method.

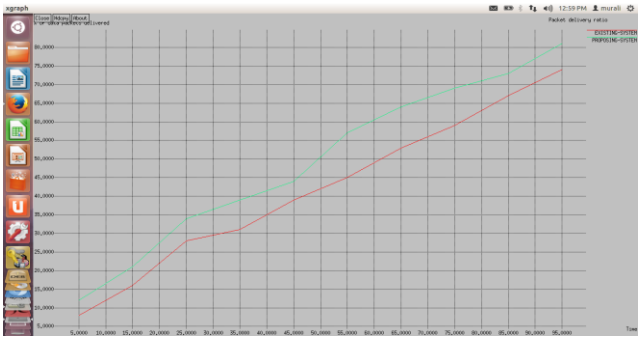

Fig -6 Packet delivery ratio

Parameter's	Existing Output Values (RING LEACH)	Proposed Output Values (EEHC)
Energy Consumption	45 Joules	36 Joules
Performance on delay	4 packets	3 packets
Performance on Dropping	10 Packets	7 packets
Packet delivery ratio	74%	90%
Network Output	88 mega bits/sec	92 mega bits/sec

Table -2 Comparison of existing and proposed system

6. CONCLUSIONS AND FUTURE SCOPE

Out of several schemes proposed in the literature, LEACH concept provides less end to end delay for communication with authentication. In the current study, RING-LEACH concept is compared with energy efficient hierarchical clustering (EEHC) scheme. The RING-LEACH [4] mechanism doesn't support the complete energy levels calculation for every cluster node in network.

So energy efficient hierarchical clustering (EEHC) is being proposed for formation of clusters in network properly and improves the storage level of energy at individual node. Using this mechanism energy consumption is decreased. Advantages of proposed system are energy consumption is low, distance calculation is easy, network performance is more, routes are maintained properly for communication and fake messages are stopped to base station. Here, cluster base network is formed and analyzed by the energy levels through system generated data. In EEHC, vitality is measured just for cluster heads and the information is effectively conveyed to base station. Vitality utilization of proposed framework is less contrasted with existing framework and packet conveyance proportion of proposed framework is high contrasted with existing framework. Subsequently proposed framework is more effective than existing framework.

The proposed strategy can be further enhanced to accomplish high packet conveyance proportion and network output. The energy consumption can be further diminished by expanding the cluster heads.

REFERENCES

[1] B Jiana and E Xu, "An Energy-efficient Security Node-based Key Management Protocol for WSN," 2nd International Symposium on Computer, Communication, Control and Automation, 2013.

[2] C. R. Lin and M. Gerla, "Adaptive Clustering for Mobile Wireless Networks", Journal on Selected Areas in

Communication, Vol. 15 pp. 1265-1275, September 1997.

[3] C. Intanagonwiwat, R. Govindan, and D. Estrin, "Directed diffusion: A scalable and robust communication paradigm for sensor networks," in Proc. Fourth Annu. ACM Int. Conf. Mobile Computing and Networking (MobiCom), Boston, MA, Aug. 2000, pp. 56–67.

[4] Jaydeep Barad and Bintu khadhiwala, "Improvement of deterministic key management scheme for securing cluster based sensor networks i.e. RING-LEACH", pp.978-1-4799-3486-7/14, 2014.

[5] MB Leonardo, O Hao and C Wong, "Sec leach: A Random Key Distribution Solution for Securing Clustered sensor networks," IEEE Network Computing and Application, pp.145-154, April 2006.

[6] M Ba, I Niang and B Gueye, "A Deterministic Key Management Scheme for Securing Cluster-based Sensor Networks," 8th International Conference on Embedded and Ubiquitous Computing IEEE, pp. 422- 227, 2010.

[7] Simplicio Jr MA, Barreto PSLM, Margi CB and Carvalho TCMB, "A survey on key management mechanisms for distributed wireless sensor networks," Computer Networks 2010.

[8] WB Heinzelman, AP Chandrakasan and H Balakrishnan, "An Application-Specific Protocol Architecture for Wireless microsensor networks," IEEE Transactions on Wireless Communications. vol. 1, pp.660–670, October 2002.

[9] W. R. Heinzelman, A. Chandrakasan and H. Balakrishnan, "Energy- Efficient Communication Protocol for Wireless Microsensor Networks", in Proceedings of IEEE HICSS, January 2000.

[10] Y. Wang, G. Attebury, and B. Ramamurthy, "A survey of security issues in wireless sensor networks," IEEE Communications Surveys, vol. 8, pp.2-23, 2006.

BIOGRAPHIES

Dr.M.Kezia Joseph obtained Ph.D and B.Tech from JNTU Kakinada, M.Tech from IIT Madras. She has published 20 research papers in various journals, international and national conferences. Her research interests include signal and image processing, wireless communications and medical electronics. She received young woman achiever and research excellency awards.

Shafia Tasneem obtained her Bachelor's degree in Electronics and Communication Engineering from Shadan women's college of engineering and technology affiliated to JNTUH, Hyderabad. She is currently pursuing Master's degree in Stanley college of engineering and technology for women's affiliated to OU, Hyderabad. Her zones of interest incorporate remote sensor systems, PC systems, system security and other most recent patterns in innovation.