Journal of ISMAC (2019)
Vol.01/ No. 01, June 2019, pp: 38-55 ISSN: 2582-1369 (online)
DOI: https://doi.org/10.36548/jismac.2019.1.004

ENERGY-AWARE SECURITY ROUTING PROTOCOL FOR WSN IN BIG-DATA APPLICATIONS

Dr. S. Smys,
Professor,
Department of ECE,
RVS Technical Campus,
Coimbatore, India.
Email: smys375@gmail.com

Abstract: The dense deployment of the wireless sensor networks has caused enormous data flow leading to a Big-Data generation. To enable a continuous transmission for the huge volume of data packets, it becomes necessary to readapt the routing protocol to facilitate the routing in handling the Big-data scenario. Since energy is the main constraint in the wireless sensor network, as the sensor are battery powered, and the routing methods consuming enormous of the energy for route discovery thereby reducing the network life time, many conventional methods were developed to address the problem of energy consumption with the, increased network latency, overhead, security issues and delay. So the paper proposes the energy-aware routing protocol that could handle the security issues, arising in the enormous data generation satisfying the QOS requirements. The node with substantial resources are selected to overcome the problems of energy consumption and the network life time handling the security issues , delay, network latency and the overhead problem. Further validation of the proposed method in the Network Simulator-3 is performed to evaluate the network latency, packet delivery ratio, throughput, power consumption, network lifetime and Cost.

Keywords: Wireless sensor networks**,** Big-Data, Energy efficiency, Security, Quality of service

1. Introduction

The wireless sensor networks are wireless framework framed by densely deployed tiny sensors used in the sensing of the environmental changes and the industries. Similar to the adhoc wireless network that frame their own wireless network spontaneously, the wireless sensor network also transmits its data wirelessly by forming a network impulsively using the spatially distributed autonomous sensor nodes. The distributed sensor nodes co-operates within themselves to enable the transmission of the data that were collected by sensing. These wireless sensor networks that are low powered, small and unattended are very advantageous as they are inexpensive, very simple to use, flexible, scalable, with the easy accommodation of any devices at any time and can be employed many areas that are beyond human reach.

These superior features made possible the wireless sensor networks to reach to a greater heights in providing the monitoring services to a wide range of applications ,further the recent advances in the technology has increased the amount of data generated in the WSN through sensing. This has made the WSN to be employed in constant sensing in the health, military, environment, home and other commercial areas causing huge volume of data flow resulting in the Big-Data generation. All these data generated are to be carefully routed to its destination to achieve its destiny. The routing is made possible by the proper path establishment in the network by the sensor nodes that work in one accord. Many conventional methods proposed for routing establishment achieve the possible routes for the data to be transmitted at a high energy consumption. The wireless sensor that are designed with the sensing capabilities using the limited battery power either becomes dead or fails in the continues transmission of the data as they run out of energy by huge energy consuming process that were used for routing in the traditional methods. Further the data flow in huge volumes and high speed to be transmitted without interruptions is once again a tedious process as the routing has to be done keeping in mind the energy consumption and the network lifetime. So some novel methods of routing to support the continuous data transmission and energy consumption by modifying the traditional AODV routing protocols [9], by integrating the intelligent approach such as swarm and classical[8], by enabling a multipath routing [6] and inter –cluster communication were proposed to afford the reduction in the energy consumption and the prolong the network longevity all these methods managed in providing the efficient means of energy consumption and network longevity on normal data generation conditions with the increased latency, overhead and security issues.

So the paper proposes an energy aware routing that provides security for the data gathered by the WSN, meeting all the other needs that are required in minimizing the network latency, routing overhead, and delay in the Big-Data Scenario.

The paper is organized with 2 Related works on the routing with energy efficiency and security, 3 the proposed work on the energy-aware secure routing, 4 result evaluation 5 Conclusion.

2. Related Works

Yan et al [1] the paper addresses the problem of extending the network life time in WSN by planning an energy efficient routing protocol by separating the currently prevailing routing problems into two categories based on their network structure that are homogenous or heterogeneous and static or mobile . The overview of the characteristics, limitations and applications along with the open issues of the energy efficient routing is addressed in the paper. Khan et al [2] the routing for the WSN is proceeded with two different modes one known as power controlled routing in which the nodes are related to the CH on the basis of the weight and the other is the enhanced power

controlled routing in which the nodes are related to the CH on the basis of distance to provide energy efficient routing protocol that offers prolonged network life time, and enhanced quality of service using the transmission power variation and clustering Dong et al [3] the energy efficient data gathering methods by integrating the mobile servers and the mobile agent is done and the optimal routing technique considering the flexibility in the services are done to improve the energy consumption and the execution time in the WSN to make it efficient in terms of time and energy. Puranikmath et al [4] the paper is about the data aggregation method in the wireless sensor network to overcome the data redundancy and address all the challenges incurred in the wireless sensor network with the authentication to the data fusion schemes. Karlof et al [5] is the analyses on the goals of secured routing protocols for the wireless sensor networks in the peer to peer and the adhoc networks by introducing two attacks sink hole and HELLO floods and suggest countermeasures with the design considerations. Nasser et al [6] proposes an alternative multipath routing between two nodes to offer security and the network lifetime longevity for the wireless sensor networks. Pathan et al [7] the wireless communication technology suffers from various types of security threats , the methods to identify the security related issues and challenges in wireless sensor networks is proposed in the paper with the holistic view of security for ensuring layered and robust security levels for WSN Guleriaet al [8] the survey provides knowledge for the hierarchical routing protocol based on the categories swarm and classical intelligence approach with the summary of the approaches according to their characteristics, load balancing, scalability, data aggregation positioning, query based, fault tolerance and multipath to have improvement in the energy and the network longevity. Ganesh.et al [9] the SNR dynamic clustering is combined with the ADOV to have protocol that is efficient in terms of energy and security, the security provisioning and the error eradication is done in the inter cluster routing to have the end to end error recovery further the malicious nodes are been isolated to enhance the security provisioning. Du et al [10] the paper provides the state of art research for the security provisioning of the wireless sensor network as survey, addressing the challenges in the security and privacy of WSN involved in the real time monitoring. Liu et al [11] gives the three phase disjoint routing scheme to offer a security and enhanced energy efficiency using a secret sharing algorithm by making multiple shares of the packet to ensure safety enhancements in the routing. Dhakne et al [12] DTBID enables the development of the trust model to prevent the malicious attack in the wireless sensor networks considering the energy, reliability and data. Amouri et al [13] the intrusion based on the cross layer feature collection from medium access control and network layers. With a hierarchical based approach that eludes the clustering and the sequentially transmits the packet within its communication range. Takaishi, et al [14] the paper is about the novel mobile sink routing and the data collection method through network clustering based on the altered expectation and maximization technique. The energy consumption minimization is achieved by driving the optimal number of clusters Elhoseny et al [15] the genetic algorithm is used to optimize the heterogeneous sensor node clustering to extend the network lifetime and the average improvement based on the second optimal performance that is related to the first node die and the last node die to have a balanced energy consumption to improve the network life time and even sensor energy distribution. Farouk et al [16] this is analysis of the protocol to prevent various attacks by making it unconditionally secure by providing N user authentication key. Elhoseny et al [17] the paper is about the building of the four phase routing protocol to in the WSN to ensure

Journal of ISMAC (2019)
Vol.01/ No. 01, June 2019, pp: 38-55 ISSN: 2582-1369 (online)
DOI: https://doi.org/10.36548/jismac.2019.1.004

security and the energy efficiency in all the phases such as clustering, head selection data aggregation and distribution. Wang et al [18] the paper aims in achieving the energy efficiency by the clustering, dividing the network into sectors and framing into cluster and elects the cluster-head estimating the weight and nodes added as members to it estimates the power consumption by selecting an optimal routing by analyzing the various routing strategies. The CH are connected into chain to perform the inter-cluster communication using the greedy algorithm. Rios et al [19] the paper proposes the integration of the Big-data tools on the gathering, analyzing and the data generated by the WSN to tackle the challenges in the collection, manipulation and the exploitation of the data generation by the wireless sensor networks. Fouad et al [20] the paper aims at the over load reduction in the Big-data volume and the cause a limited resource usage for the wireless sensor network by promoting new data mining and the data fusion techniques in WSN by introducing the in-network pre-processing to reduce the complexity of the big-data.

3. Proposed Work

The energy-aware secure routing is proposed in the paper to provide a routing that is energy efficient and secure, full filling the QOS constraint for the transmission of the huge volume of data's that are usually known as the Big-Data. The proposed system helps the big-data scenario by prioritizing the applications and satisfying the QOS constraints according to their requirements by selecting the nodes with the substantial resources using the probability mass function and establishing a key for each sensor node using the approach of public key cryptography (APKC) based on the plane algebraic curve that is defined over a finite field. During each transmission stage that takes place the AKPC is performed for having a routing that is secure from the mishandling and the malicious attacks.

The Secure routing protocol that is energy efficient is initiated on demand with the complete process that is categorized into the three steps such as identification of the path, transmission of information and the path maintenance with the path identification initiated by the destination so as to find the nodes near to the destination, and the security provisioning is done in the each step of the transmission proceeding from the sensors nodes. The route initiation is done to all the nodes neighboring to the destination until it reaches the source nodes with information of all possible paths available by retransmitting of the path identifier message using the intermediate nodes.

3.1Energy-Aware Secure Routing

Journal of ISMAC (2019)
Vol.01/ No. 01, June 2019, pp: 38-55 ISSN: 2582-1369 (online)
DOI: https://doi.org/10.36548/jismac.2019.1.004

The energy-aware secure routing protocol (EASRP) proposed, is to provide the security provisioning, and limit the energy consumption with the increase in the network life during the data transmission, satisfying all the QOS requirements of the big- data applications. This proposed protocol is initiated on demand and proceeded as three stages (i) the path identification process, (ii) the Information transmission, and the (iii) path maintenance process. The consumption in the energy is limited by gathering the nodes information regularly and upgrading it to the routing information table.

3.1.1Path Identification

The path identification is initiated by the sink node, by multicasting the RREQST (route requisition) to the neighboring nodes. The neighboring nodes on receiving the RREQST immediately updates the Routing Information Table(RIT) with the necessary merits and the capabilities of the neighbor node that transmitted the RREQST to it, the merits include the energy consumed, residual energy and its distance with the sink node. This relaying of the RREQST is continued until it reaches the start node with all possible path availability for the transmitting of the information.

The energy consumption in the sink node during the process of data transmission is calculated as zero, as it doesn't have an active participation in the data transmission. The sink node initiates the RREQST and broadcasts it to all the neighboring nodes and the nodes that receive the RREQST includes the details of the node that relayed the information to it, to the table , depending on its distance from the sink node, as the nodes closer to the sink can help the data transmission within few hops.

Consider two nodes $Node_X$ and $Node_Y$, on information being broadcasted by the sink node $Node_{sink}$, if the $Node_X$ receives the RREQST from the $Node_Y$, then $Node_X$ includes the information of the $Node_Y$ to the routing information table if $Node_Y$ is closer to the sink node compared to $Node_X$ and the farer from the startup node$Node_{src}$. This is given in the equation (1) and (2)

$$Dist(Node_Y, Node_{sink}) \leq Dist(Node_X, Node_{sink}) \quad (1)$$

$$Dist(Node_X, Node_{src}) \leq Dist(Node_Y, Node_{src}) \quad (2)$$

Journal of ISMAC (2019)
Vol.01/ No. 01, June 2019, pp: 38-55 ISSN: 2582-1369 (online)
DOI: https://doi.org/10.36548/jismac.2019.1.004

The equation (3) gives the energy consumption (EC) of the data transmission from $Node_X$ through $Node_Y$ to the $Node_{sink}$

$$EC(X,Y) = e(Node_Y) + e(Node_X, Node_Y) \quad (3)$$

Where $e(Node_Y)$the energy is consumed in the transmission from node Y and$e(Node_X, Node_Y)$ is the energy consumed during the data transmission between the Node X and Y. Where equation (4) gives the ($Er_{x,y}$) energy required to transmit the data packet from the $Node_X$ to $Node_Y$, and the remaining energy of the node $Node_X$ (Re_x)

$$e(Node_X, Node_Y) = Er_{x,y} Re_x \quad (4)$$

The nodes that consumes high energy for the transmission of the data is eliminated and proceeded with the routing information updation using the nodes that cause minimum energy for the information transfer. The equation (5) shows the elimination of the high energy consuming nodes.

$$RIT_X = [Y | EC(X,Y) \leq w(\min(Node_X, Node_z)] \quad (5)$$

The probability (Prob) of selecting the nodes with the limited energy consumption is given in the equation (6)

$$Prob_{X,Y} = \left(1/EC(X,Y)\right) \Big/ \left(\sum_{Z \in RIT_X} 1/EC(X,Y)\right) \quad (6)$$

So the total energy consumption for the transmission of the data from $Node_X$ to the $Node_{sink}$ is given in the equation (7), the information of the energy consumption for the data transmission is included to the table before the $Node_X$ relays it to the next node.

$$Total_{EC} = \sum_{Z \in RIT_X} EC(X,Y), Prob_{X,Y} \quad (7)$$

So the process is stopped when it reaches the $Node_{src}$ with the possible number of path availability included in the routing information table.

Journal of ISMAC (2019)
Vol.01/ No. 01, June 2019, pp: 38-55 ISSN: 2582-1369 (online)
DOI: https://doi.org/10.36548/jismac.2019.1.004

3.1.2Information Transmission

The startup point starts the data transmission by randomly selecting the nodes listed in the table. The intermediate nodes forwards the packets by selecting the appropriate nodes with the limited energy consumption for transmission until the data packets are reached to the destination. In this stage each transmission round that is initiated by the sensor nodes are secured to avoid the false data being transmitted to the sink node. This is done by proceeding with the establishing a key for each sensor node using the approach of public key cryptography(APKC) that is based on the plane algebraic curve that is defined over a finite field. The approach of the public key cryptography generates a key of 176 bits, in which the 128 bits are assigned to the Key of the AKPC, 13 bits are assigned to the identification of the node, the 15bits assigned to the encode the distance between the sensor nodes, and the 20 bits is the transmission round bit that is assigned to the, information on energy consumption on the data transmission, energy remaining in the each node and the distance between the node and the sink node. On each round the information of each node is gathered from the routing information table and updated in the transmission round index. The 128 bit key assigned is alone hashed using the secure hashing algorithm and the remaining components are made visible to each nodes in the network.

3.1.2(a) Process of Encryption and Decryption

The proposed Energy- aware secure routing proceeds through the three steps for the process of encrypting and decrypting the information so as to stop the false data intrusions in the nodes and the false data transmission to the destination. The information encrypted is decrypted only in the sink node.

The encryption and the decryption method engages three stages of simple operations to cause the confusion and the diffusion. They are the EX-OR operation, Substituting and the permuting. For this process the key of the encryption is divided into two equal halves in which the first part is constituted of the random bits and the second part is the reference bits that supports by extending guidance for the process of encryption.

The process of encryption are as follows.

EX-OR operation: The random input data and the reference bits are X-ORed.

Substituting: This performed on the reference bits sections it calculates the number of ones for every 8 bit and alters the two consecutive values that are the starting point of a byte.

Journal of ISMAC (2019)
Vol.01/ No. 01, June 2019, pp: 38-55 ISSN: 2582-1369 (online)
DOI: https://doi.org/10.36548/jismac.2019.1.004

Permuting: This is also performed in the reference bits, it counts the number of ones in every 11 bits and replaces the value of either the two consecutive or three consecutive or four consecutive values depending on the increasing order of the consecutive counts.

The decryption process is followed by proceeding in the reverse order of the encryption process. The process of encryption and the decryption are shown in the Fig 1.

So the information is completely secured and are transmitted to the destination by looking for the information in the transmission round index gained from the routing information table. This helps the node to identify the node with maximum residual energy, minimum energy consumption and minimum distance to the sink node, to enable a prolonged network lifetime satisfying the QOS enhancements required

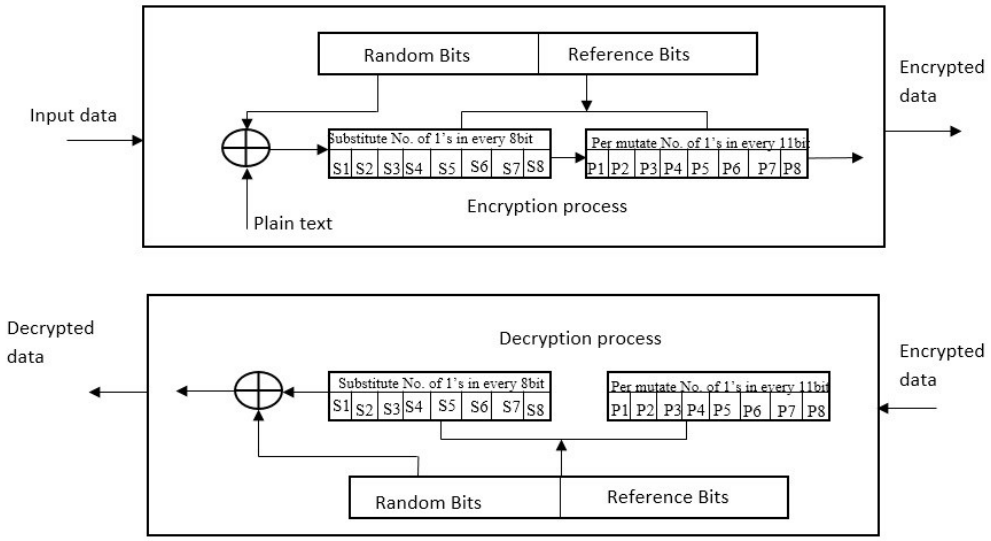

Fig 1 Encryption and Decryption process

3.1.3Path Maintenance

The path maintenance takes care of the periodic updates of the routing information table by performing the regular path identification to identify the failed nodes to remove them from the table and add new nodes that are included in the network. So this enables the network to have the prevailing status of all the nodes.

Journal of ISMAC (2019)
Vol.01/ No. 01, June 2019, pp: 38-55 ISSN: 2582-1369 (online)
DOI: https://doi.org/10.36548/jismac.2019.1.004

3.2. Energy-Aware Secure Routing in Big-Data Application

The energy-aware secure routing protocol is readapted according to the Big-Data applications to ensure a quality of service in the situation that are vital, for eg. The emergency healthcare conditions, unknown attacks, accidents or natural disasters requires a high quality of service by rendering timely delivery and quick response which otherwise would lead to adverse situations. So the Energy-aware secure routing protocol is structured to satisfy the QOS requirements of the Big-Data applications based on its criticality, the applications are segmented based on their vitality and the application with the highest significance is addressed first. The exigent situations are addressed with higher importance whereas the other normal environmental sensing are assigned the lowest importance.

The application assigned with the highest importance are addressed first by verifying whether the QOS constraint are satisfied. It is ensured that the QOS constraints that is the maximum delay that can be subjected by the each node in data transfer and the minimum bandwidth requirement for transfer of the data are satisfied and the deviation from the QOS parameters is measured by assigning two parameters $BDmin$ and $DDmax$. For each application the importance values are assigned based on their importance and the lowest importance value is given the highest priority. For instance for the application H is assigned highest importance if the$importance_{value} = low$, now the QOS Constraints that are optimal are assigned for the application of higher importance and $BDmin = 0$ and $Ddmax = 0$ then ensures that there is no deviation in the QOS constraints assigned and enables the routing that strictly done according to the QOS constraints assigned. By this the routes that satisfy the QOS constraint can be selected and multitude of routes for handling large data flow can be established.

Consider the applications $\{H_1, H_2 \ldots H_n\}$ are set importance value as shown in the equation (8), the $Bmin$ and $Dmax$ are assigned values as shown in the equation (9) and (10)

$$Importance_{value\ H_1} < Importance_{valueH_2} < \cdots < Importance_{ValueH_n} \quad (8)$$

$$BD_{Min_{H1}} < BD_{Min_{H2}} < \cdots\cdots < BD_{Min_{Hn}} \quad (9)$$

$$DDmax_{H1} < DDmax_{H2} < \cdots\cdots < DDmax_{Hn} \quad (10)$$

The energy-aware secure routing protocol is structured according to the Big-Data applications by also including the information about the QOS parameters and the importance value of the application into the RREQST before

Journal of ISMAC (2019)
Vol.01/ No. 01, June 2019, pp: 38-55 ISSN: 2582-1369 (online)
DOI: https://doi.org/10.36548/jismac.2019.1.004

initiating to the neighbor nodes. Now the neighbor nodes, on receiving the RREQST from the intermediate nodes updates the table with the information of the nodes including the QOS constraints along with the energy consumption, Residual energy, and the distance from the sink node. The nodes that satisfy the QOS constraints according to the conditions mentioned in the equation (11) and (12)

$$banwidth_{node} >= minimum_{bandwidth} - BD_{MIN} \tag{11}$$

$$(maximum_{delay} + DD_{max}) - node_{distance} >= 0 \tag{12}$$

are included in handling the highest importance function and the rest are assigned in handling the application of decreasing importance. Now the nodes selected for the transmission based on the probability function given in the equation (13)

$$Prob_{X,Y} = \left(bandwidth_{node} \Big/ EC(X,Y) + node_{distance}\right) \Big/ \left(\sum_{Z \in RIT_X} bandwidth_{node} \Big/ EC(X,Y) + node_{distance}\right) \tag{13}$$

and the information to be transmitted are ensured with the security in the each round of transmission by encryption to avoid the mishandling of the information in the critical applications and decrypted only in the base station to ensure that the information are in the safe hands without any intrusions. The path maintenance is done to check the nodes energy and if the nodes energy goes below the 50% of the energy required in the transmission then immediately the node is eliminated from the routing information table and the re-identification process for the path continues to upgrade the routing table details with the current status of the network. The Fig 2 shows the flow chart of the proposed EASRP for Big-Data applications.

Journal of ISMAC (2019)
Vol.01/ No. 01, June 2019, pp: 38-55 ISSN: 2582-1369 (online)
DOI: https://doi.org/10.36548/jismac.2019.1.004

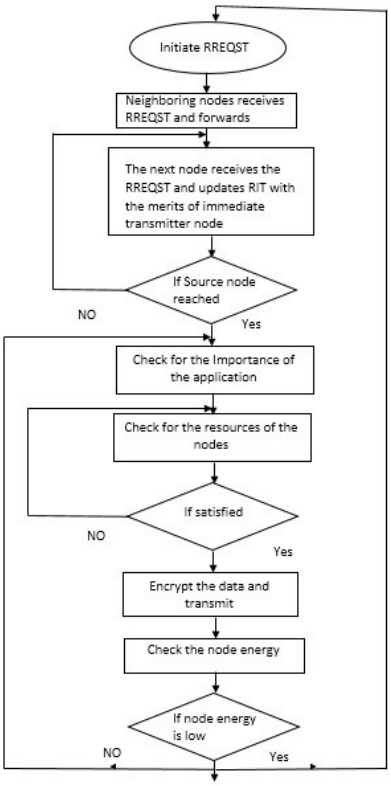

Fig 2 Flow Chart of proposed EASRP

4. Result Evaluation

The proffered energy-aware secure routing protocol is simulated using the network simulator 2 with the number of nodes varying from 100 to 200, the proposed method is validated to check with its performance on the grounds of energy consumption, network lifetime, throughput, packet delivery ratio and the latency and compared with the existing system LCRP and the LEACH to evince the efficiency of the energy-aware secure routing protocol. The table 1 shows the parameters and the value used in the simulation process.

Journal of ISMAC (2019)
Vol.01/ No. 01, June 2019, pp: 38-55 ISSN: 2582-1369 (online)
DOI: https://doi.org/10.36548/jismac.2019.1.004

Table 1 Simulation Parameters

Parameter	Values
Simulation time	100seconds
Allotted area	40m*2500m
Number of nodes	200
Packet size	1024 bits
Packet data rate	1 packet /second
Initial Energy	100 joules
Channel Capacity	2Mbps

(a)Energy Consumption

The EASRP proffered gather the node with the high energy values to be involved in the transmission process, taking into consideration the distance of the nodes from its destination, the equation (1) and (2) helps in finding the nodes with the minimum distance from the sink node. Further the bandwidth capacity and the delay of the node included to the routing information table enables the source to decide with the path enriched with the nodes with high QOS values to allow the transmission of the information without much delay or channel overhead. The Security provisioning further ensures the secure transmission of the information and elude the retransmission process which would result in even high energy consumption. Since the security servicing generates concise keys without altering the size of the information the energy consumption of the security provision is also very less so the proposed EASRP is efficient in terms of energy consumption compared to the existing methods.

The Fig 3 shows the energy consumption of the EASRP in comparison with the existing method, the proffered method shows a less energy consumption on different number of nodes varying from 100 to 200, for different applications with varying importance values. The similar situation on the existing methods shows high energy consumption than the proposed method.

Journal of ISMAC (2019)
Vol.01/ No. 01, June 2019, pp: 38-55 ISSN: 2582-1369 (online)
DOI: https://doi.org/10.36548/jismac.2019.1.004

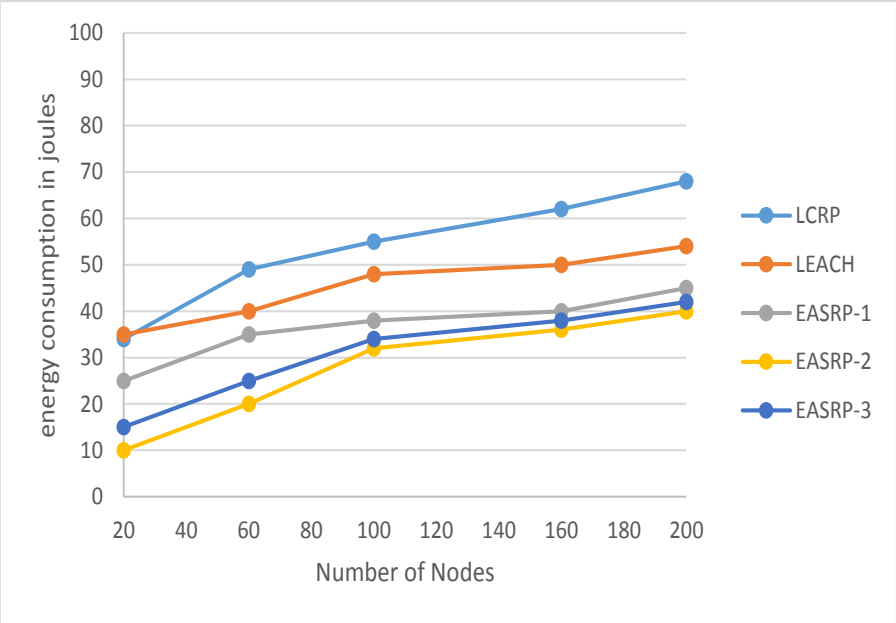

Fig 3 Energy Consumption

(b)Network Life Time

The Fig 3 to evince the reduce energy consumption shows less energy consumption of the proposed EASRP. From the above simulation result on the energy consumption, it is clear that the battery powered nodes would have prolonged network lifetime using the proposed system compared to the existing methods.

Journal of ISMAC (2019)
Vol.01/ No. 01, June 2019, pp: 38-55 ISSN: 2582-1369 (online)
DOI: https://doi.org/10.36548/jismac.2019.1.004

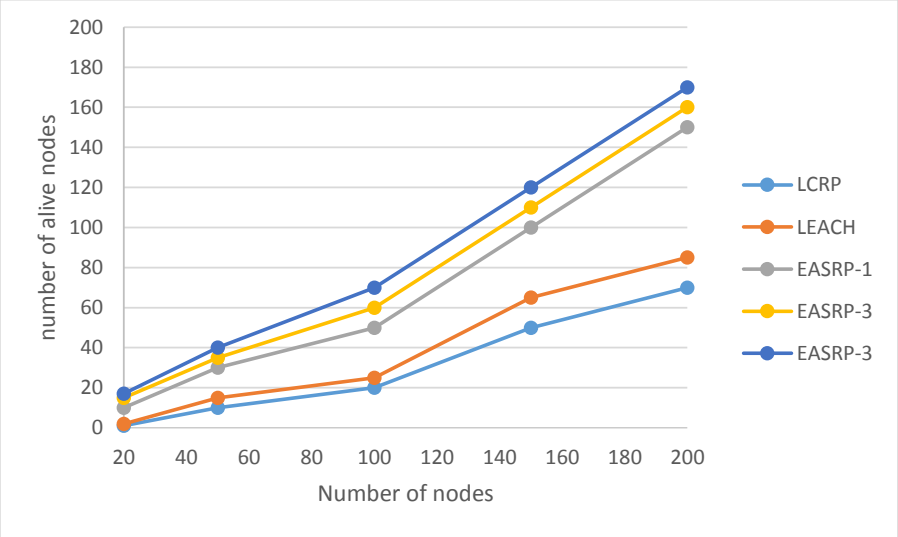

Fig 4 Network Life Time

The simulation result in the Fig 4 shows the prolonged life time of the nodes for varying number of nodes and different applications, compared to the existing LCRP and the LEACH protocols. Therefore this ensure less failure in nodes extending the interruption less continuous transmission of information.

(c)Throughput

The reduced node failures ensure the continuous information transmission without any losses due to the link failures, the throughput that gives the measurement of the number of successfully transmitted information for the number of transmissions that was initiated, is verified through the simulation of the proposed network to ensure its throughput enhancements. The bandwidth capacity and the delay considered in the selection of the nodes also help in improving the continuous transmission by avoiding the network latency and the channel overhead. Further the security provisioning's enabled on the each round of the transmission, once again helps in the successful transmission of the information without any mishandling or the false data inclusions.

The Fig 5 shows the enhanced throughput achievement of the proposed compared to the existing methods. The throughput achieved for the different application based on their priorities using the proposed system is very high compared to the throughput achievement of the existing least cost routing protocol and the LEACH.

Journal of ISMAC (2019)
Vol.01/ No. 01, June 2019, pp: 38-55 ISSN: 2582-1369 (online)
DOI: https://doi.org/10.36548/jismac.2019.1.004

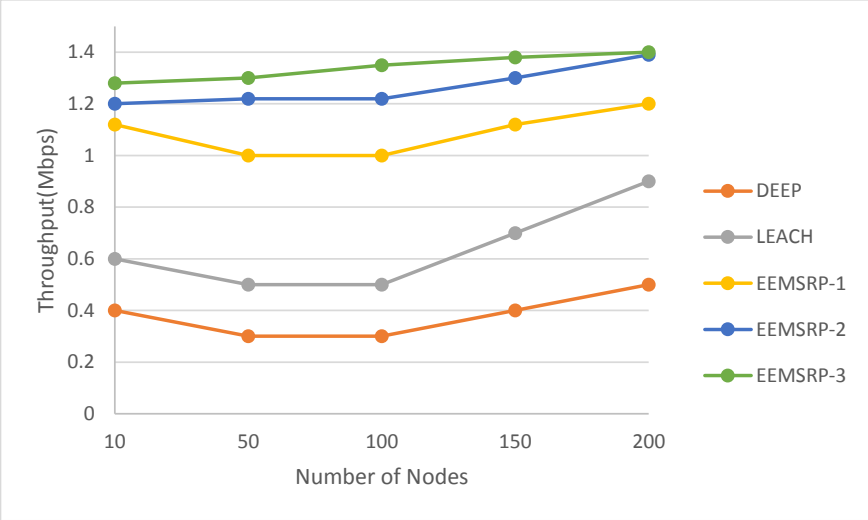

Fig 5 Throughput

(d)Packet Delivery Ratio (PDR)

The PDR gives the successful number of packets delivered compared to the number of packets sent, the improved energy efficiency the , decreased node failures and the throughput enhancement of the proposed system shows that the packet delivery ratio for the different set of nodes and different application of varying importance would be high compared to the existing methods. Moreover the security provisions of the proposed EASRP is afforded with the secure data transmission on its each round to complete the data transfer to the authenticated sink node without any mishandling helps in increasing the successful packet delivery without any loss.

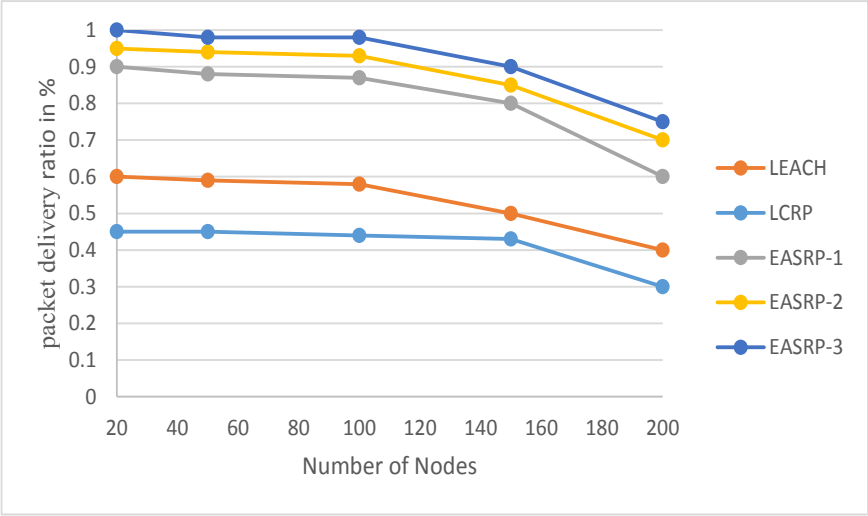

Fig 6 Packet Delivery Ratio

Journal of ISMAC (2019)
Vol.01/ No. 01, June 2019, pp: 38-55 ISSN: 2582-1369 (online)
DOI: https://doi.org/10.36548/jismac.2019.1.004

The Fig 6 shows the improved PDR achieved by the proposed energy-aware secure routing protocol compared to the existing methods. The PDR values are high when the number of nodes are less and then takes a slight fall as the number of node increases, even then proves to be efficient than the existing methods of routing.

(e)Delay in Response Time

The delay in the response time gives us the details about the delay incurred in the receiving of the information, it usually calculates the time difference in the transmission and the reception of the information. The details included in the routing information table and the proper security provisioning in the proposed system helps it manage the time constraints and deliver the data before its value is timed out.

The Fig 7 shows the simulation results of the proposed system delay calculation. The delay incurred in proposed system for the varying application with increasing and decreasing importance proves to have a reduced delay in the response time compared to the existing methods of routing.

Thus the proposed system proves to be efficient in terms of the energy consumption, delay, throughput, network life time, and PDR.

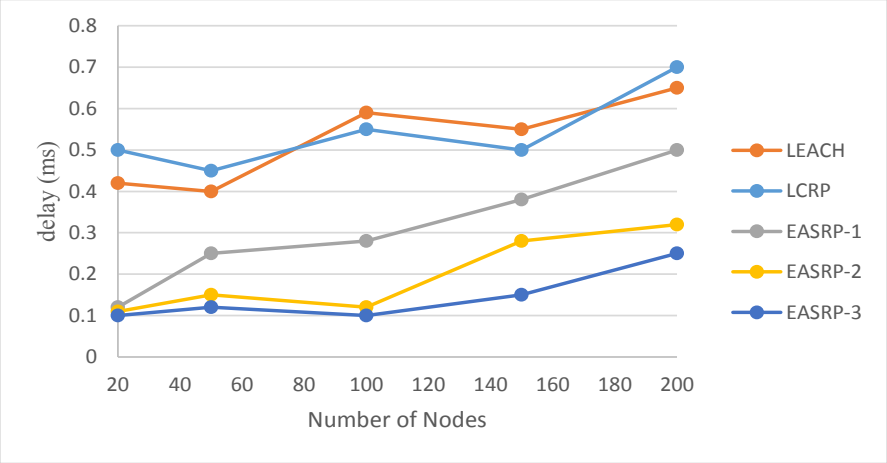

Fig 7 Delay in Response Time

Journal of ISMAC (2019)
Vol.01/ No. 01, June 2019, pp: 38-55 ISSN: 2582-1369 (online)
DOI: https://doi.org/10.36548/jismac.2019.1.004

5. Conclusion

The energy-aware secure routing protocol was proposed to handle the Big-Data applications, by prioritizing the applications based on the importance. The routing protocol proposed proceeded as three stages, with the first stage as path identification that gathers the nodes merits on its energy, bandwidth, distance to the sink and delay to update in the routing information table and the next on is data transmission that is done considering the optimal nodes with the rich resources and minimum distance to the sink node, along with the security provisioning achieved through the APKC method of key generation in each round of transmission. And finally the path maintenance that updates the routing information table with the current status of the network. The further validation of the proposed system on the grounds of energy consumption, delay, throughput, network life time and the packet delivery ratio, proves the efficiency of the proposed system compared to the existing methods of LCRP and LEACH in handling the big-data applications fulfilling its QOS constraints.

References

[1] Yan, Jingjing, Mengchu Zhou, and Zhijun Ding. "Recent advances in energy-efficient routing protocols for wireless sensor networks: A review." *IEEE Access* 4 (2016): 5673-5686.

[2] Khan, Atta Ur Rehman, Sajjad A. Madani, Khizar Hayat, and Samee Ullah Khan. "Clustering-based power-controlled routing for mobile wireless sensor networks." *International journal of communication systems* 25, no. 4 (2012): 529-542.

[3] Dong, Mianxiong, Kaoru Ota, Laurence T. Yang, Shan Chang, Hongzi Zhu, and Zhenyu Zhou. "Mobile agent-based energy-aware and user-centric data collection in wireless sensor networks." *Computer networks* 74 (2014): 58-70.

[4] Puranikmath, Veena I., Sunil S. Harakannanavar, Satyendra Kumar, and Dattaprasad Torse. "Comprehensive Study of Data Aggregation Models, Challenges and Security Issues in Wireless Sensor Networks." *International Journal of Computer Network and Information Security* 11, no. 3 (2019): 30.

[5] Karlof, Chris, and David Wagner. "Secure routing in wireless sensor networks: Attacks and countermeasures." In *Proceedings of the First IEEE International Workshop on Sensor Network Protocols and Applications, 2003.*, pp. 113-127. IEEE, 2003.

[6] Nasser, Nidal, and Yunfeng Chen. "SEEM: Secure and energy-efficient multipath routing protocol for wireless sensor networks." *Computer communications* 30, no. 11-12 (2007): 2401-2412.

[7] Pathan, Al-Sakib Khan, Hyung-Woo Lee, and Choong Seon Hong. "Security in wireless sensor networks: issues and challenges." In *2006 8th International Conference Advanced Communication Technology*, vol. 2, pp. 6-pp. IEEE, 2006.

[8] Guleria, Kalpna, and Anil Kumar Verma. "Comprehensive review for energy efficient hierarchical routing protocols on wireless sensor networks." *Wireless Networks* 25, no. 3 (2019): 1159-1183.

[9] Ganesh, Subramanian, and Ramachandran Amutha. "Efficient and secure routing protocol for wireless sensor networks through SNR based dynamic clustering mechanisms." *Journal of Communications and Networks* 15, no. 4 (2013): 422-429.

[10] Du, Xiaojiang, and Hsiao-Hwa Chen. "Security in wireless sensor networks." *IEEE Wireless Communications* 15, no. 4 (2008): 60-66.

[11] Liu, Anfeng, Zhongming Zheng, Chao Zhang, Zhigang Chen, and Xuemin Shen. "Secure and energy-efficient disjoint multipath routing for WSNs." *IEEE Transactions on Vehicular Technology* 61, no. 7 (2012): 3255-3265.

[12] Dhakne, Amol R., and P. N. Chatur. "Distributed trust based intrusion detection approach in wireless sensor network." In *2015 Communication, Control and Intelligent Systems (CCIS)*, pp. 96-101. IEEE, 2015.

[13] Amouri, Amar, Luis G. Jaimes, Raju Manthena, Salvatore D. Morgera, and Idalides J. Vergara-Laurens. "A simple scheme for pseudo clustering algorithm for cross layer intrusion detection in MANET." In *2015 7th IEEE Latin-American Conference on Communications (LATINCOM)*, pp. 1-6. IEEE, 2015.

[14] Takaishi, Daisuke, Hiroki Nishiyama, Nei Kato, and Ryu Miura. "Toward energy efficient big data gathering in densely distributed sensor networks." *IEEE transactions on emerging topics in computing* 2, no. 3 (2014): 388-397.

[15] Elhoseny, Mohamed, Xiaohui Yuan, Zhengtao Yu, Cunli Mao, Hamdy K. El-Minir, and Alaa Mohamed Riad. "Balancing energy consumption in heterogeneous wireless sensor networks using genetic algorithm." *IEEE Communications Letters* 19, no. 12 (2014): 2194-2197.

[16] Farouk, Ahmed, Josep Batle, M. Elhoseny, Mosayeb Naseri, Muzaffar Lone, Alex Fedorov, Majid Alkhambashi, Syed Hassan Ahmed, and M. Abdel-Aty. "Robust general N user authentication scheme in a centralized quantum communication network via generalized GHZ states." *Frontiers of Physics* 13, no. 2 (2018): 130306.

[17] Elhoseny, Mohamed, and Aboul Ella Hassanien. "Secure Data Transmission in WSN: An Overview." In *Dynamic Wireless Sensor Networks*, pp. 115-143. Springer, Cham, 2019.

[18] Wang, Jin, Yu Gao, Wei Liu, Arun Kumar Sangaiah, and Hye-Jin Kim. "Energy Efficient Routing Algorithm with Mobile Sink Support for Wireless Sensor Networks." *Sensors* 19, no. 7 (2019): 1494.

[19] Rios, Lidice Garcia. "Big data infrastructure for analyzing data generated by wireless sensor networks." In *2014 IEEE International Congress on Big Data*, pp. 816-823. IEEE, 2014.

[20] Fouad, Mohamed Mostafa, Nour E. Oweis, Tarek Gaber, Maamoun Ahmed, and Vaclav Snasel. "Data mining and fusion techniques for WSNs as a source of the big data." *Procedia Computer Science* 65 (2015): 778-786.

Journal of ISMAC (2019)
Vol.01/ No. 01, June 2019, pp: 38-55 ISSN: 2582-1369 (online)
DOI: https://doi.org/10.36548/jismac.2019.1.004