Journal of Theoretical and Applied Information Technology
30th November 2017. Vol.95. No 22

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

A CERTAIN INVESTIGATION ON SECURE LOCALIZATION ROUTING PROTOCOL FOR WSN

[1]N. A. NATRAJ, [2]Dr. S. BHAVANI,
[1]Research Scholar, Department of ECE, Karpagam Academy of Higher Education, Coimbatore
[2]Professor and Head, Department of Electronics and Communication Engineering,
Karpagam Academy of Higher Education, Coimbatore, India.
E-mail: [1]vallanat@gmail.com , [2]bhavanisridharan7@gmail.com

ABSTRACT

Wireless Sensor Network (WSN) is an advancement of wireless network where nodes are located with respect to static or dynamic. Secure Localization is a major challenge in WSN where location of unknown nodes may not be identified. In previous work, authors focused on secure localization but not balancing energy consumption. In this proposed work, Secure Localization Routing Protocol (SLRP) is developed to attain balancing between secure location integrity and energy efficiency. This protocol contains three phases. In first phase, cluster member selection and route formation is implemented to forward packet to next hop node efficiently. In second phase, localization procedure is adopted based on location hop distance value, residual energy of node for location discovery and minimum cost function. In last phase, secure localization scheme is implemented to secure location information about cluster members from attackers. Localization procedure is implemented with confidentiality using effective cryptography technique to protect messages from attackers and worms. The extensive simulation results are performed over SLRP, RMSR, ECHERP and ENSOR in terms of location integrity rate, location accuracy, location update rate, control overhead, packet delivery ratio and packet delay. Proposed protocol SLRP produces better results than existing schemes.

Keywords: *WSN, Cluster Member Selection, Route Establishment, Localization Procedure, Secure Localization Scheme And Minimum Cost Etc.*

1. INTRODUCTION

Wireless Sensor Networks (WSNs) is a selected reasonably unintended network, extremely localized, and while not infrastructure. They are made up of multiple micro-transceivers, additionally referred to as detector nodes that enable end users to collect and transmit environmental information from areas which could be inaccessible or hostile to masses. The transmission of information is finished severally by every node, employing a wireless medium. The energy of every node is prescribed to the capability of its battery. The consumption of energy for each communication and data process should be reduced. Sensor networks use multi-hop communications. The target is to route the collected information to end user's victimization. The information should be directed towards the front users of the WSN. Routing algorithms in WSNs are often classified by totally different criteria. The routing protocols usesensor node positions to route the information within the network. Location routes are ordinarily not determined and prioritized. Indeed, the sensors nodes deployed into the geographical region wherever the information should be collected, then they work along to find their position.

Localization in WSN

The localization aware routing may be a terribly essential step that has to be secured so as to make sure that the integrity of the WSN and its associated services. Firstly, this method permits the sensor node to line up the required parameters to determine the methods which will lead their information towards finish users. The data of their position is additionally an important requirement for the ultimate application that processes the info collected by sensors, i.e., the user has to understand the origin of collected information before victimization it. Finally, the final users may need to

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

question some nodes by causing the position wherever data has to be collected. The localization method is so crucial. Puneet Gurbani et.al [1] surveyed hierarchical cluster based energy efficient routing protocol for WSN. Based on location information and energy level of sensor nodes, cluster routing protocols were adopted. In the proposed research work, secure location aware routing is established from source to destination to improve location accuracy.

The paper consists of five chapters. First chapter dealt with introduction about location aware routing in sensor network. Chapter 2 analyzes the existing protocols which are relevant to energy efficient routing and secure localization models. In chapter 3, the proposed protocol is implemented. In chapter 4, simulation results and justifications are given. Last chapter concludes the proposed work and future enhancement is given.

2. PREVIOUS WORK

In [2], authors proposed the security based energy efficient routing protocol to increase the lifetime of wireless sensor nodes. Secure routing and energy balancing were addressed using cost aware secure routing protocol. Both position and energy level of neighbor nodes were maintained and the information was also forwarded to nearby sensor node. There are two routing strategies that follows to find shortest path routing with random walking model to stop jamming attacks. The reason for preventing this attack is to protect the network from jammer to continue packet flooding.

In [3], TinyMD5 was introduced which is a one way hash function to restrict the external attacks during data transmissions. The attempts were also made for external attacks during packet transmission period. The data analysis was made by the proposed energy efficient secure routing where long range of data is converted into medium level to avoid data exposure. Only one part was achieved i.e. encryption. It was impossible to find the whole data transmission information and only a partial amount of data information transmission can be obtained.

Sutagundar and Manvi [4] proposed location aware event multipath routing with the help of static and mobile node agents. The path discovery procedure was triggered using an event node to estimate the number of special kind of neighbor nodes between event node and destination node in the presence of dynamic environment. Based on geographical position of sensor nodes, partial topological information was predicted for mobile agents and to find the disjoint paths between sensor nodes. Each disjoint path was associated with the estimation of path weightage factor, energy rate and hop distance factor value.

Balamurugan and Manimegalai [5] introduced a Revise Packet tree based byte stuffing algorithm to decrease the presence of attackers in the network. The paths are build with efficient weightage factor and capacity to transfer the information from source to sink node without the interruption of attackers. During packet transmission process, there are some additional fields included in each and every packet to secure the information from the attackers. These fields are removed after transmission period to avoid heavy traffic flow. Based on intermediate neighbor node database, data link can be established between two or more sensor nodes using link layer.

Sneetha Praneetha et.al [6] presented a Cost Aware Secure Routing to balance energy level among sensor nodes and to increase the network lifetime. This protocol supports both multipath routing and routing security. If the node receives the node energy level of neighbor sensor nodes, the geographical position of sensor nodes will also be included. Based on this information, different categories of filters were created to provide tradeoff between authentication and energy efficiency. But the computational cost during secure authentication mechanism will consume more energy consumption and it will lead to less span of network lifetime.

Junqi Duan et.al [7] developed the Trust Aware Secure routing framework based on trust computation and management systems. Optimized routes were built with this framework to protect paths and nodes from attackers. Neigbor nodes are discovered and identified from trust table of source node. Sink node receives the information based on node location information. This information will not be disclosed to attacker nodes. In each and every node's packet information, trust metric was included to meet the reliability requirements of sensor network.

Tran Dinh hieu et.al [8] developed the Stability Aware Geographic routing to balance the node stability and energy level during route discovery and route maintenance process. To achieve stability of network, expected transmission count metric was

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

calculated and added in all node's routing table. Duty cycle was also calculated to ensure link quality information. The information was protected from the attackers and stability was enhanced in all nodes. Location information was issued once the node moves near the sensor node.

Celso Moraes and Dongsoo Har [9] dealt with the Clustering and Energy trading in WSN using the charging scheme. Mobile charger was used for initial stage and energy trading was analyzed between sensor nodes. In target phase, cluster heads and maximum number of cluster member were charged during first level. The paths were also charged based on the distribution of cluster region heads. In second stage, the energy trading method was adopted to balance energy consumption in the presence of packet loss and route failures.

Hamid Mahboubi et.al [10] investigated the maximum lifetime strategy to track and monitor a moving sensor node in the sensor field. The resources and obstacles were found for sensing and communicating the information between sensor nodes. The reasons for path blocking were also identified to increase the network lifetime. An efficient motion strategy was also finalized to track the location information of sensor nodes. Sensor node location and information transmission was found using shortest path algorithm.

Hong Fu et.al [11] introduced an Adaptive Energy and Location Aware Routing Algorithm (AELAR) to discover energy efficient paths from source to sink node. The routing request zone was divided and next hop node was chosen based on select equation. Nodes are randomly moving in and around of network region. Both selected equation and routing zone can be adjusted based on node location. Paths are found quickly and energy consumption was reduced by means of adaptive mechanism.

Firdozali and Nagamalar [12] introduced an energy aware mobile sink based routing protocol to reduce the energy dissipation of sensor nodes. Energy dissipation of sensor nodes was observed and summarized in this work. Node selection and energy minimization were successfully achieved to increase energy efficiency. Mobility radius of destination node was estimated to improve network span.In some cases, the static destination nodes are located to increase energy level irrespective of mobility radius of destination node.

Abinaya et.al [13] introduced energy aware routing protocol to provide load balancing with minimum energy consumption. The loads were adjusted using congestion control procedure based on neighbor node capacity and packet length.

Deyu Zhang et.al [14] introduced a novel resource-allocation solution to increase the maximum channel detected time period. Spectrum sensors were assigned to allocate channels with the required transmission power and time to prolong the network lifetime. The optimality and energy efficiency were obtained using energy harvested routing algorithm.

Zubair et.al [15] introduced spin torque sensors to reduce delay and energy consumption of WSN. Some interconnect systems were utilized to locate the sensor nodes in the presence of mobility period. Only low voltage interconnect swing sensor nodes are adopted for discovering minimum energy aware routing.

Haijun Zhang et.al [16] introduced cognitive smart cell and investigated about sensor optimization issues and power control problem. Only cross tier interference mitigation was analyzed for optimum energy efficiency. A non-convex optimization problem for power allocation and node localization was also summarized in this work. An iterative power control algorithm and optimal sensing method was adopted for energy efficiency and spectrum sensing.

Ashutosh Kumar Tiwari and Suresh Gawande[17] developed SPIN algorithm to locate sensor nodes to discover energy efficient routing. Energy efficiency was improved in two dimensional surface of sensor network.

3. SECURE LOCALIZATION SCHEME FOR WSN

In the proposed scheme, nodes are located in a specific region to increase network lifetime. To improve the quality of WSN, Cluster region is formed and cluster member is chosen based on Received Signal Strength Indicator (RSSI), packet loss rate, distance between nodes. The reason for selecting cluster member is to enhance location accuracy of all nodes inside the cluster region. To protect data and node location information, the concept of signature generation and verification scheme is adopted. To obtain optimal routes, route hop distance metric is used. To increase the location accuracy, localization error, minimum cost

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

function of all paths and residual energy are estimated.

Network model

In the proposed protocol, communication and propagation model is implemented for large number of sensor nodes as well as small number of sensor nodes. Network environment is created based on network parameters and coverage region. Nodes are assumed to be static and dynamic based on location information about neighbor nodes. In this work, WSN is created with 100 sensor nodes with the network area of 1000 x 1000 m^2 randomly. Any node if it is a source or neighbor node, it may initiate a route discovery process. Remaining node may act as destination node for those nodes. The selection of source and sink node pair can be done randomly. Sensor nodes are grouped together and form a cluster region. Cluster Head (CH) acts as a major role for detecting any malfunctions and monitoring the behaviors of cluster members. Cluster member (CM) has the responsibility of forwarding data packets to the intended destination. All sensor nodes are having limited resources with limited transmission range.

Mobility model

In general case of mobility model, sensor nodes are kept as static. In our proposed protocol, there are two categories of sensor nodes. One is static and other is dynamic. Static sensor nodes are anchor node which monitors the mobility of dynamic sensor nodes to increase the packet delivery rate. Here the mobility model for WSN in our proposed protocol is random walk mobility model.

Selection of Cluster member in Cluster region

In cluster region, cluster member selection plays a major role to forward the data packets from source to destination node. In order to identify efficient route, cluster member must be chosen effectively. Some of the factors are used for determining neighbor cluster member in cluster region. It is given as follows.

Step1: Once CH and destination CH are found, intermediate cluster member will be searched by Source CH. The hop distance signal request packet is broadcasted by source CH.

Step 2: Hop distance is calculated and replied from destination CH towards source CH. Based on Euclidean's distance formula, distance of cluster member is estimated as,

$$D(x,y)=\sqrt{\left[(p_1-p_2)^2+(q_1-q_2)^2\right]}$$

Node *x,y* are located with hop distance with co-ordinates of *p,q*.

Step 3: Choose the cluster member with maximum weightage factor. The weightage factor is assigned based on node capacity, received signal strength and stability metric. Stability metric is estimated based on Signal to Noise Ratio (SNR). The SNR is calculated based on Bit Error Rate.

Step 4: Packet loss rate ($P_{lr}(t)$) of path is calculated as,

$$P_{lr}(t)=\frac{N_{pl}(t)}{N_T(t)}\times 100$$

$N_{pl}(t)$ is the number of packets lost at a function of time period from one CM to another CM.

$N_T(t)$ is the number of total packets delivered at a function of time period.

Step 5: Node location information is obtained based on Received Signal Strength Indicator (RSSI).

Step 6: Cluster head choose the node with nearest location based on threshold factor which includes minimum packet loss rate, hop distance metric and weightage factor.

Step 7: Once the acknowledgement is received, Source CH will choose cluster member based on threshold factor.

Route formation in Cluster region

Once the cluster members are chosen, routes are formed with minimum cost and shortest path routing algorithm. The next hop is formed based on following steps.

Step 1: The minimum cost function (M_c) for an individual route is formed with current routing table of Source CH. It is determined as,

$$M_c=\beta d_k+(1-\beta)\frac{L\tau}{n(n-1)}E_{con}$$

Where β is the adjusting parameter according to transmission range. d_k is the hop distance from source CH to nearby cluster member. *L* is the number of data packets. τ is time delay from source to sink node. *n* is number of sensor nodes actively participating in the cluster region. E_{con} is the energy consumed by data packets.

Step 2: Optimized Hop Distance (OHD) between cluster members is estimated as,

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

$$OHD_{ij} = \frac{\sum_{i=1,j=1}^{n} \sqrt{(a_i - a_j)^2 + (b_i - b_j)^2}}{Mc}$$

Where (a_i, b_i) and (a_j, b_j) are the coordinates of the anchor nodes i, *j* and minimum cost.

Step 2: Based on minimum cost and optimized hop distance, next hop route is formed from source CH to CM.
Step 3: Source CH broadcasts minimum cost to all cluster members.
Step 4: Routing paths are formed and added if there is no routing information based on minimum cost and optimized hop distance.

Localization Approach to increase location accuracy

In this phase, localization approach is deployed to increase accuracy of node position and to provide balancing to energy consumption of unknown nodes. There are five steps to illustrate the performance of proposed localization approach.

Step1 : Unknown sensor node enters the cluster region and asks the permission from CH. CH checks stability and geographical position of node with less localization error and issue the ID. Unknown sensor node becomes cluster member and participates in packet forwarding. It will be monitored based on packet loss rate by CH.

Step 2: Localization error (Δ_{PE}) is predicted based on estimated and original location information. It is calculated as,

$$\Delta_{PE} = \frac{\sum_{i=1=}^{M} \sqrt[2]{(A_{pei} - A_i)^2 + (B_{pei} - B_i)^2}}{M}$$

M is the number of static nodes.

Step 3: Estimate the remaining energy (E_r) for individual cluster member located at cluster region.

$$E_r(k) = \frac{BC(k) - E_i(k)}{P_{aut}(k) - P_{avg}(k)}$$

Where *BC* is the batter capacity of node *k*. $E_i$is the initial energy of node *k*. $P_{aut}$is the automatic powered sensor node and P_{avg} is the average power of sensor node.

Step 4 : Estimate the location period of all cluster members and newly joined cluster members. Node location metric is divided into two cases i.e. M-A. where A is the number of anchor nodes.

Step 4: Update the location accuracy (L_a) of cluster members based on optimized hop distance and localization error.

$$L_a = \frac{\sum_{i=1}^{M} [OHD_{ij} - \Delta_{PE}]}{E_r}$$

Location accuracy is estimated based on optimized hop distance and energy consumed for discovery geographical position of sensor node with the negligible of localization error. This accuracy is maintained throughout the entire period to improve network lifetime.

Secure localization approach

In this phase, secure localization is integrated and it is mandatory to protect location information about sensor nodes to attackers. If any attacker wants to retrieve the location information, it may join the cluster region with fake ID and tries to find the location information. Authentication and data integrity plays a major role to protect location information and data packets from attackers. A concept of digital signature generation and verification [18] is used to retrieve the location information.

Key generation for Location information

Step 1: Each CM creates two different keys i.e. public key and private key. Public key is for signature verification and private key is for message authentication.
Step 2: Each CM should choose set $S_{CM} = \{S_{CM,o} : o \in U\}$ where $S_{CM,o}$ is one to one mapping for transformation of message signing.
Step 3: Transformation of message verification $(V_{CM})$is constructed without the knowledge of signer's private key.
Step 4: Obtain public key and private key for CM.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

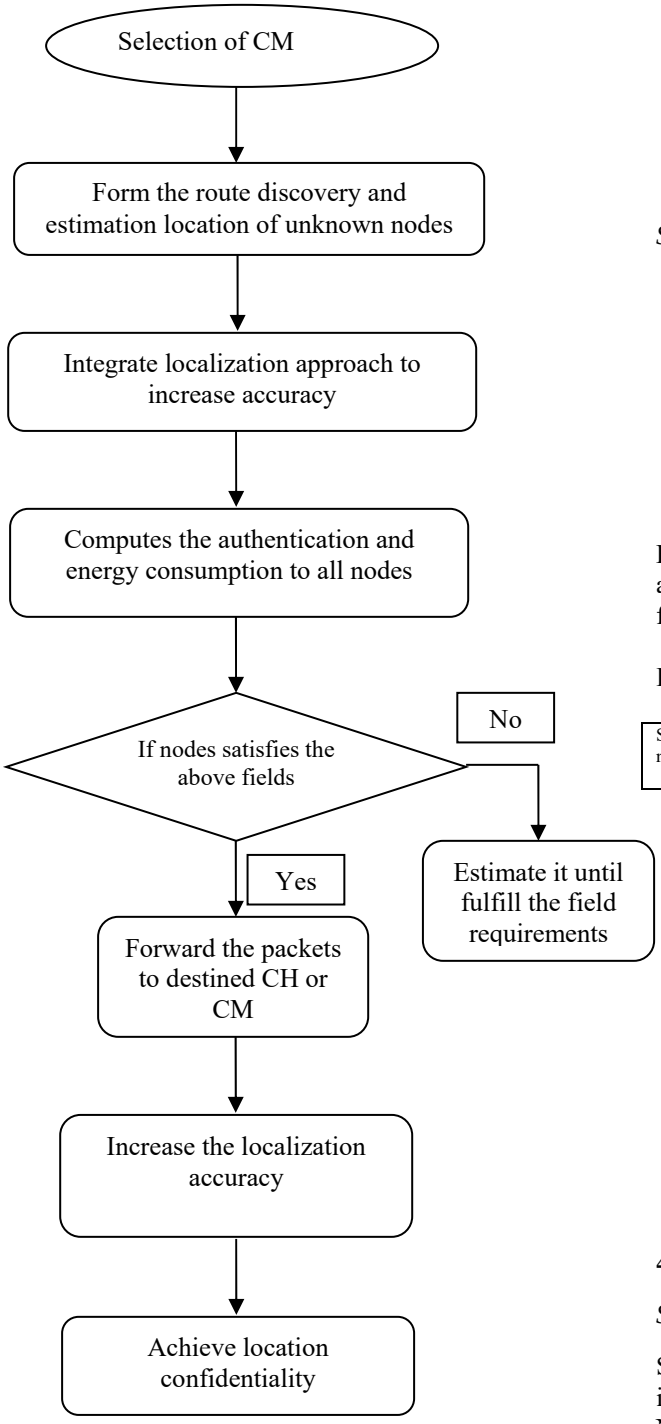

Figure 1. Flow of SLRP

Signature Generation

Cluster member should do the following:

1. Choose location message $L \in U$
2. Compute message transformation and signature transformation of unknown node location.
   $m = U(m), s = S_{CM,o}(m)$
3. Cluster member signature is S used to verify the signature and recover message from it.

Signature Verification

1. Find the CM's authentic public key V_{CM}.
2. Estimate $m = V_{CM}(s)$
3. If the signature is accepted, it belongs to $m \in M_U$ otherwise it is rejected.
4. Recover original message about location information *m* by computing $U^{-1}(m)$.

Figure 1 illustrates the flow of SLRP. The location accuracy is improved based on security and route formation among cluster members.

Packet format of Proposed Approach

Source node ID	Sink Node ID	Min. Cost Fn.	Location error	OHD	CRC
2	2	4	4	2	2

Figure 2.Proposed Packet Format

In Figure 2, the packet format of proposed scheme is shown. Both source and sink ID occupies 2 bytes. The location update value is obtained and it is obtained based on minimum cost function. In fourth field, location error is estimated and intimated to all cluster members. Optimal hop distance is estimated to keep shortest path between cluster members. CRC is Cyclic Redundancy Check used for error detection and error correction process.

4. PERFORMANCE EVALUATION

Simulation Model and Parameters

SLRP is simulated using Network Simulator tool. It is available as open source simulator. Updation of NS2 is more than other tools. The background language is C++ and front end is tool command language (tcl). It is easy to code and run the wireless network as well as ad hoc sensor network. The simulation settings are illustrated as given below.

Journal of Theoretical and Applied Information Technology
30th November 2017. Vol.95. No 22

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Our simulation settings and parameters are summarized in table 1

Table: 1Simulation Paremeters

No. of Nodes	100
Area Size	1200 X 1200 m^2
Mac	802.15.4
Radio Range	200m
Simulation Time	100 sec
Traffic Source	VBR
Packet Size	512 bytes
Mobility Model	Random Walk
Protocol	LEACH
Transmission power	0.895 watts
Received Power	0.0793 watts

Performance Metrics

The following metrics are defined to evaluate the performance of the proposed protocol SLRP.

Location accuracy: It defines the number of exact geographical position of sensor nodes which are normal to total number of location predicted.

Location update rate: It defines the ratio of node location update to unknown node locations.

Packet delay: Transmission of packets with time period from source to destination node.

Packet Delivery Ratio: It defines the number of packets received to number of packets sent.

Location Integrity Rate: It defines the integrity of location information to normalized location update value.

Control overhead: It defines the ratio of number of excessive control packets to number of data packets

The simulation results are presented in the next part. We compare our proposed protocol SLRP, with RMSP [11], MLS [10] ECHERP [19] and ENSOR [20] in the presence of unknown nodes.

C. Results

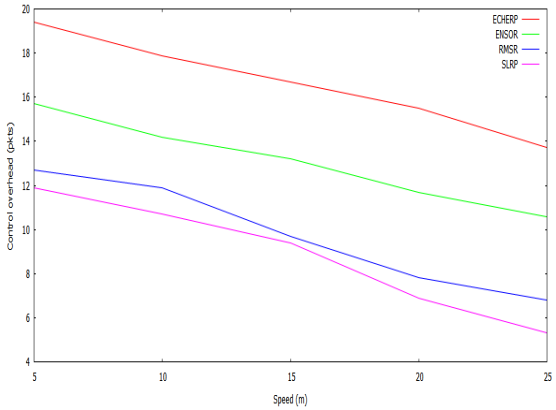

Figure 3. Control Overhead Vs Speed

Figure 3 shows the results of Overhead Vs Speed. Speed is varied as 5, 10, … 25 secs. Compared to existing schemes and protocols, the proposed protocol SLRP achieves less overhead because of location update value. This value is used to decrease the number of control packets during packet transmission phase. In existing scheme, localization procedure is not established based of minimum cost function.

Figure 4 show the results of packet delivery ratio by varying the number of nodes from 10 to 100 nodes. Clearly our protocol SLRP achieves more packet delivery ratio than schemes systems. The scheme comprises of two major aspects i.e. cluster member selection and route establishment.

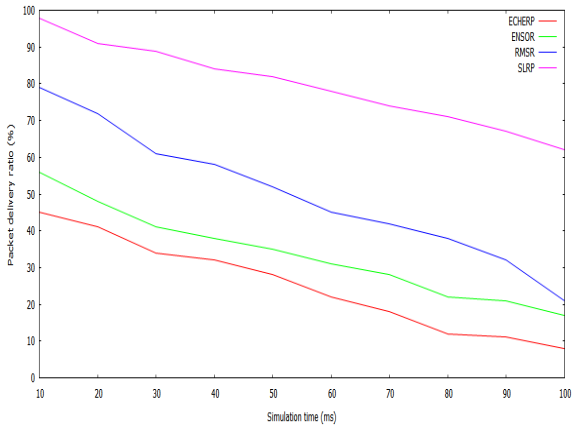

Figure 4. Packet Delivery Ratio Vs Simulation Time

Journal of Theoretical and Applied Information Technology
30th November 2017. Vol.95. No 22

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

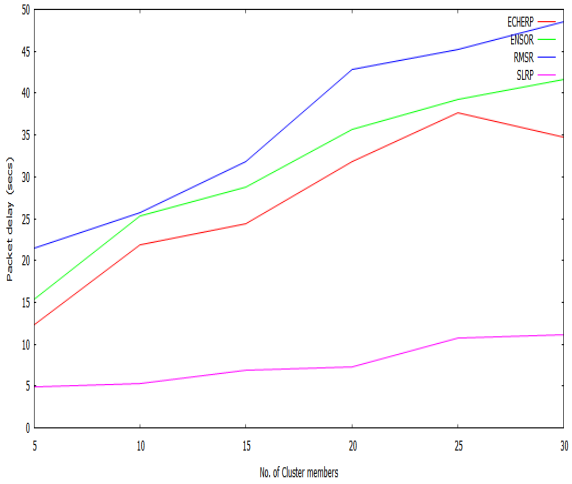

Figure 5. Packet Delay Vs No. Of Cluster Members

Figure 5 shows the results of Packet delay Vs cluster members. Based on the simulation results, SLRP achieves less delay than RMSR, ECHERP and ENSOR The proposed protocol reduces delay by means of distributed routing.

Figure 6 shows the results of location update rate Vs pause time. From the results, we can see that propose protocol SLRP achieves high location update rate because of iteration of trilateration model.

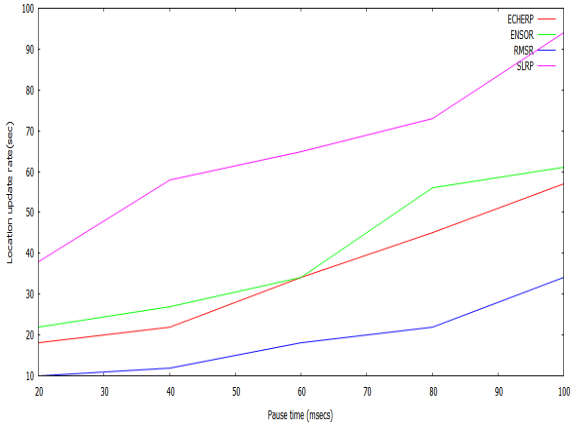

Figure6. Location Update Rate Vs Simulation Time

Figure 7 shows the results of Location Integrity Rate Vs No. of cluster members. From the results, we can see that proposed protocol SLRP has more location integrity rate than the previous work. The proposed system increases integrity rate by adding secure location authentication scheme.

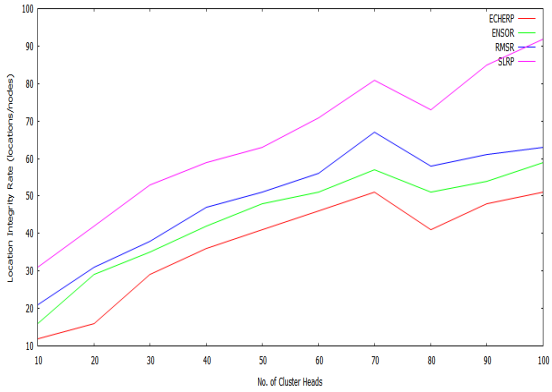

Figure 7. Location Integrity Rate Vs Number Of Cluster Members

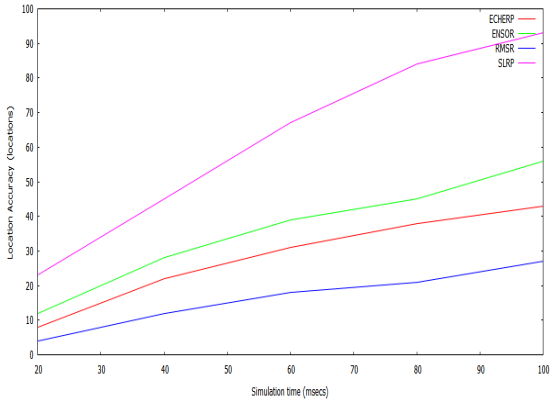

Figure 8. Location Accuracy Vs Simulation Time

Figure 8 shows the results of Location accuracy Vs No. of simulation time. Based on the extensive simulation results, the proposed protocol SLRP achieves more location accuracy than existing protocols.

5. CONCLUSION

Security is a major concern in all kinds of networks. In WSN, security localization is a major issue while packet transformation in the zone. Integration of security and energy is a difficult issue to compensate battery power and authentication of nodes as well as packets. In this research work, Secure Location Routing Protocol (SLRP) is proposed based on distance and packet loss rate. Nodes are located based on minimum cost function and optimized hop distance value. Security based localization approach is introduced to achieve authentication of location information. Based on the simulation results, the proposed scheme performs better than existing schemes and it is introduced to balance energy and

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

authentication based on location discovery procedure. In future, it is planned to secure the checkpoint by location aware routing in order to achieve a balance between location integrity and energy consumption.

REFERENCES

[1] Puneet Gurbani , Hansa Acharya , Prof. Anurag Jain, "Hierarchical Cluster Based Energy Efficient Routing Protocol for Wireless Sensor Networks: A Survey", International Journal of Computer Science and Information Technologies, Vol. 7 (2) , 2016, pp.682-687.

[2] P. Thangaraju and Kanjana S, "A Secure Energy Efficient and Aware Protocol for WSN", International Science Press, IJCTA, Vol.9, No.26, 2016, pp.357-362.

[3] Kyoungsoo Bok,1 Yunjeong Lee,2 Junho Park,3 and Jaesoo Yoo, "An Energy-Efficient Secure Scheme in Wireless Sensor Networks", Journal of Sensors, 2016, pp.1-11.

[4] A.V. Sutagundar and S.S. Manvi, "Location aware event driven multipath routing in Wireless Sensor Networks: Agent based approach", Egyptian Informatics Journal, 2013, Vol.14, pp.55–65

[5] M. Balamurugan and Dr. P. Manimegalai, " Efficient Tree Structure Based Revise Packet Byte Stuffing In Wireless Sensor Networks", Journal of Applied Sciences Research, 2016, Vol.12, No.10, pp.29-38.

[6] Sneetha Praneetha, Deepthi Janaga and Anjaneyulu, " Cost Aware Secure Routing (CASER) Protocol Design for Wireless Sensor Networks", International Journal of Advanced Technology and Innovative Research Volume. 08, IssueNo.12, September-2016, pp. 2397-2401.

[7] Junqi Duan, Dong Yang, Haoqing Zhu, Sidong Zhang, and Jing Zhao, "TSRF: A Trust-Aware Secure Routing Framework in Wireless Sensor Networks", International Journal of Distributed Sensor Networks, 2014, pp.1-14.

[8] Tran Dinh Hieu, Le The Dung and Byung-Seo Kim, "Stability-Aware Geographic Routing in Energy Harvesting Wireless Sensor Networks", MDPI, Sensors journal, Vol.16, 2016, pp.1-15.

[9] Celso Moraes and Dongsoo Har, "Charging Distributed Sensor Nodes Exploiting Clustering and Energy Trading", IEEE Sensors Journal, Vol. 17, No. 2, January 15, 2017, pp.546-555.

[10] Hamid Mahboubi, Walid Masoudimansour, Amir G. Aghdam and Kamran Sayrafian-Pour, "Maximum Lifetime Strategy for target monitoring with controlled node mobility in sensor Networks with Obstacles", IEEE Transactions on Automatic Control, Vol. 61, No. 11, 2016, pp.3493-3508.

[11] Hong Fu, Xiaoming Wang and Yingshu Li, "Adaptive Energy and Location Aware Routing in Wireless Sensor Network", Scientific Research Foundation of State Education Ministry for the Returned Overseas Chinese Scholars, 2016, pp.1-5.

[12] Cs. Firdozali and T. Nagamalar, " Energy Aware Mobile Sink Based RPL Routing Protocol for Wireless Sensor Networks", International Journal of Latest Technology in Engineering, Management & Applied Science, Vol.5, No.4, 2016, pp.74-78.

[13] P.Abinaya, S.Kohila, V.Idhayarani, A.Ramya and Mrs.A.R.Devi, " Load balancing in Wireless Sensor Network using energy aware routing protocol", International Conference on Emerging Engineering Trends and Science, pp.82-86.

[14] Deyu Zhang, Zhigang Chen, Ju Ren and Xuemin, "Energy-Harvesting-Aided Spectrum Sensing and Data Transmission in Heterogeneous Cognitive Radio Sensor Network", IEEE Transactions on Vehicular Technology, Vol. 66, No. 1, 2017, pp.831-843.

[15] Zubair Al Azim, Ankit Sharma, and Kaushik Roy, "Buffered Spin-Torque Sensors for Minimizing Delay and Energy Consumption in Global Interconnects", IEEE Magnetics Letters, Volume 8, 2017,pp.1-5.

[16] Haijun Zhang, Julian Cheng, Victor C. M. Leung and Arumugam Nallanathan, "Sensing Time Optimization and Power Control for Energy Efficient Cognitive Small Cell with Imperfect Hybrid Spectrum Sensing", IEEE Transactions on Wireless Communications, Vol.16, No.2, 2017, pp.730-743.

[17] Ashutosh Kumar Tiwari and Suresh Gawande, "M-SPIN- LA Algorithm for energy efficient Wireless Sensor Networks on 2D Surface ",International Research Journal of Engineering and Technology, Vol.3, Issue 06, 2016, pp.620-625.

[18] Alfred J. Menezes, Paul C. van Oorschot and Scott A.Vanstone, " Handbook of applied cryptography", 2016, pp.1-658.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[19] Stefanos A. Nikolidakis , Dionisis Kandris , Dimitrios D. Vergados and Christos Douligeris, "Energy Efficient Routing in Wireless Sensor Networks Through Balanced Clustering", Sensors, Vol.6 , 2013, pp.29-42.

[20] Juan Luo, Jinyu Hu, Di Wu, and Renfa Li,"Opportunistic Routing Algorithm for Relay Node Selection in Wireless Sensor Networks", IEEE Transactions on industrial informatics, Vol. 11, No. 1, 2015, pp.112-121.