International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

WSEECM: Wireless Sensor Network System with Secure and Energy Efficient Cluster Management

Ruchika Jain

Smt Kashibai Navale Sinhgad College of Engineering, Affiliated to Savitribai Phule University, Vagdaon(Bk), Pune, India

Abstract: ***Increasing network lifetime of energy-constrained sensor nodes is a crucial issue, different researches are directed just to increase network uptime either by changing network topology, providing shortest routing decisions or by efficiently selecting cluster head in a cluster which reduces bandwidth usage while individual direct data forwarding by aggregating data from all nodes in a cluster and reachable to other nodes in minimum hops. Wireless Sensor Network System with Secure and Energy Efficient Cluster Management (WSEECM) elects cluster head on the basis of residual energy, the distance of a node to base station and a maximum number of nodes in its range. Cluster Head selection is secure, less energy and time-consuming increases the network lifetime of the sensor network. Security is another major issue in such network, for secure data transmission nodes encrypt their data before forwarding it and ECC algorithm is used for encryption and decryption purpose. Each time when aggregated data is sent to processing station it is verified by its cluster attribute by "Relay Cluster Head (RCH)". If the cluster head is detected as malicious it is hence discarded and further operations of that cluster are conducted by respective RCH.***

Keywords: Wireless Sensor Networks (WSN), Clustering, Relay cluster heads (RCH), Key Generation Centers(KGC), Elliptical Curve Cryptography (ECC) , Certificateless Partial Key Generation

1. Introduction to WSEECM

With the advancement of technology there is an increase in data generation, hence, this data need to be securely and efficiently monitored. In a real time scenario, this data could be as critical as medical analysis of a heart patient or a military survey. In such scenario sensing devices have played a major role but sensor nodes are restricted to their processing and battery capabilities. Hence to prolong useful their network lifetime by decreasing "wasteful" energy drainage and balancing "useful" energy drainage where network lifetime is the time elapsed till the energy depletion of anyone of the network node. Clustering is one method with which we can do load balancing, scaling, better monitoring and efficient use of energy of these sensor nodes.

Clustering is one method with which we can do load balancing, scaling, better monitoring and efficient use of energy of these sensor nodes. In clustering, we logically bind and group sensing nodes on different criteria. Hence, we need to wisely utilize the energy of the network nodes, therefore, increase their uptime. While sensor nodes collect and directly transmit the same to the central location called "base station" which process data .It is preferable to use a single node at each cluster to collect, compress, filter and verify data and then transmit it further, as a result, it reduces bandwidth usage and increases processing capabilities this node is called "cluster head(CH)". A Number of ways exist by which we can prolong the network lifetime, by reducing participating nodes for channel access, aggregating data at cluster head and through accessing a small diameter cluster head while routing [11]. If the clustering algorithm is not appropriate may cause the node to be isolated from cluster head which communicates to sink node and waste energy in such situation average of regional energy and distance of nodes from sink can be used to decide whether the node should communicate to sink or cluster head [12].

Security of data and authentication of a node is another major concern while data transmission in WSN. Through multi-hop data is forwarded to destination meanwhile traversing it can be attacked by an intruder, nodes may be cloned, Denied of services or any mischief may happen and hence data can be compromised. One solution is to use asymmetric encryption method such as ECC for secure transmission. Elliptical curve cryptography 160 point multiplication performs an equal operation as RSA-1024 bit private key [13]. Such encryption techniques are based on efficient key generation and distribution schemes. To access the information, a node should be authorized and should have access to its pair of public and private key to encrypt and decrypt the data, this key and information must be inaccessible to the compromised nodes. These keys should be updated to maintain security and resilience from attacks. In Public key infrastructure (PKI) scenario there exist many distributed certificate authority (CA) issues, revoke and authorize certificates. In some cases, these CA or the data stored may be compromised and controlled to force MITM attacks [15]. Certificate-less key management scheme eliminates the need of CA and generates keys partially with the help of key generation center and the full key pair is generated by the node [14]. An add-on benefit is achieved if the key management algorithm is secure and energy saving ,that means if the algorithm does not consume much resources and time with security to network ,as if fewer nodes are compromised less will be the key revocation process and the network will be more stable

We identify the challenging issues in previous work and proposed our new system to increase the network lifetime, security and reducing energy usage and data traffic. :

1. Limitation: Base station randomly assigns the cluster head in cluster formation process. It selects the cluster head on the basis of the residual energy of that node.

Solution: In proposed system, three parameters are taken into consideration for cluster head selection such as:

- Maximum residual energy
- Minimum distance of node to base station
- A maximum number of nodes in the transmission range of that node.

It will select the proper CH with maximum resource capacity.

2. Limitation: Cluster head is responsible for data collection, aggregation, and transmission it to the base station. Sometime CH is hacked by an attacker. When the base station detects the malicious cluster head, it does not receive the data from that node. This is the case of energy wastage and data loss. This data might be very important for further analysis for end users.

Solution: To overcome this problem, in our system we are introducing a Relay Cluster Head (RCH) node. The base station assigns the RCH for a particular group of clusters on the basis of its geographical locations. This RCH is activated when any one of CH is deactivated by base station due to attack. Then all operations of that malicious CH perform by this RCH and avoiding the data loss.

3. Limitation: The existing system uses only one Key Generation Center (KGC) which might raise the key escrow problem. That is one KGC held the keys of all nodes, and this KGC might be accessed by third party unauthorized entities. That will break the security of data transmitted by all nodes.

Solution: To avoid this, we introduce multiple KGC scheme in our system. The number of keys is randomly generated at KGC and these keys are distributed to all CHs through RCH. Because of this nobody knows the exact destination of the key generation process. This will increase the security of transmitted data.

So main aim is to propose a system that provides the maximum security over data transmission, reduce the network traffic, data loss reduction, save maximum energy and finally increase the lifetime of the network.

Further fragment II discusses study related to clustering techniques with methods of selecting cluster head and various key management schemes; fragment III describes working of WSEECM

2. Literature Survey

Cluster head selection, as well as clustering, is performed by considering weight assigned to all sensor nodes within the Multi Weight Based Clustering Algorithm (MWBCA) that is also an expanded LEACH [1]. Identity depended on Digital Signature is utilized to provide security. SNR-based dynamic clustering [2] divides the nodes into clusters and choose cluster head between nodes by determining the energy of nodes and remaining nodes are associated with a particular cluster head on the basis of the signal to noise ratio (SNR) values. End-to-end error recovery prevented through error recovery is utilized between the inter-cluster routing. Sink-based routing pattern analysis is implemented to obtain security by separating the malicious nodes. [4] In the process of TDKM both pair-wise key as well as group key are shared within three rounds for the key material trade off without encryption/decryption and exponentiation operations. [6] Cluster head selection algorithm by a deterministic component and select cluster head by specific probability [11]. It stops in O(1) time and criteria for CH selection are residual energy and communication cost with selection probability [7]. A heterogeneous energy protocol mitigates the possibility of failure nodes as well as to enhance the time interval before the death of the initial node and enhancing the lifetime of heterogeneous WSNs that is critical for several applications. [8] The Proposed algorithm is energy efficient. It is a trusted clustering algorithm, which is used to protect the WSN from various types of malicious nodes activities. With TREE-CR, the author also proposed a realistic energy consumption model. This model can accurately predict the lifetime of network and identify malicious nodes. Routing algorithm [9], which is based on game theory and reducing the energy consumption. According to this approach, the cluster head nodes supporting to data transmission instead of cooperative selection for sending and receiving groups in each cluster. Game theory selects the cluster heads on the basis of sufficient residual energy and high trust level criteria. [10] This algorithm is useful for efficient selection of cluster head. The system makes use of a new Synchronous transit algorithm. It is used for uniformity of CHs to balance clusters, RMCHS uses.

3. Implementation Details of WSEECM

This section discusses the proposed system in detail, which includes system overview, proposed algorithm, mathematical model of WSEECM,

3.1 Summarized Workflow

The architecture of WSEECM is shown in fig 1. The system consists of a number of stationary wireless sensor nodes with limited energy and resources, It consist of three dynamic base stations (BS) and a random number decides which BS will be active, these BS talks on the heartbeat. Partial Key Generating Centre (PKGC) sits at BS and generates partial/private key pairs. Sensor nodes collect the data and sending to base station in a multi-hop manner. Initially, Base Station (BS) creates some parameters with the unique identifier and assign to all sensor nodes. After getting the public keys of all nodes, BS generate member list. This member list contains the nodes in the network along with their public key and identifiers. BS also assigns the individual key to all nodes. These keys are generated at multiple PKGC in a random way. For communication with neighboring nodes, each node broadcast the pair message along with its identifier and public key. This will allow the communication among two neighboring nodes. After successful network deployment, clustering is performed by a base station. It divides all nodes into a number of clusters and assigns the cluster head; here each cluster member including

CH possesses a unique attribute. CH sends data to BS through nearest RCH (Relay Cluster Head) which keeps a list of all attributes linked to each cluster which it uses to authenticate a data packet at first level. Only RHC knows which BS is active so that he can aggregate and forward data to correct BS. RCH is also responsible for key revocation.

Cluster head selection is based on three parameters such as Maximum residual energy, Minimum distance of a node to RCH, Maximum number of nodes in the transmission range of that node. Along with cluster head selection, BS also allocates Relay Cluster Head (RCH), it manages two or more CHs depend on the geographical location of CH.

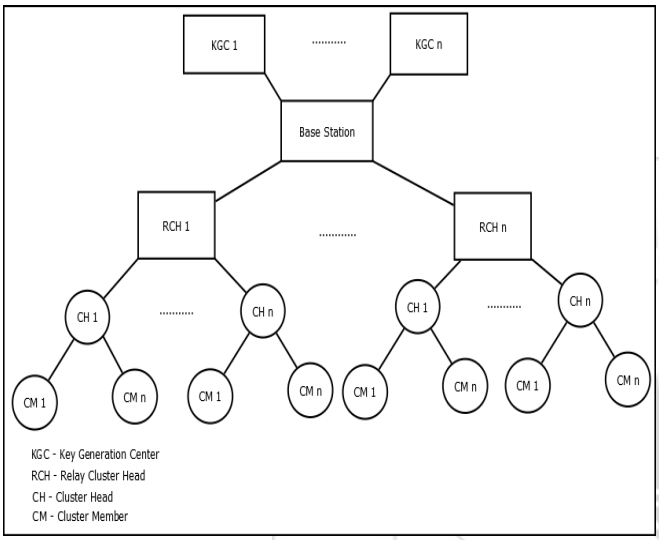

Figure 1: High-Level View of System modular Architecture

3.2 Detailed Workflow

The system is established in three phases. In the I phase initial parameters are determined. II phase clustering is performed and CH is chosen for each cluster in III phase keys are generated and IV phase key rejuvenate while cloning attack on node, backward/forward secrecy and cluster head compromise.

3.2.1 Prerequisite System Generated Parameters

At the time of system deployment eight major parameters list < C/F_s, s, G, Z_k, k, A, B>, Q_k is kept private are established those are:

- C/F_s: Elliptical Curve function on field F_s $y^2 = x^3 + ax + b \bmod s$.
- s: It is an *m* bit prime number .
- G: Elliptical curve point generator.
- Q_k: Master Private Key of multiple PKGC.
- Z_k: Public key of multiple PKGC, generated as $Z_k = Q_k G$.
- k: Multiple PKGC .
- A: List of all existing nodes registered excluding RCH, where a_i nodes within a cluster c_j.; i = 0,1… A, j = 0, 1… C. Let C be the total number of clusters in the network.
- B: List of registered RCH.

3.2.2 Clustering and Cluster Head Selection

In this clustering based system the ‚a_i" nodes within the same geographical location shares same cluster c_i and a unique attribute Att_t. Amongst the cluster members cluster head CH_i is selected which aggregates and encrypt the data with unique cluster attribute Att_t and forward it to the base station through nearest RCH with unique identity number as ID_r. So to balance the network lifetime we are selecting a CH in each round based on following three factors:

1. Maximum residual energy

To expand the lifetime of the system as well as to transmit data to base station uninterrupted and to balance the load of energy dissipation we must select the CH having the maximum residual energy among the cluster members .While transferring and receiving the data, nodes utilize some amount of energy based on the data length and the distance between two nodes.

Energy consumption of radio dissipation of sending data and receiving data are both expressed as E_m; the free space (a^2 power loss) and the multi-path fading (a^4 power loss) channel models with amplifying index ϵ_{fs} and ϵ_{amp} are used respectively; the energy consumption of data fusion is denoted by EDA.

The energy spent of a node that transmits single bits packet over distance ‚a" is:

$$E_{Trans}(l,a) = E_{Trans-elec}(l) + E_{Trans-amp}(l,a) = \begin{cases} E_m * l + \epsilon_{fs}\, a^2 * l & a < a_0 \\ E_m * l + \epsilon_{fs} + \epsilon_{amp}\, a^4 * l & a \geq a_0 \end{cases} \quad (1)$$

Where, $a_0 = \sqrt{\frac{\epsilon_{fs}}{\epsilon_{amp}}}$, and the energy consumption of receiving this message is:

$$E_{Rec}(l) = E_m * l \quad (2)$$

2. Minimum distance of node to base station

To reduce the energy consumption the distance between the CH and RCH should be as minimum as possible. We are introducing RCH at the second level which increases one hop at the cost of increasing reach-ability to BS.

$$Distance\ between\ node\ and\ RCH = \sqrt{\sum_{i=1}^{n} (X_i - Y_i)^2}$$

Where X_i, Y_i are the coordinates on x and y-axis for each node to RCH

3. Maximum number of nodes in the transmission range of that node

The number of nearest nodes to the cluster head must be as possible as it can so the cluster head can collect the data from the all the members of the cluster.

The node will be selected as a cluster head if it has max value CHN_{max} which is calculated as

$$CHN_{max} = \frac{residual\ energy \times dense\ node\ under\ range}{distance\ of\ node\ to\ base\ station}$$

3.2.3 Key generation and Distribution:

Next step of node registration is to generate pair of public / private key- Global key, and then generation of individual-BS key and lastly cluster-member key, each of which is generated with the help of PKGC as follows:

1) Public/Private-Global Key – This key is global and generally used to encrypt data while communication .At the time of initialization of network ,each member node a_i choose a random secret number „h" ,where h is an integer then compute P_i = h G. Then PKGC generates the partial key pair of a_i with input parameters i, and P_i. Then again a random secret number "k" is selected for further computation which is as bellow . Full Public Key is generated at KGC and published :
   a) P_{ppub} = k G
   b) P_{ppri} = k + Q_k . L_0(i, P_{ppub},P_i) mod s ,
   c) where L_0 is cryptographic hash function
   d) FP_{pub} = (P_i,P_{ppub})
   e) Next < FP_{pub} , P_{ppri} > is send to node where it generate full private key as FP_{priv} =(h,P_{ppri}).
2) Individual Key-BS – This key pair is used to communicate individually to BS and RCH <IB_{pub},IB_{priv}>are generated in a similar way as above except that the PKGC also takes Att_t attribute of the individual node as input in L_0.

3) Cluster-Member Key – This key is used within cluster member communication and generated after cluster formation. This key is also generated as similar to Public/Private –Global key pair <CM_{pri},CP_{pub}>

3.2.4 Key Rejuvenate

Rejuvenation of keys will be done by RCH under bellow circumstances

1. Cloning Attack: If a malignant create clones of a network node and try to send data to the BS. The data send to CH will lack in cluster attribute is which will be identified at the RCH and hence the cloned nodes will not be allowed to send data further.
2. Backward/Forward Secrecy: Whenever a node move to and froth in a cluster it should hide details from the previous cluster and similarly the previous keys should be updated.
3. Cluster Head Compromise: If RCH identifies CH has being compromised it will ask all the nodes connected to CH to directly connect to RCH or give an alternate path for data transfer , till it assigns a new CH and update the keys.

3.3 Experimental Setup

The system is developed using Java framework-version JDK 8 on Windows platform. The NetBeans version 8.1 is used as a development tool. Jung tool is used for the generating the network which contains sensor nodes. The system does not require particular hardware to run; any standard machine is capable of running the application.

4. Results and Discussion

Fig. 2 demonstrates the energy comparison between existing and WSEECM. Comparison results show the WSEECM is less energy consuming which we calculate in joules, hence the clustering algorithm and key management algorithm both efficiently save resources as compared to existing system. The existing system is implements random cluster head selection while clustering.

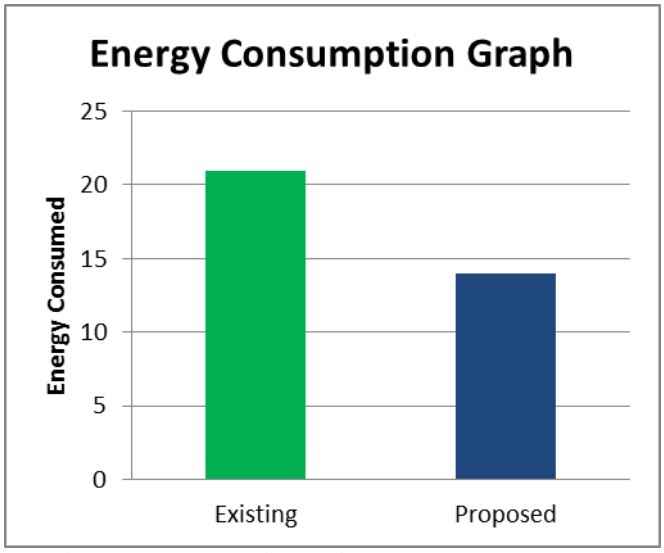

Fig. 2 Energy Consumption Graph

Fig. 3 demonstrates the comparison between existing and WSEECM on the basis of time consumption. Comparison results show that the WSEECM is executes fast .

Fig.4 demonstrates the network lifetime comparison graph between existing and proposed system. Comparison results show the network lifetime of WSEECM is increased as compared with the existing system.

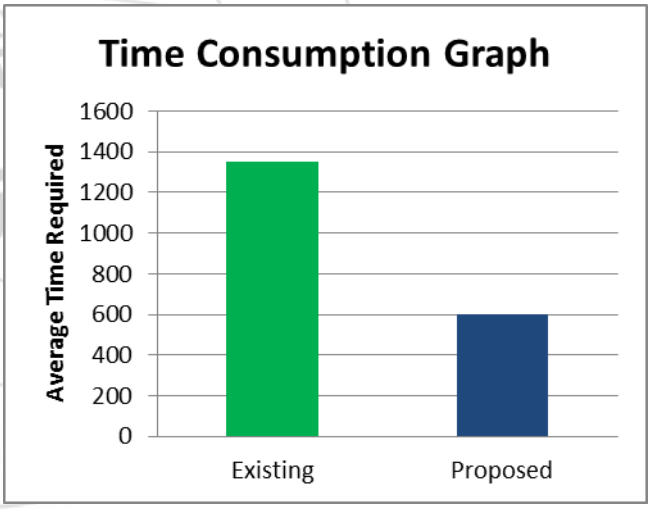

Figure 3: Time Consumption Graph

5. Conclusion and Future Scope

In this paper, we introduced three parameters for selecting cluster head during clustering procedure. It accurately and efficiently selects the CH with maximum resource saving. To reduce the data loss, we have introduced a relay cluster heads. If the CHs are attacked by attacker RCH is responsible for data collection, aggregation, and routing of that cluster. RCH also increase the data transmission efficiency. Instead of using single KGC, we have used multiple randomly activated KGC.

In future, energy aware routing will be introduced by calculating shortest path from each sensor to the base station in wireless sensor network with a mathematical model for the system will be introduced.

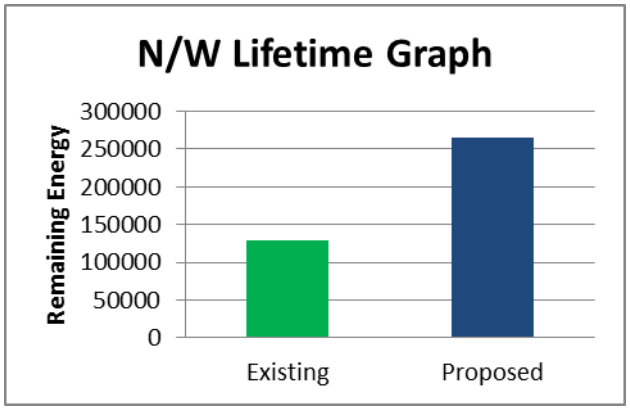

Figure 4: Network Lifetime Graph

References

[1] Roshani R. Patle, Prof. Rachana Satao, "Aggregated Identity-Based Signature To Transmit Data Securely and Efficiently in Clustered WSNs", 2015 International Conference on Computing Communication Control and Automation.

[2] Subramanian Ganesh and Ramachandran Amutha, "Efficient and Secure Routing Protocol forWireless Sensor Networks through SNR Based Dynamic Clustering Mechanisms", JOURNAL OF COMMUNICATIONS AND NETWORKS, VOL. 15, NO. 4, AUGUST 2013

[3] Kemal Akkaya ,Mohamed Younis ,"A survey on routing protocol for wireless sensor networks", Science Direct ad-hoc network 3 ,(2005) 325-349

[4] I-Hsun Chuang, Wei-Tsung Su, Chun-Yi Wu, Jang-Pong Hsu, Yau-Hwang Kuo, "Two-layered Dynamic Key Management in Mobile and Long-lived Cluster-based Wireless Sensor Networks", 1525-3511/07/$25.00 ©2007 IEEE

[5] Hu Xiong ,"Cost-Effective Scalable and Anonymous Certificateless Remote authentication Protocol " , IEEE transaction on information forensics security , jan 2007.

[6] M. J. Handy, M. Haase, D. Timmermann, "Low Energy Adaptive Clustering Hierarchy with Deterministic Cluster-Head Selection", 2002 IEEE.

[7] EZZATI ABDELLAH, SAID BENALLA, Abderrahim BENI HSSANE, MoulayLahcen HASNAOUI, "Advanced Low Energy Adaptive Clustering Hierarchy", EzzatiAbdellah et al. / (IJCSE) International Journal on Computer Science and Engineering Vol. 02, No. 07, 2010, 2491-2497.

[8] R. R. Sahoo, M. Singh, A. R. Sardar, S. Mohapatra and S. K. Sarkar, "TREE-CR: Trust based secure and energy efficient clustering in WSN," International Conference onEmerging Trends in Computing, Communication and Nanotechnology (ICE-CCN), Tirunelveli, 2013, pp. 532-538.

[9] D. Sathian, R. Baskaran and P. Dhavachelvan, "Lifetime enhancement by Cluster Head Cooperative Trustworthy Energy Efficient MIMO routing algorithm based on game theory for WSN," Third International Conference on Computing Communication & Networking Technologies (ICCCNT), Coimbatore, 2012, pp. 1-5.

[10] K. A. Prasath and T. Shankar, "RMCHS: Ridge method based cluster head selection for energy efficient clustering hierarchy protocol in WSN," International Conference on Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials (ICSTM), Chennai, 2015.

[11] Ossama Younis and Sonia Fahmy," HEED:A Hybrid, Energy-Efficient, Distributed Clustering Approach for Ad Hoc Sensor Networks", , Published by the IEEE CS, CASS, ComSoc, IES, & SPS,VOL 3, NO. 4 ,Oct-Dec 2004.

[12] Jeng-shiou and Tung-Hung ,"Energy Efficient Clustering Scheme for Prolonging the Lifetime of Wireless Sensor Network with Isolated Nodes",IEEE communications Letter Vol. 19,No.2,Feb 2015.

[13] N. Gura, A. Patel, A. Wander, H. Eberle, and S. C. Shantz, "Comparing elliptic curve cryptography and RSA on 8-bit CPUs," in Proc. 6th Int. Workshop Cryptograph. Hardw. Embedded Syst., 2004, pp. 119–132.

[14] Seung-Hyun Seo, Member, IEEE, Jongho Won, Student Member, IEEE, Salmin Sultana, Member, IEEE, and Elisa Bertino, Fellow, IEEE, "Effective Key Management in Dynamic Wireless Sensor Networks", in IEEE Transaction on Information Forensic and Security, Vol. 10, NO. 2, Feb 2015.

[15] Rolf Oppliger, "Certification Authorities under Attacks:A Plea for Certificate Legitimation", IEEE Internet Computing nov. 2012.

Author Profile

Ruchika Jain received the B.Tech. degrees in Computer Engineering from Rajasthan University in 2013.Presently pursuing M.E in Computer Engineering from Savitribai Phule University