Circuits and Systems, 2016, 7, 2014-2024
Published Online June 2016 in SciRes. http://www.scirp.org/journal/cs
http://dx.doi.org/10.4236/cs.2016.78175

ECBK: Enhanced Cluster Based Key Management Scheme for Achieving Quality of Service

Y. Harold Robinson[1], S. Balaji[1*], M. Rajaram[2]

[1]Department of Computer Science and Engineering, SCAD College of Engineering and Technology, Cheranmahadevi, India
[2]Vice-Chancellor, Anna University, Chennai, India
Email: yhrobinphd@gmail.com, [*]sbalajiphd@gmail.com, rajaramgct@rediffmail.com

Received 20 April 2016; accepted 15 May 2016; published 29 June 2016

Abstract

Wireless sensor networks consist of many small nodes with distributing devices to monitor conditions at different locations. Usually wireless sensor nodes are sprinkled in a sensor field grouping limited areas. This paper highlights the Enhanced Cluster Based Key management (ECBK) protocol to achieve secure data delivery based on clustering mechanism. This protocol gives more importance to Cluster Coordinator node, which is used to coordinate the members and provide protective communication among the sensor nodes to enhance reliability. In Enhanced Cluster Based Key management two types of nodes are deployed. The high power nodes form clusters with surrounding nodes to enable the routing process without interference. This paper introduces ECBK protocol that balances the load among the clusters, achieves high throughput, end to end delay will be reduced, routing overhead also reduced and also it prolongs the network lifetime. Simulation results show that the presence of high transmission nodes reduces the delay, load balance, routing overhead, and enhances the throughput increased by 45% compared to other similar methods.

Keywords

WSN Security, Cluster Head, Cluster Coordinator Node, Dynamic Self-Healing, Energy

1. Introduction

Wireless sensor network (WSN) is a collection of micro sensors that are powered by low energy batteries and

[*]Corresponding author.

How to cite this paper: Robinson, Y.H., Balaji, S. and Rajaram, M. (2016) ECBK: Enhanced Cluster Based Key Management Scheme for Achieving Quality of Service. *Circuits and Systems*, **7**, 2014-2024. http://dx.doi.org/10.4236/cs.2016.78175

equipped with micro processors, small memory and radio transceivers. Security of these networks emerges as a critical issue [1]. Without proper security, it is impossible to trust [2]-[4] the results collected from sensor networks [5]. Main security threats in WSN are node Sybil attack, compromise attack, code injection attack Hello flood attack and selective forwarding attack. Security mechanisms and key management schemes are used to detect threats to individual sensor nodes [6]-[8]. To design secure wireless sensor networks, security measures may be incorporated in sensor nodes.

Sensor nodes trusts on battery power providing. Their communication capability and energy storage capability are very restricted [9]. Hence efficient utilization of node energy, balancing network energy consumption and extension of network lifetime has become a primary design objective for wireless sensor network. Clustering is proved to be an efficient scheme for growing the lifetime of WSNs [10] [11]. In a clustering scheme the nodes are divided into groups. They are mostly based on geographical properties. Each group has a single leader (Cluster Head) and several ordinary nodes (Member Nodes). A cluster head usually serves as a local coordinator for its cluster, playing intra-cluster transmission arrangement, data aggregation, forwarding [12] and so on. In the network model, gateway nodes connect between different clusters if there is no direct communication between the cluster heads [13]. The objectives of the clustering are to decrease the total of the transmission power which is summed up over selected path of the nodes and to balance the load among the selected path of the nodes for growing the network lifetime [14] [15].

Enhanced Cluster Based Key management scheme for wireless sensor network can be used to increase the network lifetime in a secured way. These protocols have the Cluster Head Algorithm which is used to generate the coordinator node to increase the enhancement of the network lifetime of the Wireless Sensor Network.

2. Related Work

Clustered routing is suitable for networks which deploy large number of nodes and are highly scalable. In 2004, the first clustering algorithm LEACH was proposed for dropping power utilization. In LEACH, the clustering task is rounded among the selected paths of the nodes, based on time period. Cluster Head (CH) is used to communicate directly to forward the data to the Base Station (BS). Even as most efforts so far have focused on an energy-efficient clustering scheme [16], attention to the performance of multi-hop network was quite limited. In [17] hierarchical soft clusters with fuzzy enabling non-exclusive overlap clusters are implemented using a total version of time-division multiple access (TDMA). Although the clustering shows good performance, the sink is assumed to be reachable which may not be the case always. A new protocol LEACH-R planned in [18] improves the choice of cluster-head by considering the residual energy of the nodes throughout selection of cluster-head, thereby reducing the likelihood of low-energy nodes being selected. However, analysis of the cluster head trustworthiness has not been thought of. CLENER protocol [19] provides energy-efficiency by cluster formation using fuzzy logic and Cluster Head election based on a probability function. The drawback is that the base station has not been subjected to energy restrictions and is located inside the sensing field. Trust evaluation of Cluster Head has been successfully carried out in [20]. Every Cluster Head reports its trust execution result to all other Cluster Heads to the BS that is infallible with all other physical security. A novel Cluster Based Routing Protocol (CBRP) for prolonged sensor network lifetime has been proposed in [21]. In the set-up phase, clusters are generated followed by the steady-state phase where a routing tree is constructed and aggregated data are sent to the sink node. In CBRP protocol, each node maintains a table that contains the neighborhood information about its neighbors consuming time to build the routing tree and maintaining the table. In [22] a Cluster-based Energy-efficient Scheme (CES) for elect a cluster-head to evenly issue energy utilization in the overall network and therefore obtain a longer network lifetime has been proposed. Each sensor is responsible for maintaining a table called Table Cluster, in which information from the local cluster members is stored. Hence proper updating of table information becomes necessary. Cluster based routing protocol for heterogeneous WSN proposed in [23] minimizes the energy consumption and increases the network survivability. However, the nodes are assumed to be uniformly distributed in the network. All nodes can send data to the base station. Hence reliability and trust are not considered [24]. Proposes Uniform Distribution Technique (UDT) for selecting CHs and to make a network throughout that every sensor remains within the transmission vary of CHs and so, the amount of the network is prolonged. This technique does not consider heterogeneous nodes. An energy-efficient scheme is usually evaluated by the network lifetime which is measured by the time that the first or the last node dies. Thus, network lifetime is tightly coupled with the network performance [25]-[28].

A Distribution Group Key theme for Wireless Sensor Networks has been proposed in the net of things situation. As an imperative a part of the web of Things (IoT), Wireless Sensor Networks (WSNs) need to be completely integrated into the web. Key cluster distribution scheme for WSNs in the IoT scenario organizes sensor nodes into groups. Each group has a hierarchical structure. The secure finish-to-end communication [29] protocol is employed to distribute cluster keys for subgroups to the trustworthy head nodes and also the head nodes then share out the cluster keys from end to finish underlying tree-based topology and wireless multicast to reduce energy utilization. Deals with a hybrid key management Scheme based on Wireless clustered Sensor Networks. Based on node's own location the weakness of session key is constructed. The use of hierarchical thinking reduces the amount of key storage and computing. The results of simulation show our proposed algorithm outperforms DSH (Dynamic Self-Healing) protocol [30] DD and LEACH in terms of conserving energy, security and prolonging WSN lifetime.

3. Network Model

To change the network model, we tend to affordable a few reasonable assumptions as follows. **Figure 1** demonstrates the Network Model for the Proposed System.

1) There are *n* sensor nodes that are distributed randomly in an *x*, *y* square field.
2) All the nodes and the BS are stationary after deployment.
3) All the sensor nodes can be homogeneous except cluster head.
4) Each node has an identity (*id*).
5) Assume that the cluster coordinator node has the following properties:

a) the base station sends query request tasks and broadcasts to the member nodes;
b) it maintains the energy of each node, location and other information;
c) it makes dynamic perception adding or removing nodes;
d) it establishes virtual path among the cluster nodes and other cluster coordinator nodes for information transmission and maintains established routes;

4. ECBK Working Process

Trustworthy ECBK is used to improve the security of the network, by introducing a simple key management mechanism. Data transmission take place between the clusters and cluster members is completed through associate increased multi-path mechanism which additional improves the responsibility of data transmission and implements network load equalization. The cluster objectives area unit to minimize the overall transmission power aggregated over the nodes within the designated path and to balance the load among the nodes for prolonging the network life.

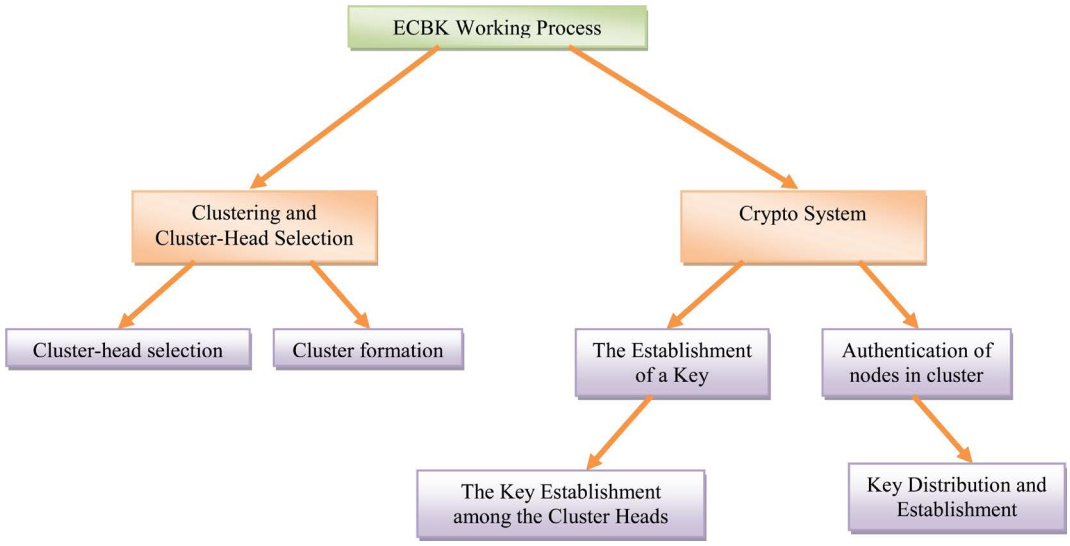

Figure 1. Network model.

ECBK protocol is composed of the following modules:

1) Clustering and Cluster-Head selection
2) Cryptosystem which includes
- Authentication of the nodes in cluster
- Key Distribution and Establishment
3) Routing Protocol for sensor network

4.1. Clustering and Cluster-Head Selection

Nodes are randomly deployed. Transmission range of nodes is set to either 250 m or 350 m. Nodes with range 350 m are deployed less compared to nodes with 250 m range. Nodes with 350 m range are labeled Cluster-Head (CH) and nodes with 250 m range are labeled cluster Member Node (CMN). This research work is intended for intra cluster communication for cluster formation and CH selection is based on high energy.

Phase-I Cluster-head selection

Sensor nodes deployed within the environment, all the nodes send their energy levels to the base Station. On the energy level and geographic area, a node with high energy will be selected as Cluster Head. The base station is well educated concerning the geographical locations of the nodes. Base Station can choose the Cluster Heads and multicast this data to them.

Select Cluster Head (NetInfo)

Node Ni send N_i (EL_i, L_i) to BS//El_i is energy level of node, L_i is Location of node

If El_i > e select i^{th} node as CH//e is threshold value, CH is cluster head

Else Ni is MN//MN is member node

Phase-II—Cluster formation

After Cluster Head selection the cluster formation section starts. Each Cluster Head broadcasts its status as Cluster Head to the surrounding nodes. Nodes with Received Signal Strength Indicator (RSSI) worth response to this beacon message and show their temperament to affix this cluster. The node sends a request to the various Cluster Head and in response be a part of Confirmed Alert is shipped by the Cluster Head. In this approach clusters are formed with one Cluster Head each. One in every of the Cluster Member will act as a Coordinator node. It will not sense any data. It only coordinates and controls the Cluster Head's work such as selecting the direction of data transfers.

Make cluster() Send CH(netInfo) to Ni

If Ni. RSSI = 1//RSSI is received signal strength indicator

Then send Ni(req) to CH//req is request message

Send CH(ack) to Ni//ack is ackowlegement

If Ni.ack = 1

Ni is MN//MN is member node

4.2. Crypto System

Security mechanisms and key management scheme detect threats to individual sensor nodes. To implement a secure connection between the nodes it requires the establishment of a key. Different types of keys are needed for different types of nodes. Cluster Head and Base Station stores preloaded master key whose main function is to prevent the network attack during initialization which causes information to be stolen and $K_m$generates the key pair which will be automatically sent to coordinator node. This phase is divided into three parts as follows.

4.2.1. The Establishment of a Key among Cluster Coordinator Nodes and Base Stations

Each coordinator node and base station generates a session key according as follows:

$$R_{ki} = \left(K_m, R\right) \tag{1}$$

where R is a random number for a base, with the coordinator node's private key. Base station key K_m ($m = 1, 2, \cdots, n$) encrypted obtaining R_{ki} and sent to each coordinator node. Communication between coordinator nodes and base station in order encrypt to guarantee authentication should be deposited in the key.

4.2.2. Authentication of Nodes in Cluster

Each cluster member node for data transmission contains the same initial energy and has a unique ID number. A Cluster coordinator node is identified and maintained in each cluster. It monitors cluster node and helps in the nodes authentication to the Base Station. CCN is the cluster coordinator node and CCN_i is the i is number of cluster ($i = 1, 2, \cdots, n$) node, V represent maximum number of round, MACR represent as cryptographically certified MAC**.** $A \rightarrow B\{C\}$ indicates that A sends the message C to B, and ACK is the acknowledgement [15] [16].

4.2.3. The Key Establishment among the Cluster Heads

According to R_{ki} and hash function F generate a unique key and key pair, such as coordinator node CCN ID for CCN identifier, and L_{ccn} as its position information. Based on the two key, K_{ccn} is generated as follows:

$$K_{ccn} = FR_{ki}\left(ID_{ccn}, L_{ccn}\right) \tag{2}$$

4.2.4. Key Distribution and Establishment

Cluster coordinator nodes communicate with the Base Station to inform the number and location of the Cluster Head. Each Cluster Head CH_i ($i = 1, 2, \cdots, m$) stores allocation key share. Key segmentation process is summarized as follows. The base station first generates the function ENC and E will be encrypted as secret S, E = $ENC_k(s)$. Using decomposition algorithm divide E into m obtaining $E_1, E_2, \cdots, E_m$, and assign to each cluster head. The key K is then divided into m obtaining $k_1, k_2, \cdots, k_m$. Finally put two tuples $\left(E_i, k_i\right)$ ($i = 1, 2, \cdots, m$) as Key Shadow S_i and send to the Cluster Head CH_i [16] [18]. Before communication, each kind of nodes also needs node-to-node authentication. If this succeeds, data transmission can be carried out.

4.2.5. Routing Protocol for Sensor Network

The following steps involved in the General routing- Best Forwarder selection

1) Find if Destination node is found among the neighbours.
2) If found, set the next hop as Destination node and Exit. Else continue.
3) For each member -node among the neighbours, do the following:
   //Check for positive progress towards destination
4) Check if its distance from the Destination node is greater than or equal to the distance between the current forwarder and Destination node. If yes, break. Else, add node to an array.
5) Find the nodes in the array, based on their distance to destination.
6) If the node has reception power greater than the threshold value, choose that node as the Best Forwarder. Else consider the next node in array.
7) Exit.

Algorithm for cryptosystem

1) Generate session key $R_{ki} = E\left(R, k_m\right)$ by base station and co-ordinator node.
2) CCN_i sends status request message as $CCN_i \rightarrow$ BS {i, REQ, R_{ki}} to BS.
3) BS receives REQ message and find CCN_i corresponding R_{ki} replay as BS $\rightarrow$ CCN_i {V_i, MACR_i (ACK)} to CCN_i
4) CCN_i receives this message, calculate (ID_i) and send a message as $CCN_i \rightarrow$ BS {$V*i$, ID_iMAC(ACK)} to BS.
5) If BS receives this message then CCN_i authentication is successful. Else retransmission mechanism is needed.
6) Generate key among cluster head $K_{ccn} = FR_{ki}\left(ID_{ccn}, L_{ccn}\right)$ according to hash function F as and session key R_k
7) For distribute the key CH_i first Base station generate ENC function E = $ENC_k(s)$
8) Then using the decomposition algorithm E is divided into $E_1, E_2, \cdots, E_m$ and key is divided into $k_1, k_2, \cdots, k_m$ and put the tuple as $\left(E_i, k_i\right)$ $i = 1, 2, \cdots, m$ as key shadow S_i then send to Ch_i

If these steps are succeeded then carried out the transmission.

5. Performance Evaluation

The proposed scheme is based on ECBK protocol. The main goal is to enhance the security of data transmission and prolong the network lifetime. Network parameters and values are given below (**Table 1**).

To evaluate the network performance, metrics such as load balancing, average end-to-end delay, network

throughput and routing control overhead are considered. The proposed protocol is compared with Distributed Self-Healing protocol where no cluster formation is done, DD and LEACH.

Performance Metrics

Load balancing factor uses comprehensive weight value composed of distance between the head and the member and the residual energy to improve cluster member choice.

It also uses optimization threshold value to avoid load imbalance. B_f to measure the balance degree of clusters is given by

$$B_f = 1/n - m\left(N_{\text{low}}\right) \tag{3}$$

where N_{low} is the number of nodes with energy lower than the average of the total number of nodes in the network, m is the number of cluster coordinator nodes, n is the total number of nodes, $n - m$ is the number of participating nodes in the data transmission.

The graph in **Figure 2** shows the load balance factor of the proposed protocol. The simulation time is plotted along the X axis and load balance value is plotted along the Y axis. This graph shows that ECBK outperforms the other protocols in terms of load balance factor. ECBK chooses the node with high energy to become the cluster head. Since the Cluster head and routing path are chosen for each transfer, the energy levels of the nodes remain balanced.

Average end-to-end delay is the average of the sum of delays for transmission of packets from source cluster head to the destination given by

$$ED = 1/n - m\sum_{t\in Ts} td \tag{4}$$

where *td* is the data transmission delay of cluster heads.

Table 1. Network parameters.

Parameters	Value
Number of nodes	Up to 500
Number of cluster head	4
Transmission range of CH	350 m
Transmission range of MN	200 m
Initial energy	100 Joules
Network topology	1000 × 1000 m^2
Antenna model	Omni antenna
Propagation model	Two-ray ground
Simulation time	100 sec

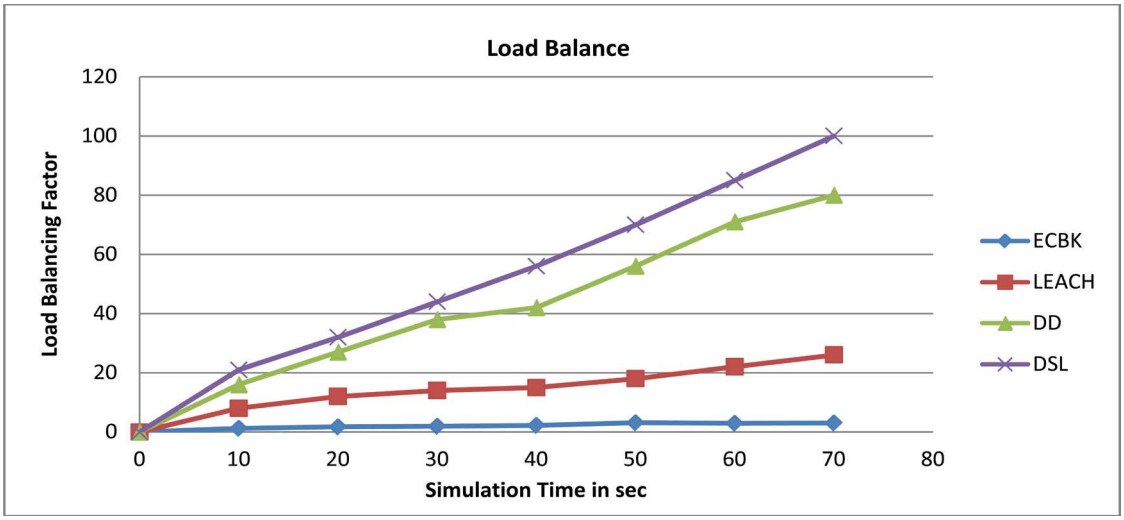

Figure 2. Load balance.

In **Figure 3** the average number of time delays is plotted against end-to-end delay. The graph shows that the proposed protocol performs better than DCL and DD. However its performance is similar to LEACH during the start of the simulation but performs better than LEACH as time increases. In ECBK, nodes that make positive progress towards the destination are chosen. Hence path deviation is eliminated. High energy nodes tend to broadcast in a better manner. The above stated two reasons can be accounted for the less end to end delay.

Network throughput is the number of packets of successful transmission given by

$$Tp = (n-m)P_{\text{send}}/T_s \tag{5}$$

where, time is denoted as T_s and P_{send} is each cluster head that sends the packet number.

The graph shown in **Figure 4** is used to identify the network throughput in different time periods. The proposed protocol shows better network throughput compared to the other protocols.

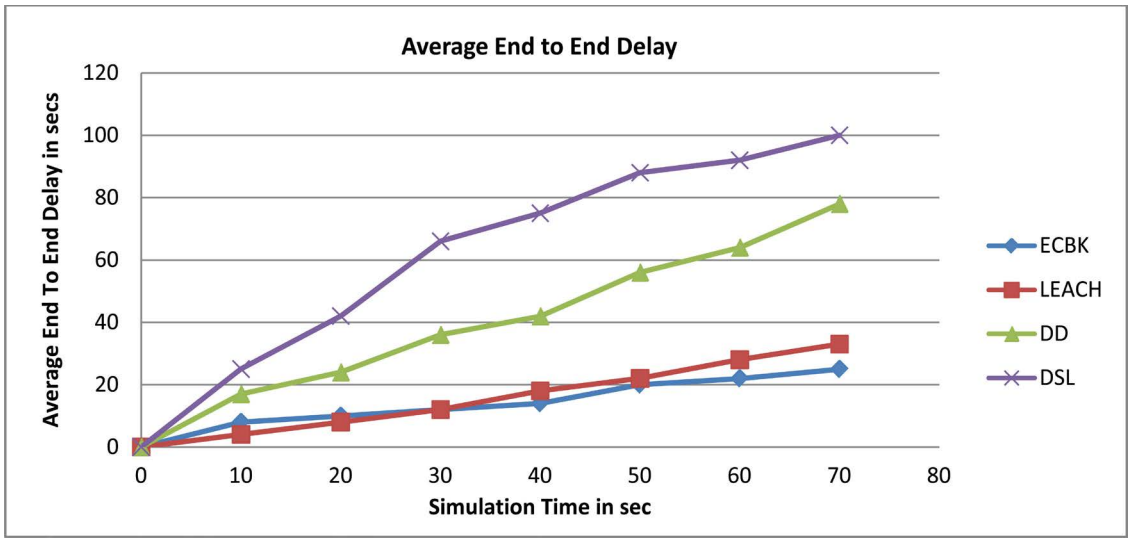

Figure 3. Average end-to-end delay.

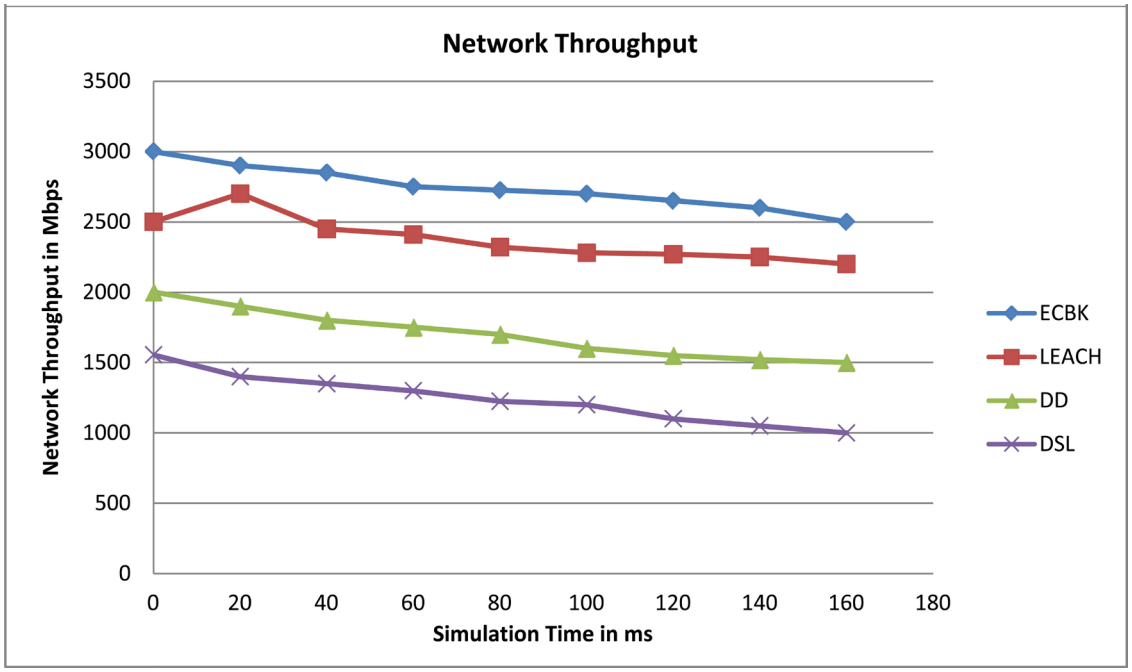

Figure 4. Network throughput.

The network throughput of ECBK is highest compared to the other protocols, as seen in **Figure 5** because high energy nodes are chosen as Cluster Heads and only nodes with the threshold reception power are chosen for intermediate hops.

Routing Control Overhead: overhead will increase the extent of disseminated unwanted data and redundant process at intermediate nodes further as base station

$$EC = D_C + T_C \tag{6}$$

where D_C is the pay expenses which are cluster coordinator node controlling according to the built path transmission cluster heads need and

T_C is multiple paths in need of the overhead of data transmission.

Figure 5 shows the routing overhead in network. The proposed protocol performs far better than DSL and DD. As time increases it performs better than LEACH. Opportunistic routing done by ECBK is responsible for the reduced routing overhead.

Longevity

The numbers of alive nodes are calculated for several simulation periods.

The graph in **Figure 6** indicates that ECBK ensures more number of nodes alive for the different simulation times

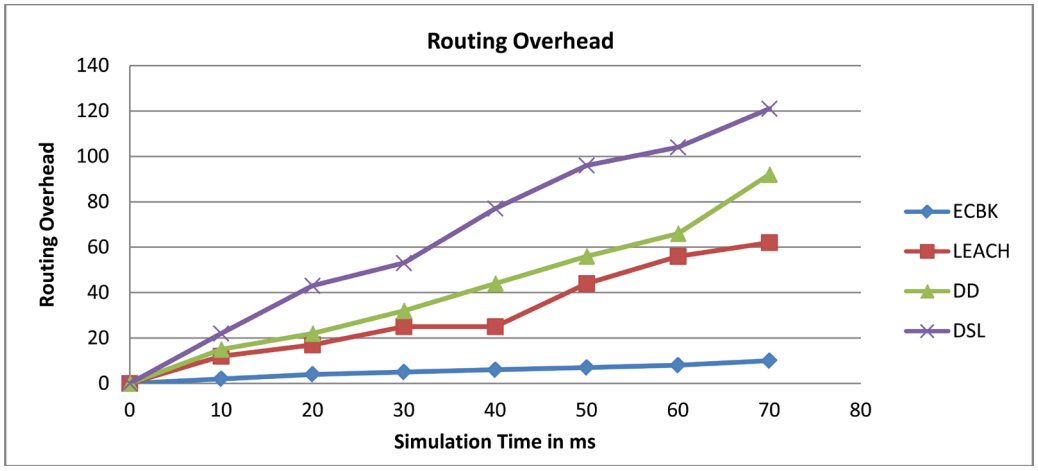

Figure 5. Routing overhead.

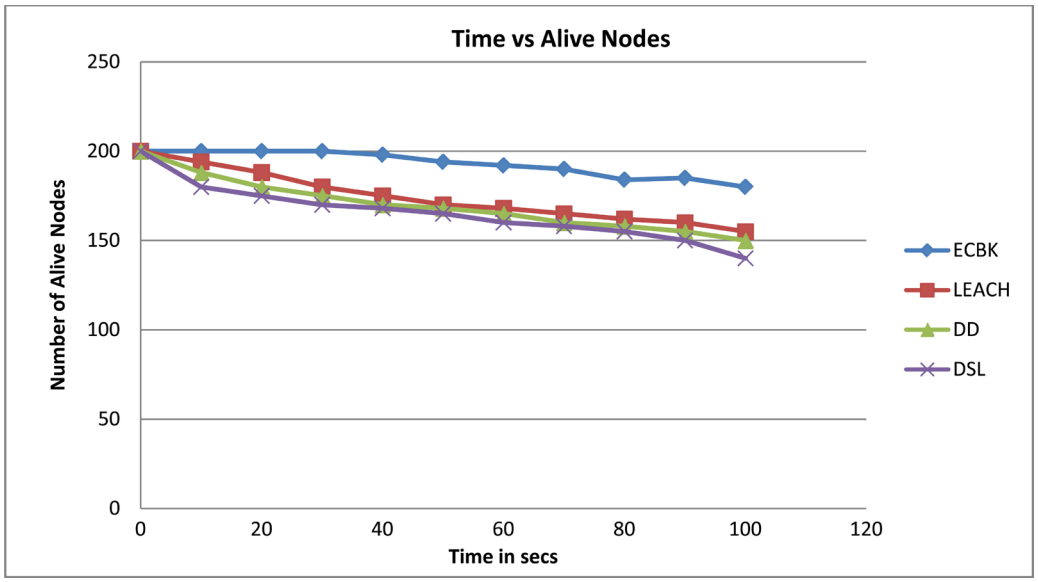

Figure 6. Node longevity.

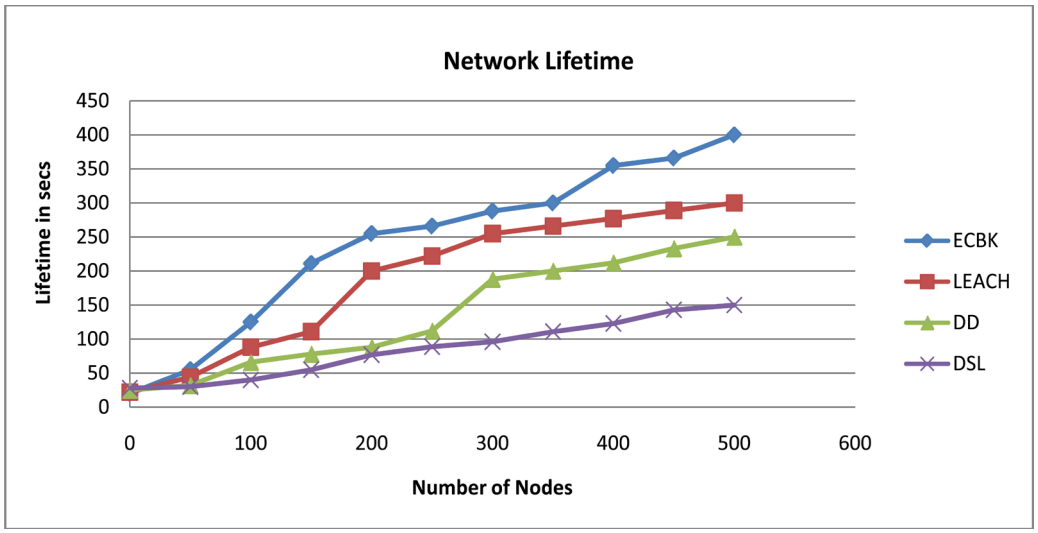

Figure 7. Network Lifetime.

Network Lifetime

As seen in **Figure 7**, ECBK prolongs the lifetime of the network due to increased longevity of nodes. High energy node selection for Cluster Head and opportunistic routing can be accounted for the better performance.

6. Conclusion

In this paper clustering with key management scheme ECBK is proposed for routing in WSN. ECBK helps to solve the problems encountered in data transmission security by introducing a simple key management mechanism, the secret sharing technology. In order to increase the reliability of the working node we also introduced the node evaluation mechanism is incorporated and low trust value nodes have been dropped. General routing-Best cluster selection algorithm is employed, which further improves the reliability of data transmission and implements network load balancing. The clustering objectives are to minimize the total transmission power of the selected path of the nodes and the balancing in the selected path of the nodes for increasing the lifetime of the network. Simulation tests demonstrate that ECBK performs much better than LEACH, DD and DHL in terms of load balance, average end to end delay, throughput and routing overhead. The simulation results proved that the ECBK is performed well compared to all the other Cluster based Scheme methods. Congestion control algorithms, mobile sink and proper scheduling methods can be incorporated into ECBK as future work.

References

[1] Akyildiz, I.F., Su, W., Sankarasubramaniam, Y. and Cayirci, E. (2012) Wireless Sensor Networks: A Survey. *Computer Networks*, **38**, 393-422. http://dx.doi.org/10.1016/S1389-1286(01)00302-4

[2] Golden Julie, E., Tamil Selvi, S. and Harold Robinson, Y. (2014) Opportunistic Routing with Secure Coded Wireless Multicast Using MAS Approach. World Academy of Science, Engineering and Technology, *International Journal of Computer*, *Electrical*, *Automation*, *Control and Information Engineering*, **8**, 1247-1250.

[3] Harold Robinson, Y. and Rajaram, M. (2015) Energy-Aware Multipath Routing Scheme Based on Particle Swarm Optimization in Mobile Ad Hoc Networks. *The Scientific World Journal*, 1-9. http://dx.doi.org/10.1155/2015/284276

[4] Harold Robinson, Y. and Rajaram, M. (2015) Establishing Pairwise Keys Using Key Predistribution Schemes for Sensor Networks. World Academy of Science, Engineering and Technology, *International Journal of Computer*, *Electrical*, *Automation*, *Control and Information Engineering*, **9**, 608-612.

[5] Harold Robinson, Y. and Rajaram, M. (2014) A Novel Approach to Allocate Channels Dynamically in Wireless Mesh Networks. World Academy of Science, Engineering and Technology, *International Journal of Computer*, *Electrical*, *Automation*, *Control and Information Engineering*, **8**, 1865-1868.

[6] Modirkhazeni, A., Ithnin, N. and Ibrahim, O. (2010) Secure Multipath Routing Protocols in Wireless Sensor Networks: A Security Survey Analysis. *Proceedings of the 2nd International Conference on Network Applications, Protocols and Services* (*NETAPPS*'10), Kedah, 22-23 September 2010, 228-233. http://dx.doi.org/10.1109/netapps.2010.48

[7] Harold Robinson, Y., Rajaram, M., Golden Julie, E. and Balaji, S. (2016) Dominating Set Algorithm and Trust Evaluation Scheme for Secured Cluster Formation and Data Transferring. World Academy of Science, Engineering and Technology, *International Journal of Computer, Electrical, Automation, Control and Information Engineering*, **10**, 388-393.

[8] Taruna, S., *et al*. (2013) A Cluster Based Routing Protocol for Prolonging Network Lifetime in Heterogeneous Wireless Sensor Networks. *International Journal of Advanced Research in Computer Science and Software Engineering*, **3**, 658-665.

[9] Ramalakshmi, S. and Robinson, Y.H. (2014) ATMPH: Attaining Optimal Throughput Capacity of MANET with Power Control in Heterogeneous Network. *Programmable Device Circuits and Systems*, **6**, 111-115.

[10] Long, J.Z., Chen, Y.T., Deng, D.M., *et al*. (2011) Assistant Cluster Head Clustering Algorithm Based on LEACH Protocol. *Computer Engineering*, **37**, 103-105.

[11] Zhang, T., Li, L. and Yan, C. (2009) A Secure Cluster-Based Router Protocol for WSNs. *Chinese Journal of Sensors and Actuators*, **22**, 1612-1616.

[12] Balaji, S. and Rajaram, M. (2016) SIPTAN: Securing Inimitable and Plundering Track for Ad Hoc Network. Wireless Personal Communications, Springer, 1-21. http://dx.doi.org/10.1007/s11277-016-3187-y

[13] Zhao, P.C., Xu, Y. and Nan, M. (2012) A Hybrid Key Management Scheme Based on Clustered Wireless Sensor Networks. *Proceedings of the IEEE 2nd International Conference on Computer and Management*, 1394-1397. http://dx.doi.org/10.4236/wsn.2012.48029

[14] Nadimpalli, B.V., Mulukutla, P., Garimella, R. and Srinivas, M.B. (2004) Energy-Aware Routing in Sensor Networks Using Dual Membership Clusters and Data Highways. *Proceedings of the IEEE Region* 10*th Conference Analog and Digital Techniques in Electrical Engineering* (*TENCON*'04), 21-24 November 2004, C184-C187. http://dx.doi.org/10.1109/tencon.2004.1414738

[15] Sun, X. and Coyle, E.J. (2012) The Effects of Motion on Distributed Detection in Mobile Ad Hoc Sensor Networks. *International Journal of Distributed Sensor Networks*, **1**, 14 p.

[16] Rijin, I.K., Sakthivel, N.K. and Subasree, S. (2013) Development of an Enhanced Efficient Secured Multi-Hop Routing Technique for Wireless Sensor Networks. *International Journal of Innovative Research in Computer and Communication Engineering*, **1**, 506-512.

[17] Harold, R.Y. and Rajaram, M. (2016) A Memory Aided Broadcast Mechanism with Fuzzy Classification on a Device-to-Device Mobile Ad Hoc Network. *Wireless Personal Communications*, 1-23.

[18] Kamath, H.S. (2013) Energy Efficient Routing Protocol for Wireless Sensor Networks. *International Journal of Advanced Computer Research*, **3**, 95-100.

[19] Neto, A. (2013) A Cluster-Based Approach to Provide Energy-Efficient in WSN. *International Journal of Computer Science and Network Security*, **13**, 55-62.

[20] Harold, R.Y. and Rajaram, M. (2015) Trustworthy Link Failure Recovery Algorithm for Highly Dynamic Mobile Adhoc Networks. World Academy of Science, Engineering and Technology, *International Journal of Electrical, Computer, Energetic, Electronic and Communication Engineering*, **9**, 233-236.

[21] Bager, Z., Zeynali, M. and Nezhad, V.M. (2010) Novel Cluster Based Routing Protocol in Wireless Sensor Networks. *International Journal of Computer Science*, **7**, 32-36.

[22] Lehsaini, M., *et al*. (2008) CES: Cluster-Based Energy-Efficient Scheme for Mobile Wireless Sensor Networks. Vol. 264, *Proceedings of the* 2008 *IFIP Conference on Wireless Sensor and Actor Networks* (*WSAN 08*), *Ottawa*, 14-15 July 2008, 13-24. http://dx.doi.org/10.1007/978-0-387-09441-0_2

[23] Beldjehem, M. (2013) Toward a Multi-Hop, Multi-Path Fault-Tolerant and Load Balancing Hierarchical Routing Protocol for Wireless Sensor Network. *Wireless Sensor Network*, **5**, 215-222. http://dx.doi.org/10.4236/wsn.2013.511025

[24] Robinson, Y.H. and Rajeswari, S.R. (2011) Energy-Based Dynamic Encryption for Wireless Sensor Networks. *Wireless Communication*, **3**, 661-663.

[25] Nabizadeh, H. and Abbaspour, M. (2011) IFRP: An Intrusion/Fault Tolerant Routing Protocol for Increasing Resiliency and Reliability in Wireless Sensor Networks. *Proceedings of the International Conference on Selected Topics in Mobile and Wireless Networking* (*ICOST*'11), Shanghai, 10-12 October 2011, 24-29. http://dx.doi.org/10.1109/icost.2011.6085830

[26] Yu, H., He, J., Zhang, T. and Xiao, P. (2012) A Group Key Distribution Scheme for Wireless Sensor Networks in the Internet of Things Scenario. *International Journal of Distributed Sensor Networks*, **2012**, Article ID: 813594. http://dx.doi.org/10.1155/2012/813594

[27] Alrajeh, N.A., Khan, S. and Shams, B. (2013) Intrusion Detection Systems in Wireless Sensor Networks: A Review. *International Journal of Distributed Sensor Networks*, **2013**, Article ID: 167575.

http://dx.doi.org/10.1155/2013/167575

[28] Lopez, J., Roman, R., Agudo, I. and Fernandez-Gago, C. (2014) Trust Management Systems for Wireless Sensor Networks: Best Practices. *Computer Communications*, **33**, 1086-1093. http://dx.doi.org/10.1016/j.comcom.2010.02.006

[29] Lu, R., Lin, X., Zhu, H., Liang, X. and Shen, X. (2012) BECAN: A Bandwidth-Efficient Cooperative Authentication Scheme for Filtering Injected False Data in Wireless Sensor Networks. *IEEE Transactions on Parallel and Distributed Systems*, **23**, 32-43. http://dx.doi.org/10.1109/TPDS.2011.95

[30] Balaji, S. and Rajaram, M. (2014) EUDIS-An Encryption Scheme for User-Data Security in Public Networks. World Academy of Science, Engineering and Technology, *International Journal of Computer, Electrical, Automation, Control and Information Engineering*, **8**, 2039-2044.