Jestr

Journal of Engineering Science and Technology Review 13 (2) (2020) 82 - 91

JOURNAL OF
Engineering Science and Technology Review

Research Article

www.jestr.org

An Energy Efficient and Secure Mechanism (EES-WSN) in Wireless Sensor Networks for Reliable Data Transmission

Kakelli Anil Kumar*, Aju. D and Keshvi Khambhati

School of Computer Science and Engineering, Vellore Institute of Technology, Vellore, TN, 632014, India

Received 18 March 2019; Accepted 13 March 2020

Abstract

Wireless sensor networks (WSNs) having spatially dissipated and independent sensors for detecting heterogeneous events of industrial, military, environmental and health care services for betterment of society. Power efficiency, security and performance are the significant concern regions in designing WSNs. In real-world scenario the communication using wireless sensor networks (WSN) is becoming highly vulnerable and insecure. Numerous security mechanisms have been introduced for secure communication using WSN however none were accomplished the required level of security, performance and energy efficiency. Considering these essential requirements, it is highly essential to design a hybrid mechanism which can give the mentioned characteristics to provide energy efficient secure transmission in wireless sensor networks. Our experimental results are demonstrating that the proposed mechanism has achieved high performance in terms of packet delivery ratio (PDR), network throughput, energy-efficiency and secure communication in WSN.

Keywords: Wireless Sensor Network (WSN), Secure Mechanism, Reliable data transmission, Energy efficient.

1. Introduction

Wireless sensor network (WSN) is a prominent technology which covers an immense territory of utilizations, for example natural observing, open wellbeing, medicinal research, forest fire identification and so on. WSNs are involving limited processing and power source, constrained memory in like manner little for estimation [1]. In the focused network type, there is exchange off among security and vitality effectiveness. Since regarding security more noteworthy measure of computation is required consequently more prominent measure of memory is required hence proficiency isn't conceivable. One response for this issue can be that the structure of sensor nodes should accord their application. For example, for military applications security is most essential to the nodes which can be exorbitant. While for temperature detecting application use of security isn't critical issue anyway nodes shouldn't be expensive and should be imperativeness viable. For security using asymmetric key cryptography prompts more estimation and that prompts more energy usage. The energy preservation of WSN can be restricted by allowing the nodes called cluster heads. The information assembled from all the nodes in the network are totaled and lessen with the help of group heads. From this point forward, the totaled information is forwarded to the base station (BS) or sink node. And real issue is energy utilization and it's focused over the bunch heads. To determine the problem, the cluster-based routing is used to disperse energy usage with the cluster heads as shown in figure 1. Information gathering is a productive strategy for saving energy in sensor networks. The significant reason for information collection is to expel repetitive information as well as spare transmission vitality. The energy preservation of WSN can be restricted by allowing the nodes to form clusters. The data collected from every node in the system are aggregated and minimize it with the help of cluster heads and the data has forwarded to the base station. The main problem is cluster heads (group heads) are overloaded due to continuous data receive, aggregation, and dissemination. To decide the issue, the bunch-based directing is utilized to scatter essentialness utilization with the group heads. Data social affair is a beneficial methodology for sparing vitality in sensor systems. The critical purpose behind data gathering is to oust dreary data just as extra transmission essentialness. An information gathering calculation incorporates some total strategies to limit the information activity. It lessens the quantity of data trade between the Base Station and all the nodes. The execution of information assembling in wireless sensor nodes be described in view of the speed at which the detecting data can be accumulated and sent to the base station. Specifically, the theoretical quota to catch the bad marks for accumulation handling in the focused network is the limit with regards to many-to-single information accumulation. Information gathering limit tells how much proficient the sink can accumulate detecting information from every sensor from the nearness of obstruction [2]. The information accumulation capacity over Cluster Head causes noteworthy vitality wastage. If there should be an occurrence of same type of sensor networks, Cluster Head will before long bite the dust and again clustering should be started. It creates huge amount of vitality utilization. Other conventional safe routing conventions aren't ready for providing security against every possible conceivable aggression since all of them have supposition that all interest nodes have trustful and conjoint quality within them [3]. However, it isn't for all intents and purposes remedy on the off chance that if node gets into mischief or if there should arise an occurrence of insider attacks. WSNs are exceptionally defenseless to security final offer, energy imperatives and breach by malignant nodes. All disguised malevolent nodes there in wireless sensor networks

*E-mail address: anilsekumar@gmail.com
ISSN: 1791-2377
doi:10.25103/jestr.132.12

can truly mutilate the typical working of WSNs. If one time the vindictive nodes dispatch an assault, the attacks will be difficult to recognize. Sensor nodes are battery fueled which is protected with some restricted vitality asset and is one of the urgent requests with regards to network outline thought. The dependable directing, network inactivity, secure information accumulation as well as network energy are the critical problems in WSNs [4].

2. Literature Survey

Two SET conventions for Clustered WSNs, named SET-IBS and SET-IBOOS [5], by using Identity-Based programmed Signature (IBS) conspire and the Identity-Based Online/Offline advanced Signature (IBOOS) plot, separately. An IBS plot actualized for Clustered WSNs comprises of the activities like, setup at the Base Station, key identification and marking of the data sending nodes, as well as confirmation of the data accepting nodes. Furthermore, IBOOS conspire actualized for Clustered WSNs comprises of comparable activities as SET IBS yet it has disconnected specifying at the Cluster Heads and internet marking of the data sending nodes. In SET-IBS, safety relies on the stiffness of the problem names in the common space. SET-IBOOS additionally removes the calculation overhead for security, that's vital for WSNs, though it's safety relies on the stiffness of the discrete logarithm problem. It illustrates the achievability of the conventions namely SET-IBOOS and SET-IBS regarding the safety pre requirements as well as safety examination opposed to various assaults. The end analysis shows that, the mentioned conventions are having preferable execution over the recent safety conventions for Clustered WSNs, as far as safety overhead as well as energy utilization and it does neighbourhood validation, stockpiling cost is low yet the computational overhead is high.

Energy Optimized Secure Routing (EOSR) [6] depends over circulated confidence assessment structure to get recognize as well as detach malignant node. EOSR steering convention planned a multifaceted directing procedure, considering the node's confidence level, the rest of the vitality and way space. The mentioned procedure will not only just guarantee that information is sent via the confided in nodes, yet in addition adjusts energy utilization among the confided in nodes. This convention incorporates trust assessment, course development and course support. The trust assessment is in charge of computing the trust estimation of the node in light of the node's correspondence conduct. The course development exhaustively takes into consideration the trust measurement of the node, the rest of the vitality as well as the bounce check of course to locate a solid and vitality adjusted course. At the point if there is a malignant or an inadequate energy node in the course, course upkeep will inform the source node to set up another sending way. By recreating the current steering calculations, the EOSR convention indicates better execution in parcel conveyance rate, arrange throughput and node normal energy utilization.

Optimized Radio Energy Algorithm (OREA) [7] and Power-Aware Distance Source Routing (PADSR) bunching protocol is made for expanding age of the Network and decreasing the correspondence cost of WSNs. The OREA calculation is inferred conditions, which computes the energy productivity while information transmission and gathering are in dynamic mode by considering message length, transmission remove, electronic energy, and way lessening and enhancer transmitter. Conditions got from OREA is figure out the vitality dissemination between sender and recipient. The PADSR Protocol is a convention that depends on source-directed on-request steering. Node has course reserves having mindful origin courses. At whatever point the node finds out about new courses, it refreshes the sections in the course store. This calculations strategy gives Quality of Service and furthermore as for arrange lifetime, parcel conveyance rate and rest modes as for loads in the system is enhanced when contrasted with ABR and AODV conventions.

Secure and Energy Efficient Clustering Scheme with Data Aggregation protocol [8] is an energy effective grouping plan with collection of data to spare the transmission capacity prerequisite which thus draws out the system lifetime. This convention is prepared in two-phases. In the principal phase of bunching, all nodes compute their potential score in view of the closeness of development, leftover energy and thickness in disseminated way. Every node chooses whether it ought to end up a bunch head or not, by utilizing a potential score. In the second stages, each node picks its bunch head among those group head hopefuls. A Higher potential value having node is picked for the role of group head. At the point when a bunch part needs to transmit the information to aggregator (cluster head), and security is given utilizing RSA calculation. The recreation results demonstrated that the proposed method has enhanced throughput, parcel conveyance proportion with decreased bundle drop, less energy utilization and guarantees information security contrasted and LEACH.

Energy Efficient Cluster Routing Protocol (EET2FL) [9] is utilized to send bundles to remote sensor from origin sensor organize BS by means of the head of the group, utilizing the fuzzy rationale compose 1 with three parameters, for example, confidence factor and separation. The node having high confidence factor and close to base station CH is predicted by the fuzzy rationale will be chosen as ace message passer by utilizing fuzzy rationale of type 1. To make the group, it utilizes the fuzzy rationale control framework (FLCS) is utilized. The FLS comprises of 3 stages. Beginning with 1st stage which is fuzzifier, impedance motor be the second stage and the DE fuzzifier be the last one. The fuzzy rationale handles framework is actualized to pick the likelihood contender for best CH for sending the gathered information. Fuzzy rationale control framework (FLCS) registers the likelihood utilizing 3 information parameters as separation, energy and confidence factor. The FLCS yield has an arrangement of nodes having high likelihood of their 3 parameters. It will direct to build the existence time of system in addition to decrease the overhead of system, organize age is expanded as well as vitality is spared. Notwithstanding, the downside of this methodology is that tenets for EET2FL are settled as well as characterized by involvement.

A convention CH Restricted Energy Efficient Protocol (CREEP) [10] has been invented to conquer this confinement as well as to additionally enhance the system age by changing the Cluster Head choice limits in a 2-stage heterogeneous WSN by choosing Cluster Head in light of separation from different nodes and energy it has. Additionally, in CREEP, the idea of different bouncing is connected. In single-bounce mode, the sensors found more remote far from the BS cease to exist quicker because of the long-separate correspondence. With a specific end goal to palliate this issue, double bounce correspondence is being utilized between the CHs. Crawl approximates the square WSN field as a roundabout field and considers a circle of span R with BS at its middle. Any CH which is existing in this plate transmits its amassed

information specifically to the BS in one single bounce. In any case, for CHs lying outside this plate, double jump correspondence is required between the CHs. The CHs lying at a separation more prominent than R transmit their collected information to a CH that exists in the separation R of BS and not specifically to the Base Station. In this way, the vitality of the distant Cluster Heads is spared.

Intelligent Energy Aware Secured Algorithm for Routing (IEASAR) [11] that safeguards by utilizing a Trust relied approach and is vitality effective in the meantime. For the above-mentioned reason, other vitality effective convention is been proposed as a part of above invention utilizing Fuzzy C which considers node's trust esteem and way trust esteem that are sent to the Fuzzy grouping module to bunch the nodes. First, the fundamental trust is computed utilizing direct dialog with the neighbours. In every node, insightful specialist is sent considering the end goal to register the essential trust also to keep up record about the neighbours. Two kinds of trusts are kept up fundamental and current trust for every last node. Also, an altered least traversing tree approach is connected to recognize the base separation way between the sending and the goal node and thus an ideal and anchored directing way is chosen considering the limit esteem the CH are picked. The real accomplishments are decrease in energy use and increment in the measure of bundles conveyed.

Secure and Efficient ID-Based Aggregate Signature Scheme for WSN [12], the fundamental spotlight is on data respectability assurance, gives a profile based overall mark connive with an assigned verifier for WSN. Besides, the security of character based total mark conspire is thoroughly displayed in view of the computational Diffie-Hellman key exchange. ID-based total mark conspires for WSNs, which can pack numerous marks produced using sensory nodes into a tiny one, that is, it can lessen the correspondence as well as capacity worth.

A topology positioned secure and efficient Cost-Aware Secure directing (CASER) [13] protocol for Wireless Sensor Networks without relying on flooding. This protocol enables data to be sent using 2 steering procedures, arbitrary strolling and deterministic directing, for a similar system. It centres around two steering systems for message sending: most limited way message sending, and secure message sending through arbitrary strolling to make directing way eccentrics for source protection and sticking aversion. The appropriation of these two methodologies is dictated by the particular security prerequisites. CASER convention has two noteworthy points of interest: (I) It ensures composed energy usage of the sensor organize with the goal that the age of the Wireless Sensor Networks can be amplified. (ii) CASER protocol underpins various directing systems in light of the steering required basics, comprising fast/medium paced information conveyance as well as safe information conveyance to counteract steering drive back charge as well as pernicious movement sticking charges in Wireless Sensor Networks. Both imaginary investigation as well as recreation outcomes shows that CASER has a brilliant directing execution as far as vitality adjust and driving way dispersion for driving way security.

TESRP is extraordinary compared to other trust based secure steering convention, however it is not safeguarding from wormhole assault. The convention named Fighting against Wormhole Attack in Trust and Energy Aware Secure Routing Protocol (TESRP) in WSN [14] safeguards against wormhole assault in TESRP by utilizing confidence-based calculation and arrangement idea. The convention named trust calculation combined with succession no. idea is been utilized for anchoring TESRP from wormhole assault. The trust demonstrates figures CRF (Composite Routing Function) measurement, which consolidates node's lingering vitality, confidence, and bounce tallies. For registering expense of CRF, leftover vitality, confidence and jump include are totalled weighted way. Choice of nodes to course bundles should be possible just on the off chance that they are dependable and have leftover energy more than determined limit. It incorporates course setup process which has RREP (Route Reply) as well as RREQ (Route Request) process, when there are few broken as well as pernicious nodes in the system. Reproduction results demonstrate the correlation of estimations of TESRP in 3 classifications (before wormhole, many attacks and after counteractive action) as far as leftover vitality, Packet conveyance proportion, throughput and end-to-end deferral so in this way noteworthy increment in execution is seen.

SALMA is elaborated as State-Aware Link Maintenance Approach [15] combines two of the steering conventions called the receptive and proactive for diminishing the over-head for the greater part for nodes and expands arrange execution by lessening heap of system revelation alluvia on dynamic nodes. The above-mentioned convention partitions all system nodes in 3 classes: (1) mindful as well as dynamic nodes called as dark node, (2) mindful yet not doing information exchange aside from information sending which are known as dim nodes (3) white nodes who are sit still as well as don't keep any steering data. SALMA utilizes an information arrangement known as Keep Awake Buffer, clarified in following segments, for deciding the sort of all nodes. The methodology works responsively in start of any arrangement. Once any node begins the activities the course is kept up productively to diminish the over flowing of control bundles for course disclosure. This proposed protocol uses measurements of utilization for node. On the off chance that a node is ceaselessly inactive, this node is kept sit without any sending bundle or its own usefulness can repudiate moving as well as it. A functioning node intermittently recognizes its neighbours to refresh the course data. Similar to Optimized Link State Routing (OLSR) connections as well as neighbours were detected by creating a message HELLO intermittently. The sit out of gear nodes don't react to the HELLO messages considering constantly the final goal to decrease the utilization of their restricted assets. This convention is profoundly impacted by Dynamic Source Routing (DSR) convention for course disclosure system and some way or another in course support. Course is kept up principally proactively by embracing a few fundamentals of OLSR convention. Results demonstrate that SALMA gave direct and aggregately better outcomes when contrasted with DSR, OLSR, ZRP, and HOPNET conventions as far as power devoured, steering overhead, number of rounds finished and so on.

A secure energy efficient location aware information collecting way [16] is acquainted with protected information collection. An Elliptic Curve Diffie Hellman Key Exchange (ECDHKE) calculation used for age of key as well as trade of key among the sensor-nodes to keep up protection as well as keep the information being malevolent nodes. This convention initially networks development at that point key age utilizing ECDHKE plot at that point neighbours estimation by thinking about the separation first and after that from the nodes with less separation it checks energy of those less inaccessible nodes and after that routes processing checks confirmation and does information encryption where total of all the node's information is done at base station to send

information to the goal node. The execution of the proposed conspire is approved as far as vitality usage, throughput and drop of parcel, lifetime of system and lingering energy.

Considering the final goal to expand system inertness as well as to settle the protection barriers prompted by covered malevolent hubs in WSN, the lingering trust as well as vitality esteems are utilized for framing an anchored grouping, the system lifetime is expanded by utilizing the reinforcement nodes with a specific end goal to disseminate the heap amidst the Clusters which are protected as well as Reliable Multipath Node Disjoint Route Discovery algorithm (SLBC-RMRD) [17] is invented. A safe load adjusted node has bunching and utilizing trust estimations of nodes, auxiliary reinforcement CH nodes and giving dependable hub disjoint multi way course finding strategy in the remote sensor systems. The veiled malevolent nodes are distinguished in view of social shifting of nodes and the system age of the sensor organize been expanded by adjusting the leftover energy, trust esteems and the reinforcement CH nodes is utilized to apportion the heap amidst the groups. Amid bunching, the node makes utilization of DSDV directing convention for the underlying information sending among the far generally node and the given node. After the underlying information sending, the rest of nodes are resolved and esteems based on trust is registered in view of the affirmation bundles gotten by nodes amid transmission. At that point the solid disjoint multipath course finding is done where bunch head announces a course ask for parcels with a few parameters with the mystery key and that ought to coordinate with the neighbouring nodes and consequently MAC is figured at BS and that is checked with the sent MAC from the source node and along these lines if a hidden pernicious nodes dispatch wormhole assault or Sybil assault, at that point MAC processed at the goal won't be coordinated and the course will be for all time disengaged. The group containing the noxious nodes can be distinguished in view of the bundles dropped. On the off chance that there are tremendous bundles dropped in the group, at that point that bunch is considered to have a noxious node. The recreated test results taken with help of Network Simulator 2 stage demonstrate that the invented technique is capable of limiting impact of malignant nodes as well as enhances the age of the system for the sensor arrange by adjusting the esteems based on trust and leftover vitality of sensor nodes.

LEACH convention is confronting the accompanying issues which diminish its execution on being sent in the system. Just inward territory nodes can take an interest as bunch leader of the system. On the off chance that all the inward nodes were dead, the fringe nodes wind up disengaged in view of not having any CH. Thus, it will diminish the age of the system. EESRP is to make the coveted changes in the EECHS plot as well as furthermore build the framework increasingly An Energy Efficient Secure Routing Protocol [18] presents another idea of "status" for every group shaped. The status which is lower as compared to other nodes implies that particular bunch is having more distant separation from BS. To avert assaults on information amid sending, each sending of information is gone before by sending a parcel which is checked to goal. This Protocol decreases the intra-group correspondence distance. The calculation shows the difference in states experiencing in the system as well as how the level of vitality of every hub switch with time. It demonstrates the quantity of nodes not alive in every round as well as vitality expended in every round. This Algorithm has Initialization stage where every one of the nodes are introduced and ideal separation is computed for every node than in CH choice stage the arrangement of bunch heads is shaped in view of the energy. At that point assailant node location stage is performed where check bundles are sent from nodes to group heads and after that they sit tight for the reaction check parcel consequently from the CH, if the arrival check parcel isn't acquired by the nodes than they announce CH as workforce or malignant node. Recreation demonstrates that proposed plot has preferred energy effectiveness over EECHS conspire.

A Convention Energy efficient LEACH [19] for information collecting gives a vitality productive directing in Wireless Sensor Network in light of compelling information troupe and ideal grouping. In the above -mentioned framework, a CH is chosen for every group for limiting the vitality scattering of the sensor nodes as well as to improve asset usage. Nodes having the most extreme leftover vitality can get the vitality effective directing. Henceforth, the most elevated remaining energy nodes are chosen to forward the information to BS. The Gaussian circulation display is consolidated for node sending. The information is sent to BS from diverse sources in view of the vitality proficient directing system for which first bunch arrangement is performed and after that computation of remaining energy for every one of the nodes is performed at that point if the leftover energy is higher than it is chosen as ideal CH conveyed with information collection and afterward sending nodes are chosen in light of most elevated lingering energy after the information is sent to BS. On the off chance that the remaining energy isn't high then it is dealt with as non-CH node. It furnishes better bundle conveyance proportion with lesser vitality usage. The test outcome demonstrates that the invented EE-LEACH gives preferred execution over the current LEACH Protocol and (EBRP) Energy-balanced routing Protocol as far as better bundle conveyance proportion, less end-to-end deferral and vitality utilization. It's clearly demonstrates that the invented EE-LEACH can enhance the age of the system.

To defeat the issue of SPIN convention, for example, daze forward and information out of reach, another convention named Energy Efficient Modified SPIN Protocol with High Protection in WSN [20] has been proposed and configuration adjusted SPIN directing convention to spare vitality and give protected sending to limit overhead with information conveyance ensures. This convention finds an ideal way and productive usage of convention for information transaction, set up course lastly exchange information to particular nodes. The oddity in this proposed convention is more secure information transmission than SPIN. First information broadcasting stage is executed where source node communicates ADV message to its neighbours which contains information properties. Subsequent to getting message of ADV every node needs to check whether the node has proper amount of vitality to do errands and the nodes which does not have information will send a message of REQ to origin node. At that point in information transmission stage, the origin node sets up a course to transfer the information to the goal node. At that point after stages give data about malevolent, out of date or dead nodes and afterward keeping up every one of the requirements remaining nodes are chosen and the course is shaped. The re-enactments have been done by new working framework TOSSIM to contrast information exchange rate and correspondence security and lifetime of systems.

3. Clustering of Wireless Sensor Networks

Clustering is essential techniques for delaying the system lifetime in remote sensor systems (WSNs). It includes

gathering of sensor nodes into bunches and choosing group heads (CHs) for every one of the bunches [21, 22]. CHs gather the information from separate group's nodes and forward the accumulated information to base station or Sink-hub [23].

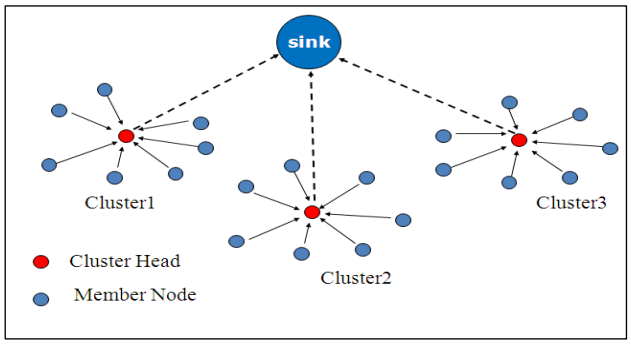

Fig. 1. Clustering of Wireless Sensor Network

In this segment, we condense these focal points and in addition the destinations of WSN bunching as takes after:

a) Scalability: In grouping steering plan, sensor nodes are isolated into an assortment of bunches with various task levels. The CHs are in charge of information accumulation, data dispersal and system supervision, and the information collection as well as their detection is done by MNs in their environment. Bunching topography can limit course arrangement inside the group, therefore lessen the span of directing table put away at the individual sensor points.

b) Information Aggregation/Fusion: Data mixture/blend, which is the path toward hoarding the data from various hubs to take out redundant transmission and give-interlaced data to the BS, is a valuable framework for WSNs to save vitality. The most popular data absolute/mix system is gathering data aggregate, in which each Cluster Head sums the assembled data and transmits the interlaced data to the BS. Ordinarily Cluster Heads are formed a tree structure to transmit totaled data by multi-bouncing through various CHs which results in basic vitality hold reserves.

c) Limited Load: Since sensors may deliver gigantic overabundance data, data aggregation or mix has ascended as a basic statute and focus in WSNs. The guideline thought of data aggregate or blend is to merge data from different sources to discard dreary data transmissions, and give a rich and multi-dimensional viewpoint of the destinations being checked. Many bundling guiding plans with data absolute limits require careful assurance for gathering approach. For clustering topology, all gathering people simply send data to CHs, and data combination is performed at the CHs, which help to fundamentally diminish transmission data and extra vitality.

d) Energy Consumption: In packing controlling arrangement, data complete serves to definitely diminish transmission data and extra vitality. What's more, bundling with intra-gathering and between cluster trades can reduce the amount of sensor hubs playing out the task of long partition correspondences, thusly allowing less vitality use for the entire framework. Furthermore, just CHs play out the task of data transmission in bundling coordinating arrangement, which can save a great deal of vitality usage.

e) Robustness: Bundling coordinating arrangement makes it increasingly supportive for compose topology control and responding to orchestrate changes including hub extending, hub movability and unpredicted dissatisfactions, etc. A packing directing arrangement simply needs to adjust to these movements inside individual gatherings; along these lines, the entire framework is even more dominant and increasingly accommodating for organization. With a particular true objective to share the CH commitment, CHs are all around turned among all the sensor hubs to keep up a vital separation from the single reason for dissatisfaction in gathering guiding counts.

f) Crash Avoidance: In the multi-bob level model, the remote medium is shared and directed by solitary hubs; consequently, this model can result in low adequacy in the advantage use. On the other hand, in the multi-bob packing model, a WSN is isolated into gatherings and data correspondences between sensor hubs include two modes, i.e., intra-bundle and between gathering, exclusively for data collection and for data transmissions. Similarly, resources can be dispensed symmetrically to each gathering to diminish impacts among packs and be reused aggregate by gathering. In like manner, the multi-hop gathering model is fitting for far reaching scale WSNs.

g) Load Balancing: In fact, even flow of sensor hubs among the gatherings is regularly considered for group advancement where CHs play out the endeavor of data dealing with and intra-cluster organization. When in doubt, creating identical estimated clusters is gotten for illustration out the framework lifetime since it keeps the inopportune vitality exhaustion of CHs. In addition, multi-way controlling is a system to achieve stack altering.

h) Adaptation to non-critical failure: The appropriateness of WSNs has decent numerous unique situations, sensor nodes may experience the ill effects of energy consumption, transmission blunders, equipment breakdown, malevolent assaults et cetera. With applications, for example, sea tempest displaying and following imagined to use an expansive no. of little sensor hubs, the expense with respect of every sensor node is obliged. Attributable to critical requirements on the expense, and along these lines on the nature of sensor bits, and the frequently antagonistic conditions in which they are conveyed, sensor systems are inclined to disappointment. Accordingly, adaptation to non-critical failure is an essential test in WSNs. In order to avoid the loss of important data from key sensor hubs, adjustment to inside disappointment of CHs is normally required in this kind of employments, accordingly effective accuse tolerant philosophies must be created in WSNs.

i) Affirmation of Connectivity: Sensor hubs when in doubt transmit data to no less than one BSs by methods for a single skip or multi-bounce guiding in WSNs, as needs be paying little respect to whether the data is viably passed on to the BS is essentially directed by the system of each hub to its next hop hub end route. Also, sensor hubs that can't talk with some other sensor hub will get bound and their data can never be transmitted to the BS. Thusly, confirmation of system is an essential target of clustering coordinating traditions in WSNs.

j) Vitality Hole Avoidance: The hubs closer to the BS to deplete their vitality first due to data packet accumulation, leaving an opening near the BS, distributing the whole

framework, and shielding the outside hubs from sending information to the BS, while numerous exceptional hubs still have vitality. Especially, uneven gathering is one of the systems for stack altering. In this technique, a smaller bundle length near the sink and a greater gathering range a long way from the sink are portrayed exclusively, so the vitality use of getting ready data in the middle of cluster is less for pack with more diminutive compass, and therefore more vitality can be used to exchange data from remote hubs.

k) Network Lifetime: Network lifetime is an unavoidable idea in WSNs, in light of the way that sensor hubs are obliged in charge supply, getting ready limit and transmission information exchange limit, especially for employments of pitiless conditions. By and large it is basic to restrict the vitality usage for intra-pack correspondence by CHs which are more extreme in resources. Additionally, sensor hubs that are close to by far most of the sensor hubs in the bundles should be slanted to be CHs.

l) Nature of Service: The system applications and the functionalities of WSNs incite the necessity of nature of administration (QoS). Normally, successful example, less postponement and impermanent accuracy are required. It is troublesome for all the steering conventions to fulfill every one of the prerequisites of QoS, in light of the fact that a few requests may break at least one convention standards. Existing bunching steering approaches in WSNs fundamentally center around expanding energy proficient instead of QoS bolster.

4. Architecture of Energy Efficient and Secure (EES-WSN) Mechanism

Considers a set of wireless sensor nodes randomly deployed in the environment and then using set of functions like residual energy ($E_{residual}$), hop count (path length) (hc), trust values (tv) etc. are calculated for all of the nodes and then all the nodes are given as an input to a clustering algorithm where using all the above calculated values of the nodes the cluster heads will be selected from the set of various wireless sensor nodes and as a result the whole set of random nodes will be converted into set of clusters, after that the route formation process starts by neglecting at the dead nodes and malicious nodes and then the packets are being transmitted to destination from source node using this path in an efficient and secure way. Lastly, energy consumption of a packet transmitted is calculated.

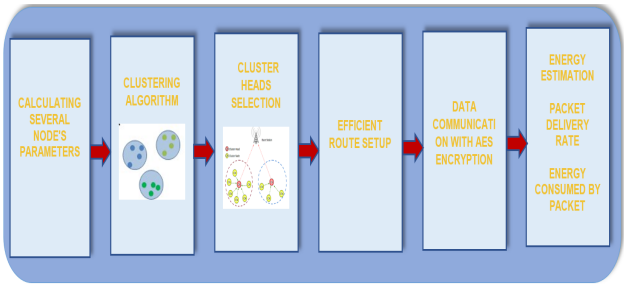

Fig. 2. Architecture of EES-WSN

Table 1. EES-WSN Secure Data Transmission Algorithm

start
Step 1:- Set of nodes N= {N1, N2…, Nn}
Step 2:- Set $E_{residual}$, hc, tv for N
Step 3:- N→*initialize* EES- Clustering
Step 4:- *routing path* SN→BS
- initialize *dataQueue, ChDataQueue, noofWirelessNode*
Step 4b:- initialize *clusterHeadSelection()*
equation 1→ CH
Step 4c:- choose *ClusterFormation()*
Step 5:- N1→ *CHIndex=0* and *SCHIndex=0*
Step 6:- set 'D0'
Step 7:- Choose *CHERx* and *CHETx*
Step 8:- estimate node energy/round
Step 9:- N status=2
Initiate identification of SCH
Step 10:- N status=3
"confirm SCH"
Step 11:- initiate AES with initial key ki
Step 12:- encrypt DP at SN
Step 13:- decrypt DP at BS
end

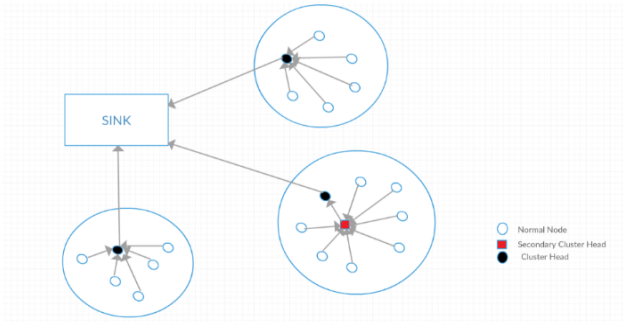

Fig. 3. EES-WSN Route establishment

5. EES-WSN Mechanism

The proposed EES-WSN mechanism is having a methodology where the initialization function will initialize the node parameters like *dataQueue, ChDataQueue, noofWirelessNode,* cluster head percentage, initialize the cluster head and forms cluster by calling *clusterHeadSelection()* and *ClusterFormation()* for each node as described in table 1. The cluster head (CH) selection process is initiated where the round number "0" is given as an input to the method and it first initializes all nodes as Normal node with their *CHIndex=0* and *SCHIndex=0*. The battery power and *distanceToBS* is calculated and also a random value called *temp_rand* is created and compared with recharge value of the node, and if the equation 1 is true then the node satisfying these criteria to select CH. According to the relation between node's distance through base station and D0 value the cluster head's *CHERx* and *CHETx* is set. Then after the cluster head selection process is completed, the optimal cluster formation method is called.

$$temp\_rand <= rechargeValue \quad (1)$$

In optimal cluster formation method, it sets cluster heads for first 5 clusters where others are considered as normal nodes. Then the cluster formation method is called where for each node having battery power greater than 0, it will ensure whether that node is the head of the cluster or not which is determined using its type and if it is cluster head then it's temp distance is calculated by taking minimum value between distance to base station and a temporary variable minimum distance and based on the above logic the cluster head's node distance till base station is updated. After wards the secondary CH formation is called where based on the vitality of the CH

node represented by E(i), the distance from BS represented by d(i) where i be the node's index in equation 2. If the cluster head node than the secondary satisfies this logic CH is chosen for this particular cluster based on the highest vitality having node in that cluster.

$$E(i) < E_{avg} \text{ or } d(i) > d_{avg} \quad (2)$$

Eavg is average energy of all nodes specific to a round. d_{avg} is the average distance of all the nodes specific to a round. Now when any message is to be sent, it goes to the handle message method where the incoming message is *cast* to *custMsg* type and based on the value of network status the messages will be sent and processed. If the value of network status value is equal to 2 than the data reliable on whether the secondary CH is appointed for that cluster, the data will be given to secondary CH than another method for sending the data to cluster head is called. If the secondary cluster head is not appointed than directly the method for sending the data is to cluster head is called. If the network status value is equal to 3 than the method for sending the data to sink is called. Output files are generated as keeping the record of several properties of the node in every round like their remaining energy, the index of cluster head node they are assigned to if it's a secondary cluster head or a normal node, the indexes of secondary cluster head a node is linked to if it's a normal node, number of nodes dead as well as alive in every round of transmission, number of cluster heads, number of secondary cluster head, Energy Consumption in each round, number of sink packets generated round wise. In addition, the scalar and vector data are generated for all the above characteristics and properties mentioned and node wise is displayed in the bar graph shown in screenshots section. For the security of the network, AES algorithm is used with initial key. The row shifting is performed where rows are shifted to left and mixing of columns with other processes like add round key and all are performed for giving security and providing confusion, which is to be, transmitted it encrypted. The key is read according to the node number, and using it the data is encrypted and is recorded with the respective round number in a text file and thus sent across the network and finally to destination node, which is a cache node of the whole network. AES decryption is performed at the destination node using the same key file to read the node specific key to decrypt the data accordingly. The decrypted data with the node number is also recorded by sink node in a text file.

6. Performance Comparison of EES-WSN Mechanism

Encryption is very important in data transmission through the network route using DES encryption algorithm with 56-bit key, and DES is easily cracked due to key size. AES algorithm has been proposed in which the data is divided into 4*4 column of 16 bytes, then in the key expansion phase the initial key is been processed using a structured process named rijndael's key schedule and the other keys are derived for other rounds using the initial key. AES for every round new key is provided, the byte substitution step is used to change the data in non-linear way, which applies confusion to the information. Even though there are various ongoing attacks as well as any side-channel assaults, AES dependably stays secure. The resistance of AES towards plain text attacks, DOS attacks, shortcut attacks and many more. Comparing various encryption algorithms like RSA, DES, 3DES, AES, BLOWFISH based on memory used as per table 2, the time taken to encrypt and decrypt individually we can conclude that either AES or BLOWFISH encryption algorithm can be used to efficiently encrypt the data and transmit it. The proposed protocol considers remaining vitality of a particular node, distance and the trust factor of that node to appoint it as a CH or a non-cluster head node, and considers data aggregation approach that aggregates the data from all the nodes at a cluster head or base station for energy efficiency.

7. Experiments and Results Investigation

The simulation experiments are conducted using Omnet++ Discrete Event Simulator V.5. Table 3 shows the simulation parameters for analysing the performance of EES-WSN mechanism. Figure 6 shows the routing path (blue dotted line) and the data transmission between two nodes 28 and 7. On the simulation window left bottom side the network parameters like remaining energy, number of CH and SCH, and average remaining energy. Figure 7 represent the encrypted routing for secure data transmission with AES algorithm from source to sink nodes. Figure 8 and 9 shows the energy consumption of each cluster and number of packets received by sink node. Table 4 represents Node's cluster head index in for each simulation round. Network throughput at base station (TP_{BS}), packet delivery ration PDR at base station (PDR_{BS}), Network life time (N_T), data packet loss rate (LR_{BS}) and Energy efficiency (E_{eff}) are estimated from equation 3, 4, 5, 6 and 7 respectively.

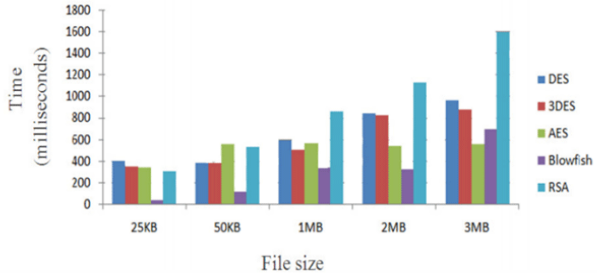

Fig. 4. File Size vs. Encryption Time of DES, 3DES, AES, Blowfish & RSA

Figure 11 and 12 shows node-wise encrypted message with AES encryption during transmission of packets between SN to BS and message decryption using AES algorithm at BS. Figure 13 represents node 0's vector and scalar data generated where yellow color represents throughput of the node, green color represents number of data in sink at that transmission time and dark blue color represents number of data sent to CH.

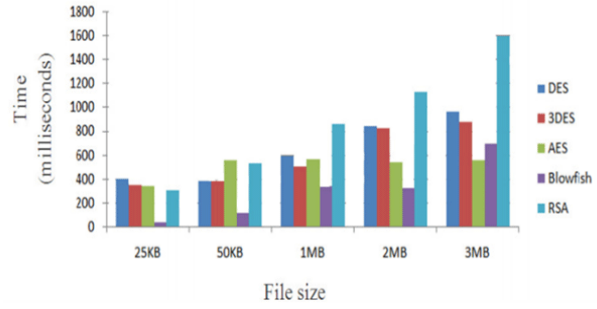

Fig. 5. File Size vs. Decryption Time for DES, 3DES, AES, Blowfish & RSA

Table 2. Memory requirement of secure algorithms

Algorithm	Memory (KB)
DES	18.2
3-DES	20.7
AES	14.7
Blowfish	9.38
RSA	31.5

$$TP_{BS} = \left(No.\ of\ \text{DP}\left(bits\right) / \ \text{TT}\ (sec)\right) \quad (3)$$

$$PDR_{BS} = \{\text{DP}\ received\ by\ \text{BS}\ \left(bits\right) \ / \ \text{DP}\ sent\ by\ SN\ \left(bits\right) \quad (4)$$

$$N_T = ST\ at\ \text{N}_1\ dead\ /\ Total\ \text{ST}_{\text{Network}} \quad (5)$$

$$LR_{BS} = \left(No.\ of\ \text{DP}\ Lost\ / \text{No.}\ of\ expected\ \text{DP at BS}\right) * 100 \quad (6)$$

$$E_{eff} = B / \mu C_T = TP_{AV} * t / \mu C_T \quad (7)$$

Table. 3. Simulation parameters

Parameters	Value
Number of Nodes (N)	50 to 100
Terrain area	100*100 m^2
No. of CH	5 to 7
No. of SCH	4 to 6
Number of Sink node	1
Communication Range (CR)	100 to 200 m
Bandwidth	244.14 KB
Number of Groups	4
Data Transmission	N→SCH→CH→Sink
Mode of Deployment	Random
Propagation limit	-111 to -222
Noise level	5 to10 dB
Radio Mode	Radio Accnoise
Frequency	2.4 ISM G.Hz
Secure Clustering Algorithm	EES-WSN with AES

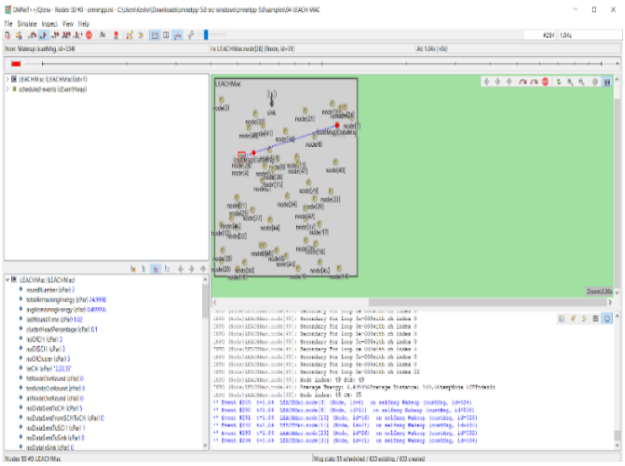

Fig. 6. Routing strategy of EES-WSN mechanism

Figure 14 and 15 represents node 8's and 40's vector and scalar data generated where blue color represents throughput of the node, green color represents number of data in sink at that transmission time.

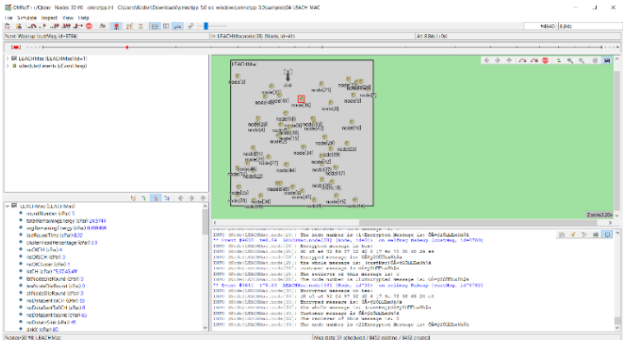

Fig. 7. EES-WSN with AES encryption

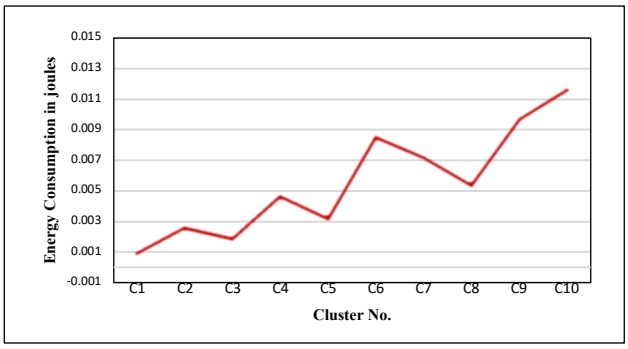

Fig. 8. Energy consumption of EES-WSN- Cluster wise

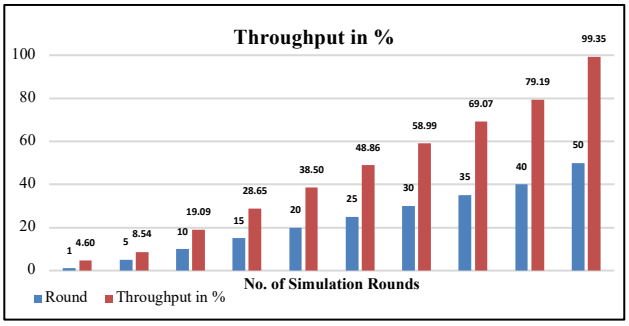

Fig. 9. Throughput in packet per rounds at sink node using EES-WSN

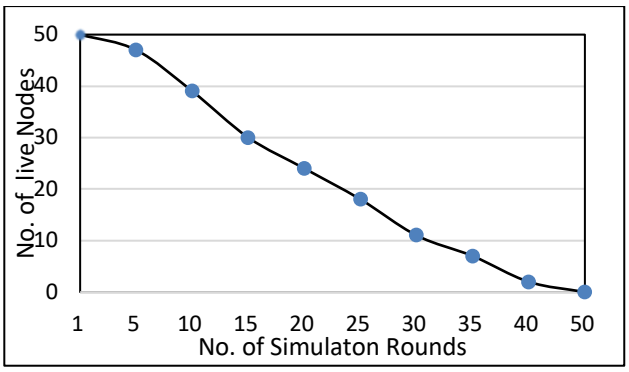

Fig. 10. Number of Alive Node using EES-WSN

Table 4. Node Index Vs Cluster Head Index of Node of EES-WSN

Round No	Node Index	CHI Index
1	1- 4	2, 35
5	5 -8	2, 35,
10	9-16	2, 22, 35
15	17-20	2, 22, 35
20	21-25	2, 22
25	26-29	2, 22, 35
30	30-36	22, 35
35	37-40	2, 22
40	41-44	2, 35

45 50	44-48 48-50	22 22

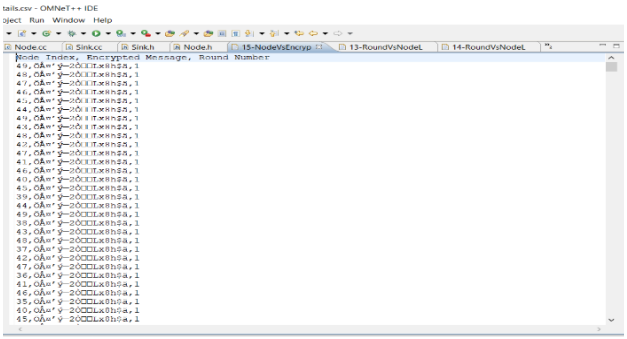

Fig. 11. Node Index Vs AES Encrypted Message of EES-WSN

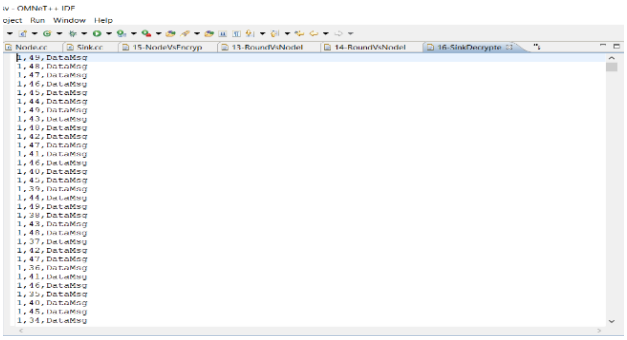

Fig. 12. Node Index Vs AES Decrypted Message of EES-WSN

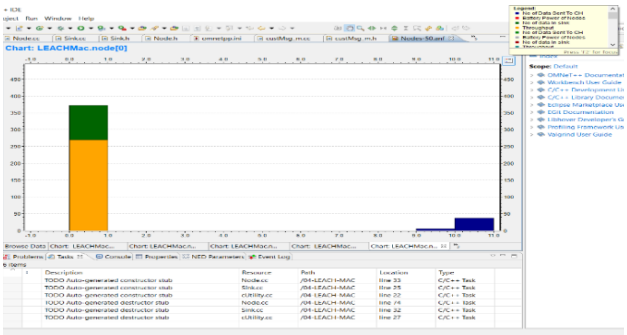

Fig. 13. Vector and scalar data of Node 0 using EES-WSN

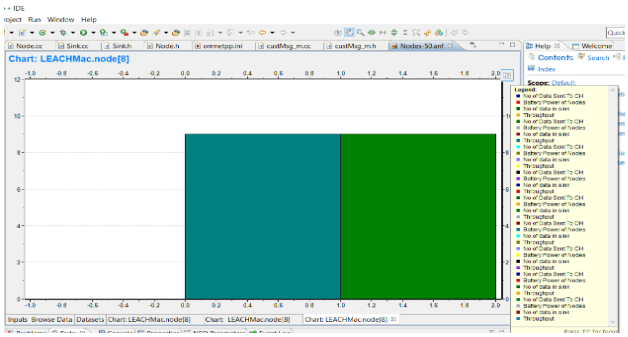

Fig. 14. Vector and scalar data of Node 8 using EES-WSN

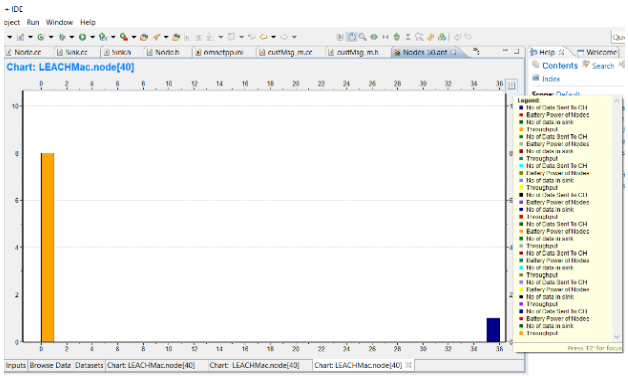

Fig. 15. Vector and scalar data of Node 40 using EES-WSN

8. Conclusion

The proposed energy efficient and secure mechanism (EES-WSN) has achieved the reliable data transmission in wireless sensor networks with energy efficiency. EES-WSN has efficient scheme for the election of secondary cluster head which can aggregate messages from nodes to minimize the load on the cluster head. This mechanism has achieved the energy efficiency by aggregating the messages from the nodes at the cluster heads (CHs). The secondary cluster heads (SCH) are selected based on the energy levels of cluster heads. Using AES algorithm in EES- WSN mechanism has resulted secure data transmission by consuming limited energy ad computation resources for encryption and decryption at sender and sink nodes in WSN. Therefore, energy efficiency and secure transmission are achieved by the proposed EES-WSN mechanism as compared to existing secure clustered protocols in WSN environments.

References

[1] S. K. Gupta, S. Kumar, S. Tyagi, and S. Tanwar, "Energy Efficient Routing Protocols for Wireless Sensor Network," in *Advances in Intelligent Systems and Computing*, 2020.

[2] D. B.D. and F. Al-Turjman, "A hybrid secure routing and monitoring mechanism in IoT-based wireless sensor networks," *Ad Hoc Networks*, 2020.

[3] S. Abbasian Dehkordi, K. Farajzadeh, J. Rezazadeh, R. Farahbakhsh, K. Sandrasegaran, and M. Abbasian Dehkordi, "A survey on data aggregation techniques in IoT sensor networks," *Wireless Networks*, 2020.

[4] A. M. Morsi, T. M. Barakat, and A. A. Nashaat, "An efficient and secure malicious node detection model for wireless sensor networks," *International Journal of Computer Networks and Communications*, 2020.

[5] H. Lu, J. Li and M. Guizani, "Secure and Efficient Data Transmission for Cluster-Based Wireless Sensor Networks," in *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 3, pp. 750-761, 2014.

[6] T. Yang, X. Xiangyang, L. Peng, L. Tonghui, and P. Leina, "A secure routing of wireless sensor networks based on trust evaluation model," *Procedia Computer Science*, vol. 131, pp. 1156–1163, 2018.

[7] J. T. Thirukrishna, S. Karthik, and V. P. Arunachalam, "Revamp energy efficiency in Homogeneous Wireless Sensor Networks using Optimized Radio Energy Algorithm (OREA) and Power-Aware

Distance Source Routing protocol," *Future Generation Computer Systems*, 2018.
[8] B. A. Mohan, K. R. Dayananda, and H. Saroja Devi, "Energy efficient clustering scheme with secure data aggregation for mobile Wireless Sensor Networks (EECSSDA)," *Proceedings of 2016 Online International Conference on Green Engineering and Technologies, IC-GET 2016*, vol. 4, no. 5, pp. 106–111, 2017.
[9] Balaji, S., Golden Julie, E. & Harold Robinson, Y. Development of Fuzzy based Energy Efficient Cluster Routing Protocol to Increase the Lifetime of Wireless Sensor Networks. Mobile Network, vol 24, pp 394–406, 2019.
[10] Dutt, S., Agrawal, S. & Vig, R. Cluster-Head Restricted Energy Efficient Protocol (CREEP) for Routing in Heterogeneous Wireless Sensor Networks. Wireless Pers Commun 100, 1477–1497 (2018).
[11] Selvakumar, K., Sairamesh, L. & Kannan, A. An Intelligent Energy Aware Secured Algorithm for Routing in Wireless Sensor Networks. Wireless Pers Communications, vol. 96, pp. 4781–4798, 2017.
[12] L. Shen, J. Ma, X. Liu, F. Wei, and M. Miao, "A Secure and Efficient ID-Based Aggregate Signature Scheme for Wireless Sensor Networks," IEEE Internet of Things Journal, 2017.
[13] R. S. Sheikh, S. Sahare, and A. Manusmare, "Cost Aware Secure Network Protocol Design for Wireless Sensor Network," vol. 3, no. 4, pp. 482–485, 2017.
[14] S. Renubala and K. S. Dhanalakshmi, "Trust based secure routing protocol using fuzzy logic in wireless sensor networks," in *2014 IEEE International Conference on Computational Intelligence and Computing Research*, 2015.
[15] M. M. Umar, N. Alrajeh, and A. Mehmood, "SALMA: An Efficient State-Based Hybrid Routing Protocol for Mobile Nodes in Wireless Sensor Networks," *International Journal of Distributed Sensor Networks*, 2016.
[16] M. Roseline Juliana and S. Srinivasan, "SELADG: Secure energy efficient location aware data gathering approach for wireless sensor networks," *International Journal of Applied Engineering Research*, Vol. 8, No. 3, 2015.
[17] P. Bhat and K. S. Reddy, "Energy efficient detection of malicious nodes using secure clustering with load balance and reliable node disjoint multipath routing in Wireless Sensor Networks," in *2015 International Conference on Advances in Computing, Communications and Informatics,* 2015.
[18] Mehra, M., Dabas, P., & Tech, M, "Energy Efficient Secure Routing Protocol (EESRP) in Wireless Sensor Network," International Journal for Innovative Research in Science & Technology, vol 2, Issue 03, 2015.
[19] G. S. Arumugam and T. Ponnuchamy, "EE-LEACH: development of energy-efficient LEACH Protocol for data gathering in WSN," *Eurasip Journal on Wireless Communications and Networking*, 2015.
[20] R. Dutta, S. Gupta, and D. Paul, "Energy efficient modified SPIN protocol with high security in Wireless Sensor Networks using TOSSIM," in *Proceedings of 2014 3rd International Conference on Parallel, Distributed and Grid Computing, PDGC 2014*, 2015.
[21] M. Revanesh, V. Sridhar, and J. M. Acken, "Secure Coronas Based Zone Clustering and Routing Model for Distributed Wireless Sensor Networks," *Wireless Personal Communications*, 2020.
[22] L. Lopriore, "Key management in wireless sensor networks," *Information Security Journal*, 2019.
[23] I. Tomić and J. A. McCann, "A Survey of Potential Security Issues in Existing Wireless Sensor Network Protocols," *IEEE Internet of Things Journal*, 2017.

List of Symbols and Abbreviations

WSN- Wireless sensor networks
CH – Cluster Head
SCH-Secondary cluster head
BS – Base Station/Destination node
d/D – distance between two sensor nodes
EES- Energy Efficient and Secure Mechanism
PDR- Packet delivery ratio
SET-Secure and Efficient data Transmission
IBS- Identity-Based digital Signature
IBOOS- Identity-Based Online/Offline digital Signature
EOSR-Energy Optimized Secure Routing
OREA-Optimized Radio Energy Algorithm
PADSR-Power-Aware Distance Source Routing
RSA- Rivest–Shamir–Adleman algorithm
DES- Data encryption standard
AES- Advanced encryption standard
LEACH- Low energy adaptive clustering hierarchy protocol
IBAS- Identity-based aggregate signature
CDH- Computational Diffie–Hellman
DSR- Dynamic source routing
OLSR-Optimized Link State Routing Protocol
ZRP- Zone routing protocol
HOPNET-Hybrid Ant Colony Optimization Routing Algorithm
DSDV- Destination Sequenced Distance Vector
MAC- Medium Access control
EESRP- Energy Efficient Secure Routing Protocol
EECHS- Energy Efficient Cluster Head Selection protocol
SPIN- Sensor protocol for information
TOSSIM- Discrete event simulator for TinyOS sensor networks
dataQueue- Data packets in queue
ChDataQueue- Cluster head data queue
noofWirelessNode- number of sensor nodes
clusterHeadSelection()- cluster head selection
ClusterFormation()- cluster formation
CHIndex and SCHIndex – cluster head index and secondary cluster head index
distanceToBS- Distance to base station
temp_rAND- *temporary distance to base station*
CHERx and *CHETx*- Cluster head receiving and transmission power
Eavg- average energy of all nodes specific to a round
d_{avg} -average distance of all the nodes specific to a round
TT- Transmission time
DP/ DP_N- Data packet/s
ST- Simulation time
B-Total delivered data packets successfully
$\mu \rightarrow$ 1 unit of consumed energy for transmitting 1 DP
C_T - DP_N count needed to transmit all data packets
μ C_T- The total consumed energy for DP_N transmissions, which numerically equals to C_T as μ =1.
t - Time in seconds
TP_{AV} –Av. throughput (bits/sec)
$E_{residual}$- Residual energy
Hc- hop count (path length)
Tv- trust value