Secured Energy-Efficient Clustering Mechanism (SEECM) Using Firefly Algorithm in Wireless Sensor Networks

E.Velumani, Dr.T.Kannaian

Abstract— **The sensor nodes deployed in wireless sensor networks are extremely power constrained, so maximizing the lifetime of the entire networks is mainly considered in the design. An energy efficient clustering algorithm with optimum parameters is designed for reducing the energy consumption and prolonging the system lifetime. Here we approach an Energy Efficient Clustering Mechanism (SEECM) with Firefly algorithm and also present a Cluster key Management for secure transmission in WSN. A Firefly Algorithm (FA) is a recent nature inspired optimization algorithm that simulates the flash pattern and characteristics of fireflies. Clustering is a popular data analysis technique to identify homogeneous groups of objects based on the values of their attributes. Firefly algorithm is a swarm based algorithm that used for solving optimization problems. This paper presents a new approach using firefly algorithm to cluster data. This paper also shows the use of firefly algorithm to find the centroid of the user specified number of clusters. We use the firefly algorithm to find initial optimal cluster centroid and then optimized centroid to refined them and improve clustering accuracy. And we propose an efficient Cluster key management (CKM) scheme for secure communication in dynamic WSNs characterized by node mobility. The CKM supports efficient key updates when a node leaves or joins a cluster and ensures forward and backward key secrecy. The protocol also supports efficient key revocation for compromised nodes and minimizes the impact of a node compromise on the security of other communication links. A security analysis of our scheme shows that our protocol is effective in defending against various attacks. Simulation results validate that the proposed FA significantly outperforms the clustering mechanisms using random selection and by considering only link quality, security and residual energy in the packet delivery ratio, energy consumption, and delivery latency.**

Index Terms— **Clustering, energy efficient, Firefly algorithm, cluster key management, routing, wireless sensor network.**

I. INTRODUCTION

In most wireless sensor network (WSN) applications nowadays the entire network must have the ability to operate unattended in harsh environments in which pure human access and monitoring cannot be easily scheduled or efficiently managed or it's even not feasible at all [1]. Based on this critical expectation, in many significant WSN applications the sensor nodes are often deployed randomly in the area of interest by relatively uncontrolled means (i.e., dropped by a helicopter) and they form a network in an ad hoc manner [2,3]. Moreover, considering the entire area that has to be covered, the short duration of the battery energy of the sensors and the possibility of having
damaged nodes during deployment, large populations of sensors are expected; It is a natural possibility that hundreds or even thousands of sensor nodes will be involved. In addition, sensors in such environments are energy constrained and their batteries usually cannot be recharged. Therefore, it is obvious that specialized energy-aware routing and data gathering protocols offer high scalability should be applied in order that network lifetime is preserved acceptably high in such environments.
Naturally, grouping sensor nodes into clusters has been widely adopted by the research community to satisfy the above scalability
objective and generally achieve high energy efficiency and prolong network lifetime in large-scale WSN environments. The corresponding hierarchical routing and data gathering protocols imply cluster-based organization of the sensor nodes in order that data fusion and aggregation are possible, thus leading to significant energy savings.

In the hierarchical network structure each cluster has a leader, which is also called the cluster head (CH) and usually performs the eventually leads to a two-level hierarchy where the CH nodes form the higher level and the cluster-member nodes form the lower level. The sensor nodes periodically transmit their data to the corresponding CH nodes. Sensor Networks Clustering in Wireless Sensor Networks 325 CH nodes aggregate the data (thus decreasing the total number of relayed packets) and transmit them to the base station (BS) either directly or through the intermediate communication with other CH nodes. However, because the CH nodes send all the time data to higher distances than the common (member) nodes, they naturally spend energy at higher rates. A common solution in order to balance the energy consumption among all the network nodes, is to periodically re-elect new CHs (thus rotating the CH role among all the nodes over time) in each cluster. The BS is the data processing point for the data received from the sensor nodes, and where the data is accessed by the end user. It is generally considered fixed and at a far distance from the sensor nodes. The CH nodes actually act as gateways between the sensor nodes and the BS. The function of each CH, as already mentioned, is to perform common functions for all the nodes in the cluster, like aggregating the data before sending it to the

Manuscript received Jan 06, 2017
E.Velumani, Associate Professor, Department Of Electronics, Psg College Of Arts And Science, Tamilnadu – India
Dr.T.Kannaian, Associate Professor, Department Of Electronics, Psg College Of Arts And Science, Tamilnadu – India

BS. In some way, the CH is the sink for the cluster nodes, and the BS is the sink for the CHs. Moreover, this structure formed between the sensor nodes, the sink (CH), and the BS can be replicated as many times as it is needed, creating (if desired) multiple layers of the hierarchical WSN (multi-level cluster hierarchy).

However, sensor devices are vulnerable to malicious attacks such as impersonation, interception, capture or physical destruction, due

to their unattended operative environments and lapses of connectivity in wireless communication [4, 5, 6]. Thus, security is one of the most important issues in many critical dynamic WSN applications. Dynamic WSNs thus needs address key security requirements, such as node authentication, data confidentiality and integrity, whenever and wherever the nodes move. To address security, encryption key management protocols for dynamic WSNs have been proposed in the past based on symmetric key encryption. Such type of encryption is well-suited for sensor nodes because of their limited energy and processing capability. However, it suffers from high communication overhead and requires large memory space to store shared pairwise keys. It is also not scalable and not resilient against compromises, and unable to support node mobility. Therefore symmetric key encryption is not suitable for dynamic WSNs. More recently, asymmetric key based approaches have been proposed for dynamic WSNs.

This study, motivated by the link aware clustering technique, proposes an Secured Energy Efficient Clustering Mechanism (SEECM) to support energy-efficient routing in WSNs. The main goal of the SEECM is to establish a persistent and reliable routing path by determining proper nodes to become cluster heads and gateways. In the SEECM, cluster head and gateway candidates use the node status and link condition to determine a clustering metric, called the Firefly. [7][11] The Firefly algorithm is defined as the number of transmissions that cluster head and gateway candidates conducts. This metric can be determined by measuring the transmit power consumption, residual energy, and link quality. The cluster head or gateway candidate depends on a priority, derived from its predicted transmission count, to evaluate its qualification for a cluster head or a gateway. The Cluster head or gateway candidate having the highest priority is elected as a cluster head or a gateway, respectively. To our best knowledge, this study is the first to investigate the routing issue based on the Firefly technique in WSNs. The main contribution of this work is that it proposes a secured energy efficient clustering mechanism, and We propose the key management scheme for dynamic WSNs. It supports four types of keys, each of which is used for a different purpose, including secure pair-wise node communication and group-oriented key communication within clusters. Efficient key management procedures are defined as supporting node movements across different clusters and key revocation process for compromised nodes. Simulation results validate that the proposed FA significantly outperforms the clustering mechanisms using random selection and by considering energy. Simulation results confirm that the SEECM can achieve a high packet delivery ratio, extend the network lifetime, and reduce transmission latency because the proposed FA can reflect the energy usage of nodes and the quality of wireless links. And give more secure transmission by using key management process.

The rest of this paper is organized as follows. Section II introduces the representative traditional passive clustering technique and the link aware clustering mechanism (LCM). Section III describes the network model and assumptions. Section IV presents the proposed SEECM in detail. Section V shows the performance evaluation results, and finally, Section VI provides concluding remarks.

II. PRELIMINARIES

This section describes the concept of passive clustering technique and link aware clustering mechanism (LCM).

A. Passive clustering (PC) technique

Previous researches have proposed many cluster head election approaches for constructing clusters [3], [8], [10], [11]. Each node in these approaches locally exchanges messages with the nodes in its communication range to determine whether it should become a cluster head. A majority of previous work has focused on active clustering techniques, but Kwon and Gerla proposed a passive clustering (PC) technique for construction of a cluster structure [12]. By using on-going data packets instead of extra explicit control packets, the PC can reduce the control overhead during constructing and maintaining

clusters. The PC technique uses five external states to represent a node's role in a cluster, and each node possesses an external state. The external states include initial (IN), ordinary (OD), cluster head (CH), gateway (GW), and distributed gateway (D_GW). The PC technique also introduces two internal states, cluster head ready (CH_R) and gateway ready (GW_R), to represent the tentative role of a node. When a node in the external state receives data packets, it may change its current state. A node in the internal state must enter the external state when it sends out a data packet. For the lack of space, the rules of state transition in the PC technique can be obtained in [12]. The PC technique proposes two innovative mechanisms: First Declaration Wins mechanism and Gateway Selection Heuristic mechanism, which are used to determine CH and GW nodes. In the First Declaration Wins mechanism, the CH candidate (i.e., CH_R) uses a contention strategy to declare that it wants to become a CH node. That is, the CH candidate first claiming to become a CH node within the communication range will successfully become a CH node. The Gateway Selection Heuristic mechanism determines the minimal number of GW nodes to guarantee that a single cluster has at least two GW nodes to maintain network connectivity. In PC, CH and GW nodes dominate the energy usage because they are the main participants in data transmission. The PC technique uses a random selection strategy to determine CH and GW nodes. Although this is an effortless approach, it is not an efficient approach because it does not consider the node status and link condition in clustering, and it is more likely to result in a disappointing routing performance.

B. Link aware clustering mechanism (LCM).

A link-aware clustering mechanism, called LCM, to determine an energy-efficient and reliable routing path.[1] The LCM primarily considers node status and link condition, and uses a novel clustering metric called the predicted transmission count (PTX), to evaluate the qualification of nodes for cluster heads and gateways to construct clusters.

Each cluster head or gateway candidate depends on the PTX to derive its priority, and the candidate with thehighest priority becomes the cluster head or gateway. In the LCM, cluster head and gateway candidates use the node status (e.g., residual energy) and link condition (e.g., quality) to determine a clustering metric, called the predicted transmission count. The predicted transmission count is defined as the number of transmissions that cluster head and gateway candidates conducts. This metric can be determined by measuring the transmit power consumption, residual energy, and link quality. The previous predicted transmission count and the procedure of priority calculation in the technique LCM, followed by an example of LCM operation.

C. Predicted Transmission Count

Although random selection is an effortless strategy to determine CH and GW nodes, it is not an efficient approach because of its disregard of node status and link condition.[1] Moreover, using only a single factor cannot expose the influence of other factors on routing performance. The proposed LCM considers node status and link condition, and proposes a novel metric, called the predicted transmission count (PTX), to evaluate the suitability of CH or GW candidates. The PTX represents the capability of a candidate for persistent transmission to a specific neighboring node. This study considers the transmit power, residual energy, and link quality to derive the PTX of CH or GW candidate. A large PTX value indicates a high likelihood of becoming a CH or GW node. Because the channel condition of wireless links varies with time, the link reliability often depends on the channel condition. If a node is associated with an unreliable link, data delivery is likely to fail, thereby leading to packet retransmissions. Thus, the candidate associated with a stable link is preferred to be selected as a CH node or a GW node. Previous research usually uses the expected transmission count, called ETX, to evaluate the level of link quality.

III. PROPOSED WORK

In many existing system scheme, process is not suitable for multiple target coverage in wireless sensor networks. We plan to extend this method of scheduling for probabilistic coverage in wireless sensor networks. We want to improve network lifetime compared to this process. We proposed an Secured Energy Efficient Clustering Mechanism (SEECM) with Firefly algorithm. And also present a Cluster key Management for secure transmission in WSN. A Firefly Algorithm (FA) is a recent nature inspired optimization algorithm that simulates the flash pattern and characteristics of fireflies. Clustering is a popular data analysis technique to identify homogeneous groups of objects based on the values of their attributes. Firefly algorithm is a swarm based algorithm that used for solving optimization problems. This paper presents a new approach using firefly algorithm to cluster data. It is shown how firefly algorithm can be used to find the centroid of the user specified number of clusters. [9][15] We use the firefly algorithm to find initial optimal cluster centroid and then optimized centroid to refined them and improve clustering accuracy. And we propose an efficient Cluster key management (CKM) scheme for secure communication in dynamic WSNs characterized by node mobility. The CKM supports efficient key updates when a node leaves or joins a cluster and ensures forward and backward key secrecy [13, 14]. The protocol also supports efficient key revocation for compromised nodes and minimizes the impact of a node compromise on the security of other communication links. A security analysis of our scheme shows that our protocol is effective in defending against various attacks.

A. Firefly Algorithm (FA)

The FA process:

- In this work, we use firefly algorithm, A Firefly Algorithm (FA) is a recent nature inspired optimization algorithm that simulates the flash pattern and characteristics of fireflies.
- Clustering is a popular data analysis technique to identify homogeneous groups of objects based on the values of their attributes.
- Firefly algorithm is a swarm based algorithm that use for solving
- optimization problems. This paper presents a new approach to using firefly algorithm to cluster data. It is shown how firefly algorithm can be used to find the centroid of the user specified number of clusters.
- We use the firefly algorithm to find initial optimal cluster centroid and then optimized centroid to refined them and improve clustering accuracy.
- Easy and efficient implementation, Easy to understand and Parallel implementation. This method helps to prolong the network lifetime.

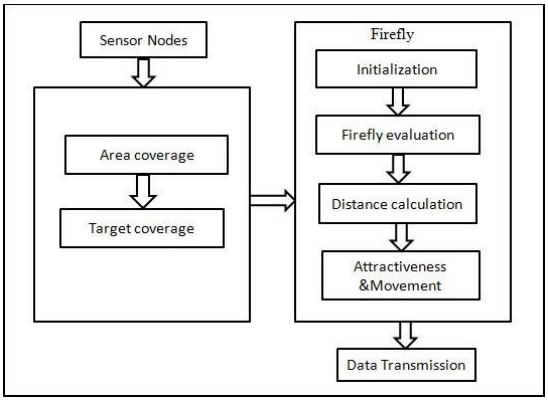


Fig.1: firefly algorithm architecture

1. Initialization

The first step in the algorithm is the initialization of the population of N fireflies where each firefly represents a candidate solution. Population size (N) represents the number of solutions or the size of the search space. An objective function is associated with the brightness of the firefly and is directly proportional to the brightness. The aim is to maximize the objective function value.

2. Firefly evaluation

- Firefly algorithm is based upon idealizing the flashing characteristic of fireflies. The idealized three rules are:-
- All fireflies are considered as unisex and irrespective of the sex one firefly is attracted to other fireflies.
- The Attractiveness is proportional to their brightness, which means for any two flashing fireflies, the

movement of firefly is from less bright towards the brighter one and if no one is brighter than other it will move randomly. Furthermore they both decrease as their distance increases.

- The landscape of the objective function directly affects the brightness of the firefly.

3. Distance calculation

The distance between any two fireflies i and j at xi and xj respectively, the Cartesian distance is determined by equation where xi, k is the k th component of the spatial coordinate xi of the i th firefly and d is the number of dimensions.

$$d_{i,j} = \text{Distance}(\mathbf{x}^i, \mathbf{x}^j) = \sqrt{\sum_{k=1}^{n} (x_k^i - x_k^j)^2}$$

4. Attractiveness

In the Firefly algorithm, there are two important issues: the variation of the light intensity and the formulation of the attractiveness. We know, the light intensity varies according to the inverse square law.

Suppose it is absolute darkness.

Light intensity of each firefly is proportional to quality of solution.

Each firefly needs to move towards the brighter fireflies.

Light intensity reduction abides the law:

(_0,)= _0/ ^2

_0 is the light intensity at zero distanced

d is the observer's distance from source

If we take absorption coefficient "ɣ" into account:

Attractiveness (_0, , "ɣ") = _0 ^(−"ɣ" ^2)

= 2 (1)

Where I(r) is the light intensity at a distance r and Isis the intensity at the source.

When the medium is given the light intensity can be determined as follows:

= 0 − (2)

To avoid the singularity at r=0 in (1), the equations can be approximated in the following Gaussian form:

= 0 − 2 (3)

As we know, that a firefly's attractiveness is proportional to the light intensity seen by adjacent fireflies and thus the attractiveness β of a firefly is determined by equation (4) where β0 is the attractiveness

At r=0. = 0 –(m≥1) (4)

5. Movement

The movement of a firefly i is attracted to another more attractive (brighter) firefly j is determined by

= + 0 − 2 − + *E*

Movement consist two elements

- Approach to better solutions
- Move randomly

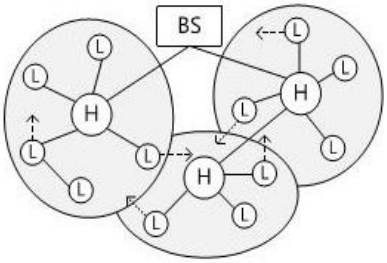
Pseudo code for Firefly Algorithm

1. Objective function of f(x),
2. Generate initial population of fireflies;
3. Formulate light intensity I;
4. Define absorption coefficient γ;
5. While (t Ii), move firefly i towards j;
6. For i = 1 to n (all n fireflies);
7. For j=1 to n (all n fireflies)
8. If (Ij> Ii), move firefly i towards j;
9. end if
10. Evaluate new solutions and update light intensity;
11. End for j;
12. End for i;
13. Rank the fireflies and find the current best;
14. End while;
15. Post process results and visualization;
16. End procedure

B. Key Management

We consider a dynamic wireless sensor network (See Fig. 2). The network consists of a number of stationary or mobile sensor nodes and a BS that manages the network and collects data from the sensors. Sensor nodes can be of two types: (i) nodes with high processing capabilities, referred to as H-sensors, and (ii) nodes with low processing capabilities, referred to as L-sensors. Nodes may join and leave the network, and thus the network size may dynamically change. The H-sensors act as cluster heads while L-sensors act as cluster members. They are connected to the BS directly or by a multi-hop path through other H-sensors. H-sensors and L-sensors can be stationary or mobile. After the network deployment, each H-sensor forms a cluster by discovering the neighboring L-sensors through beacon message exchanges. The L-sensors can join a cluster, move to other clusters and also re-join the previous clusters. To maintain the updated list of neighbors and connectivity, the nodes in a cluster periodically exchange very lightweight beacon messages. The H-sensors report any changes in their clusters to the BS, for example, when a L-sensor leaves or joins the cluster. The BS creates a list of legitimate nodes, M,

and updates the status of the nodes when an anomaly node or node failure is detected. The BS assigns each node a unique identifier. A L-sensor nLi is uniquely identified by node IDLi whereas a H-sensor nHj is assigned a node ID Hj. A Key Generation Center (KGC), hosted at the BS, generates public system parameters used for key management by the BS and issues certificateless public/private key pairs for each node in the network. In our key management system, a unique individual key, shared only
between the node and the BS is assigned to each node. The certificateless public/private key of a node is used to establish pairwise keys between any two nodes. A cluster key is shared among the nodes in a cluster.



In this section, we propose a Cluster Key Management scheme (CKM) that supports the establishment of four types of keys, namely: a certificateless public/private key pair, an individual key, a pairwise key, and a cluster key. This scheme also utilizes the main algorithms of the CKM scheme in deriving certificateless public/private keys and pairwise keys.

Types of Keys
Certificateless Public/Private Key: Before a node is deployed, the KGC at the BS generates a unique certificateless private/public key pair and installs the keys in the node. This key pair is used to generate a mutually authenticated pairwise key.
Individual Node Key: Each node shares a unique individual key with BS. For example, a L-sensor can use the individual key to encrypt an alert message sent to the BS, or if it fails to communicate with the H-sensor. An H-sensor can use its individual key to encrypt the message corresponding to changes in the cluster. The BS can also use this key to encrypt any sensitive data, such as compromised node information or commands. Before a node is deployed, the BS assigns the node the individual key.

Pairwise Key: Each node shares a different pairwise key with each of its neighboring nodes for secure communications and authentication ofthese nodes. For example, in order to join a cluster, a L-sensor should share a pairwise key with the H-sensor. Then, the H-sensor can securely encrypt and distribute its cluster key to the L-sensor by using the pairwise key. In an aggregation supportive WSN, the L-sensor can use its pairwise key to securely transmit the sensed data to the H-sensor. Each node can dynamically establish the pairwise key between itself and another node using their respective certificateless public/private key pairs.

• Cluster Key: All nodes in a cluster share a key, named as cluster key. The cluster key is mainly used for securing broadcast messages in a cluster, e.g., sensitive commands or the change of member status in a cluster. Only the cluster head can update the cluster key when a L-sensor leaves or joins the cluster.

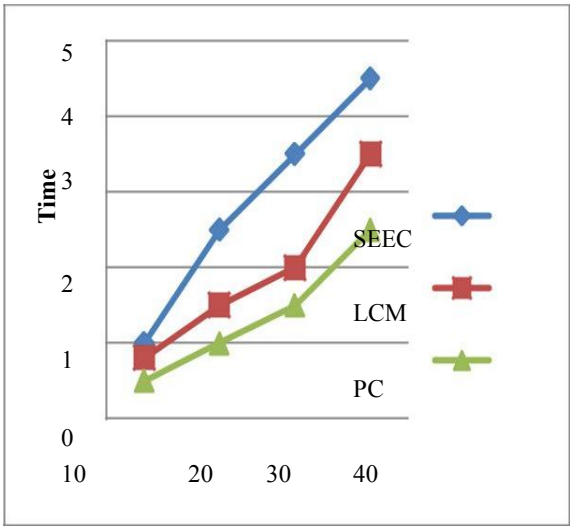
IV. EXPERIMENTAL RESULT AND DISCUSSION

This study used ns-2 as the network simulator and conducted numerous simulations to evaluate the FF performance. All sensor nodes are randomly scattered with a uniform distribution. Randomly select one of the deployed nodes as the source node. The location of the sink is randomly determined. This study evaluates the routing performance under scenarios with different numbers of sensor nodes.

This study evaluates the following main performance metrics:

1. Message delivery ratio: is the ratio of the number of report messages the sink receives to the total number of report messages the source node sends.
2. Residual energy: measures the mean value of the residual energy of all alive sensor nodes when simulation terminates.
3. Delivery latency: means the time delay experienced by the source node while transmitting a report message to the sink.

1) Message delivery ratio

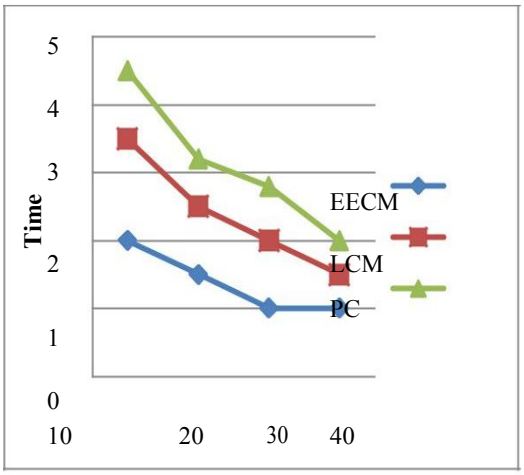


Above graph compares the simulation results of message delivery ratios of the original PC, LCM, and FF for different Nreq and NsThe message delivery ratios of the three mechanisms decreases, as Ns increases. Because increasing Ns increases the number of packets in the network, the probability of packet collisions also increases. Moreover, the message delivery ratio of the three mechanisms decreases as N req increases. In general, increasing Nreq is more likely to cause nodes along the constructed routing path to quickly exhaust their energy because of the increased frequency of message reports. In this case, the discovered routing path is broken, and the clustering mechanism must reconstruct the cluster structure. This reconstruction may lead to additional energy consumption of sensor nodes, thereby decreasing the packet delivery ratio.

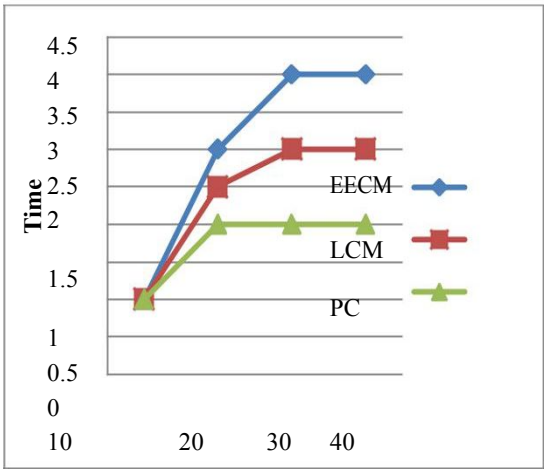
2) Residual Energy

Following graph shows a comparison of the energy consumption results of three clustering mechanisms under

scenarios with different Ns and Nreq. In general, the clustering mechanism generates more clusters as the number of Ns increases. Sensor nodes consume more energy in clustering, thereby decreasing the residual energy. Note that the increasing Nreq will increase the report frequency. Sensor nodes have to consume additional battery power to transmit the increased number of report messages. This leads to a reduction of the residual energy of the nodes in the network.



3) Delivery Latency:



Above graph shows the average delivery latency of the four clustering mechanisms under scenario with different N s and Nreq . As Ns increases, more clusters are generated and the length of the discovered routing path also increases. This leads to a long delivery latency, as illustrated in above Fig. In general, the nodes along the routing path are likely to exhaust their battery power quickly when Nreq increases. This may cause cluster reconstruction to determine a new path, thereby increasing the delivery latency. In clustering, node death and poor link quality result in reconstruction of clusters and retransmission of report messages, respectively. The reconstruction and retransmission generate a long message latency.

V. CONCLUSION

This paper has proposed framework SEECM with firefly algorithm, And Cluster key Management (CKM). A Firefly Algorithm (FA) is a recent nature inspired optimization algorithm that simulates the flash pattern and characteristics of fireflies. Clustering is a popular data analysis technique to identify homogeneous groups of objects based on the values of their attributes. Firefly algorithm is a swarm based algorithm that use for solving optimization problems. We use the firefly algorithm to find initial optimal cluster centroid and then optimized centroid to refined them and improve clustering accuracy. And we propose an efficient Cluster key management (CKM) scheme for secure communication in dynamic WSNs characterized by node mobility. The CKM supports efficient key updates when a node leaves or joins a cluster and ensures forward and backward key secrecy. The protocol also supports efficient key revocation for compromised nodes and minimizes the impact of a node compromise on the security of other communication links. A security analysis of our scheme shows that our protocol is effective in defending against various attacks. Simulation result confirm that Easy and efficient implementation, Easy to understand and Parallel implementation. This method helps to prolong the network life time. We achieve better link quality and residual energy in the packet delivery ratio. Less energy consumption and delivery latency. more Flexible, Highly accurate.

REFERENCES

[1] Sheng-Shih Wang,Member, IEEE, and Ze-Ping Chen "LCM: A Link-Aware Clustering Mechanism for Energy-Efficient Routing in Wireless Sensor Networks, 13, NO.2, Feb 2013,

[2] I.F. Akyildiz, W. Su, Y.Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," IEEE Commun. Mag., vol. 40, no. 8, pp. 102–114, Aug. 2002.

[3] C.-C. Chen and T.-K. Wu, "The survey of data aggregation techniques in wireless sensor networks: Current approaches and future directions,"in Proc. Int. Conf. Digit. Technol. Innov. Manage., 2006, pp. 1105–1126.

[4] M. Rahman and K. El-Khatib, "Private key agreement and secure communication for heterogeneous sensor networks,"J. Parallel Distrib. Comput., vol. 70, no. 8, pp. 858–870, 2010.

[5] M. R. Alagheband and M. R. Aref,"Dynamic and secure key management model for hierarchical heterogeneous sensor networks," IET Inf. Secur., vol. 6, no. 4, pp. 271–280, Dec. 2012.

[6] D. S. Sanchez and H. Baldus, "A deterministic pairwise key predistribution scheme for mobile sensor networks," inProc. 1st Int. Conf. SecureComm, Sep. 2005, pp. 277–288

[7] V.Kumar, S.Jain, S.Tiwarietal, "Energy Efficient Clustering Algorithms in WirelessSensor Networks: A survey," IJCSI InternationalJournal of Computer Science Issues, vol. 8, no. 5, pp. 1694–0814, 2011..

[8] S. Banerjee and S. Khuller, "A clustering scheme for hierarchical controlin multi-hop wireless networks," in Proc. Annu.Joint Conf. IEEEComput.Commun. Soc., Apr. 2001, pp. 1028–1037.

[9] Yang, X.S.: Firefly algorithm, stochastic test functions and design optimization. Int. J. BioInspired Comput. 2(2), 78–84 (2010).

[10] J. A. Torkestani and M. R. Meybodi,"LLACA: An adaptive localizedclustering algorithm for wireless ad hoc networks,"

[11] Comput. Electr. Eng.,vol. 37, no. 4, pp. 461– 474, Jul. 2011.

[12] Hashmi, N. Goel, S. Goel, and D. Gupta,"Firefly Algorithm for Unconstrained Optimization," IOSR Journal of ComputerEngineering (IOSR-JCE), vol. 11, pp. 75–78, May-June 2013.

Prof.E.velumani completed his Master degree (M.Sc Applied Electronics) in the year 1995 and M,phil Electronics in the year 2001 from Bharathiar university Coimbatore,Tamilnadu.
He also completed M.E Applied Electronics in the year 2010 at Anna University.He also completed MBA and MCA degrees from IGNOU. Prof.E.velumani currently working as Associate professor in PSG college of Arts and Sience,Coimbatore, Tamilnadu. His area of interest is Wireless sensor networks.