iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** V **Month of publication:** May 2017

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

Volume 5 Issue V, May 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

An Approach for Certificate Less Key Management with Energy Based Routing Protocol

S. Sathya[1,] M. Anitha[2,] R. Padmapriya[3], D. Kalaimani[4]
[1,2,3,,4]*Assistant Professor, CSE, Panimalar Engineering College, Chennai, India*

Abstract: ***In dynamic Wireless sensor networks, we enhance the Certificateless-effective key management (CL-EKM) protocol for secure communication with Efficient Energy System. We are going to find the proper value for the Tbackoff and Thold parameters using the mathematical model based on the velocity and the desired tradeoff between the energy consumption and the security level. Due to the limited energy and communication ability of sensor nodes, it seems important to design a routing protocol for dynamic WSNs so that sensing data can be transmitted to the receiver efficiently. An energy-balanced routing method based on forward-aware factor is proposed in this paper with effective key management strategies in it. In this system, the next-hop node is selected according to the awareness of link weight and FED. In addition, using reconstruction mechanism local topology is designed. The experimental results show that our system balances the energy consumption, prolongs the function of lifetime and guarantees high QoS of WSN.***

Index Terms: Certificate less-effective key management (CL-EKM)), Energy Efficient System, energy-balanced routing method, forward-aware factor, effective key management strategies, reconstruction mechanism and energy consumption

I. INTRODUCTION

Applications of wireless sensor networks (WSNs) have gained global attention in recent years. The network is built using sensor nodes which are small, with restricted computing and processing resources, and they are inexpensive [1]. These sensor nodes can sense, measure, and gather information from the environment based on application of the network deployed in the area or by some local decision process, they can transmit collected data to the user or sink node [2].

The medical applications can be of two types: wearable and implanted. Wearable devices are used on the body surface of a human or just at close proximity of the user. The implantable medical devices are those that are inserted inside human body. There are many other applications too e.g. body position measurement and location of the person, overall monitoring of ill patients in hospitals and at homes.

Body-area networks can collect information about an individual's health, fitness, and energy expenditure. WSN have large areas of applications but they are limited due some limitation of its architecture like

limited energy, processing power, scalability issues, storage capacity, bandwidth, range etc. So when it comes to different mechanisms like Key management, Routing, Data Aggregation or Tracking or other area, we must develop the techniques to make it more efficient.

Energy consumption is one of the important parameter for battery powered wireless sensor networks. It is necessary to decrease energy consumption in all the sensor nodes to increase the network lifetime [3]. In WSNs, the nodes close to the sink have tendency to exhaust their energy rapidly compared to the nodes away from the sink and such unbalanced energy drain will decrease the network lifetime. Unbalanced energy utilization can cause network detachment even though many nodes may have highest residual energy which is away from the sink [4]. Thus, it is necessary that each and every node should consume energy equally in order to increase the lifetime of the network.

Wireless sensor nodes can use up their restricted supply of energy performing computations and transmitting information in a wireless communication environment. As such, energy conserving forms of communication and computation are essential. In a multi hop Wireless sensor networks, each and every node plays a dual role as data sender and router. The malfunctioning of a few sensor nodes due to power interruption can cause significant topological changes and the might require rerouting of packets and reorganization of the network.

As dynamic wireless sensor nodes are deployed in aggressive or remote environment and unattended by human, they are prone to various kinds of attacks. So data must be transfer between nodes using encryption techniques and for that adaptation of key management is very important for WSNs. Key management is a core mechanism to ensure security in network and one of the major applications of wireless sensor network. Key management can be defined as a set of processes that support key establishment and

©IJRASET: All Rights are Reserved

Volume 5 Issue V, May 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

the maintenance of key relationships between valid parties according to the security policy [5]

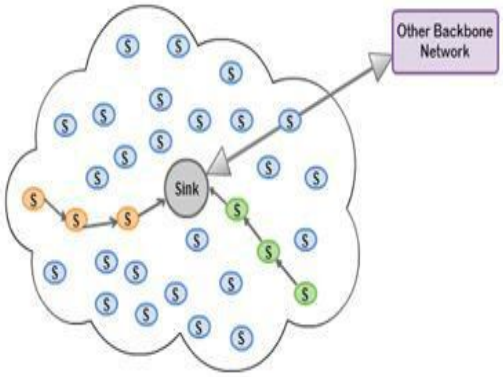


Figure1: Wireless Sensor Network Architecture

Every key management schemes should satisfy some conventional security requirements such as validation, freshness, privacy and trustworthiness. Key management may be a core mechanism to protection the security in network and may be outlined as a collection of processes that support key establishment and maintenance in a progress relation between certified parties according to the security policy [6]. The key management in WSNs consists of various processes such as creation, distribution and maintenance of the secret keys. Key management for encryption, which can make data transmission more secure and at a same time make a less resource consumption, have vital importance in WSNs. The goal of key management in wireless sensor networks is to solve the problem of creating, sharing and maintaining those secrete keys. Hence techniques for key management of encryption keys are vital importance for security in WSNs Depending on the capability to update the cryptographic keys of sensor nodes in their run time (rekeying), these scheme can be divided into two categories: dynamic key management and static key management. In static key management, the key pre-distribution is utilized, and cryptographic keys are set for the whole lifetime of the network. However, as a cryptographic key is used for a long time, its possibility of being attacked increases drastically. Instead, in dynamic key management, the cryptographic keys are cannot be fixed all over the lifetime of the network.

Dynamic key management is a process used to perform rekeying either periodically or on demand as required by the network. Since the keys of compromised nodes are revoked during runtime in the rekeying method, dynamic key management system enhances network survivability and network resilience significantly. In this paper our research focus on the providing the secure communication in the sensor nodes using the energy efficient and effective key management protocol.

The main objective is to maintain the desired tradeoff between the energy consumption and security level. It uses the energy balanced routing protocol to select the effective the cluster head for efficient data transferring and less energy consumption with higher security level in the key management protocol. Network overload also depends on the type of routing protocol. Because routing protocol decide the next hop node for transmitting the data to sink. Finally traffic load depends on the feature of environment which affects the radio communication actions of the sensor node. Based on the detailed analysis of data transmission mechanism, we describe the forward transmission area. Based on these we define an energy balanced routing with effective key management method that balances the energy consumption, security level and increase the network life time.

II. ANALYSIS

There are so many key management schemes available, but due to the limited resources available in WSNs, one can't apply the same scheme. So we discuss for the most dynamic key management scheme as well as with energy balanced routing method, which is based on cluster based WSNs, and emphasize on security, network lifetime, scalability, and performance analysis of each scheme. Hence, lots of research works has been carried out for the same in WSNs.

In Wireless sensor networks, considering the drawback of computing, communication, and energy of node, symmetric key cryptography is commonly used in WSNs because of its low power utilization. However, the traditional public key encryption is not suitable for WSNs because it is simple to go beyond the computational capacity and memory storage of nodes. Recently, some researchers have enhanced public key cryptography based on Elliptic Curve Cryptography (ECC) [7] which is feasible in wide area networks. The Elliptic Curve Digital Signature Algorithm (ECDSA) is also widely used in wireless sensor networks.

X. He et al [9] have explained different issues with key management, as sensor node have restricted power and processing

©IJRASET: All Rights are Reserved

capabilities, so it must to design the method which is more efficient and at a same time it can provides the better security. So in [9], we have decided to work on cluster based key management techniques to decrease the overhead, increase the network lifetime and scalability. Du [10] proposed routing-driven elliptic curve cryptography based on key management method where a node just need establish communication with a small segment of its neighbors, not all of them. According to the routing information, cluster heads encrypt session keys with ECC and then forward them to adjacent nodes which need to establish communication .It saves storage space, however it does not consider the key update. Zhou [11] proposed a key management method for heterogeneous wireless sensor networks based on ECC and Trivariate symmetric polynomial. The greatest resiliency against node capture can be obtained, but rekeying will consume too much energy. According to O.Hao et al [12] have propose a scheme secure Low-Energy Adaptive Clustering Hierarchy (Sec-LEACH) a probabilistic key management scheme. Sec-LEACH gives authentication and protection to network without use of base station (BS). However the scheme is scalable yet less resilient against the compromised node and doesn't give full connectivity between nodes. In this paper [13], a new protocol called Equalized Cluster Head Election Routing Protocol (ECHERP) was proposed which seeks energy conservation through balanced clustering. It represent the network as a linear system and, using the Gaussian elimination algorithm, finds the combinations of nodes that can be selected as cluster heads in order to extend the network lifetime.

In LEACH protocol [14] is one of the most famous WSNs hierarchical routing algorithms. In LEACH, the nodes organize themselves into local cluster; the protocol is isolated into a setup phase when the clusters are organized and a steady-state phase when data are transmitted to the cluster head and on to the sink from the nodes [1]–[3]. In the setup phase, each node choose any number between 0 and 1, if this number is smaller than a certain threshold T(n), the node will broadcast itself as the cluster head. The non cluster head node selects the cluster head with greater signal strength and join the cluster, and then the cluster head node gets data from all of the cluster members and transmits data to the remote sink [4]–[7].

In [15], the authors proposed an EKI approach. This approach assumes that divides the network into clusters using an appropriate algorithm for the deployment. This approach present a key management solution based on ECC and an authentication key agreement mechanism. A cluster head is deployed as a controller of the intra-cluster key encryption, which is used for cluster members. The system deploys a base station BS which is the most powerful and secure as the key controller of the entire network and cooperates with the cluster heads to produce the key of the whole system.

There other key management schemes which we have gone through are which shows as an efficient and secure session key management (ESSKM) scheme.

In [16], Qin Wang et al. have described method which is based on LEACH protocol. The scheme uses symmetric key mechanism and improved the session key by updating periodically within a cluster. Hence this scheme provides secure against different type of attack from the malicious node. This scheme achieves more security and energy saving with low storage. But it is applicable on static cluster formation and as not much resilient. It uses fewer messages to be exchanged to generate the keys so reduce the communication overhead and provide the full connectivity. The issue with the ESSKM is that like it is not scalable and CHs are static in each round and make it using Efficient in terms of energy consumption.

A. Existing System

In the existing methods, they have upgrade a Certificateless Key Management scheme that supports the establishment of four types of keys: a Certificateless public/private key pair, an individual key, a pairwise key, and a cluster key. This system also utilizes the main algorithms of the CL-HSC scheme [17] in deriving Certificateless public/private keys and pairwise keys.

The CL-EKM is comprised of 7 phases: system setup, pairwise key generation, cluster formation, key update, key revocation node movement, and addition of a new node. They assume that an adversary captures a node in the j^{th} cluster. This adversary can then extract the keys, such as the pairwise key shared with the cluster head, the public/private key pair, the cluster key, and the individual key.

However, the pairwise master/encryption key generation between any two nodes is independent of others, and hence each pair of nodes has different pairwise keys. Therefore, even if the adversary manages to obtain secure keys, it is unable to extract any information useful to compromise the pairwise keys of other uncompromised nodes. As a result, the compromise of a sensor does not affect the communication security among other clusters members sensors or cluster head sensors.

Even though the attacker can read the group communications within the cluster with the cluster key extracted from the compromised node, it cannot get any information about the cluster key of other clusters.

©IJRASET: All Rights are Reserved

Volume 5 Issue V, May 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

B. Limitations

The major limitation in the existing methods, the cluster head shares the new cluster key to each cluster node, except the revoked node, by encrypting the key with the pairwise encryption key among the cluster and each intended node. Thus, the revoked node fails to decrypt any subsequent messages by the old pairwise encryption key or cluster key. When a node joins a cluster, the cluster head generates a new cluster key by selecting a new random value.

Since the joined node receives the new cluster key, it cannot decrypt earlier messages encrypted using the cluster keys. A packet delivery in a wireless sensor network is unreliable due to unexpected obstacles, time-varying wireless channel conditions, and a low-power transceiver.

III. PROPOSED SYSTEM

This paper proposes an upgrade of the Certificateless-effective key management protocol with the energy balanced routing method using forward aware factor. Based on the detailed analysis of the data transmission mechanism of WSNs, we measure the forward transmission area, define forward energy density, which constitutes forward-aware factor with link weight, and propose another energy-balance routing protocol based on forward-aware factor with the effective key management and thus balancing the energy consumption, security level and prolonging the function lifetime.

The enhancement of the Certificateless-effective key management with energy balanced routing protocol based forward aware factor can be done using the following approaches:

A. It incorporates the forward aware factor based energy balanced routing method, by uses forward transmission area according to the position of sink and the last data flow direction.

B. Make more efficient using improved cluster head selection based forward energy density in the energy balanced routing protocol.

C. After the cluster head selection, to ensure the secure communication between the nodes, pair wise key generation would produce the master secret key establishment to the neighbor nodes with the identifier and public key.

D. Cluster head makes the secure authentication with cluster members through the cluster key encryption and then collects the data from the cluster members

E. It uses the reconstruction mechanisms for key update and key revocation.

F. It includes the adding the new node in the existing the node setup in the model

G. The main goal of this model is to maintain the minimum energy consumption among all sensor nodes

In the proposed system architecture is illustrated in the figure:2 Clusters heads all the cluster member information including their energy status to improve the network lifetime.

Based on the position of the sink and cluster node, the forward transmission area can be evaluated in this method. Forward transmission area (FTA) [8] defines the forward energy density which constitutes FAF with link weight. This proposed communication protocol sense of balance the energy utilization and increase the network life time.

A. System and Mathematical Model

The system architecture is divided into five different phases. In the first phase, Sensor nodes are randomly dispersed in the rectangular sensing field. Data are forward to the cluster head and then from cluster head to sink node. The second phase involves cluster formation and effective key management, while the third phase generates the cluster head based on forward transmission area. Energy consumption model is used in the fourth phase based on the forward energy density calculation. The fifth phase represents transferring the packet from the source to the destination.

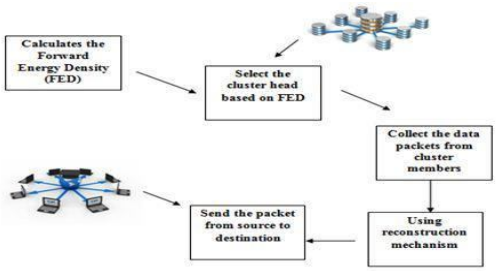


Figure 2: The proposed architecture.

©IJRASET: All Rights are Reserved

Volume 5 Issue V, May 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

B. Forward Transmission Area

The original energy of the node can be considered as E_o. When this energy is drained means node dies, however energy of the sink node can be increased. The location of the sink and sensor node can be fixed. The sink node broadcast the information to all sensor nodes in the sensing field.

Received signal strength is used to calculate the distance between source and sink node. Central node cannot be nominated at first. It can be selected after the topology development [8].

The communication scope of the sensor node is set to d_o

$$d_o = \sqrt{(\varepsilon_{fs}^2 / \varepsilon_{mp})} \qquad (1)$$

the threshold d_o can be defined as

Where ε_{fs}, ε_{mp} are energy coefficients

From fig.3 d (i, sink) is the distance between the node i and sink node. d (i ,sink) can be defined as

$$R = (X, \sqrt{((H/2)^2 + (X+W)^2)}) \qquad (2)$$

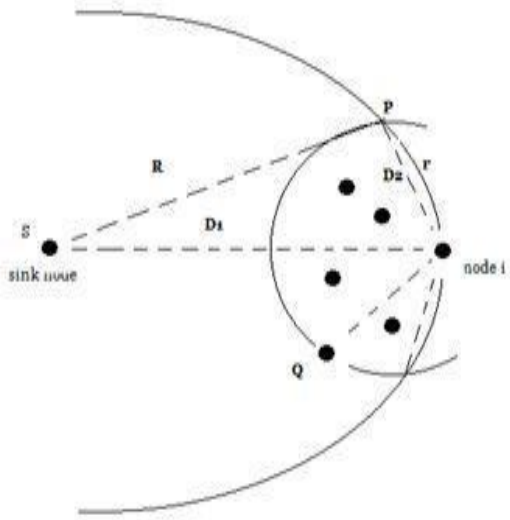


Figure 3: Forward transmission area

When i is the cluster head, the communication radius of the cluster head R_{opt} (i) is given by

$$R_{opt}(i) \propto f_1(R) \qquad (3)$$

Where f_1 (d(i ,sink) is the function of d(i ,sink). And its ranges is between 0 and

Fig 3. Shows two circle, circle 1 has d (i, sink) as the radius and sink as the center. Circle 2 has node as center and d_{ip} as radius. Forward transmission area of node I can be referred as FTA (i)

$$\text{FTA (i)} = \Theta S \cap \Theta i \qquad (4)$$

$$r = \max(d_{ij}), j \in N'(i) \qquad (5)$$

where d_{ij} is the distance between node i and node j, N(i) is the set of nodes that has the connection with node i and N′(i) is the set of nodes of N(i) that have an edge with node i[8].

©IJRASET: All Rights are Reserved

In this routing scheme, each time the node finishes the transmission, the strength of the next hop node is checked. If the hop node energy is less than the average value of all sensor node strength in forward transmission area then topology reconstruction is launched. New node is selected for next round of transmission. Energy balanced routing system based on Forward aware factor is used for the large scale WSN for static data collection and event detection [9]. This algorithm classified into several stages

1) Decide the FTA (i) and the possible next hop nodes of node i. The node that adjacent to sink than node i constitute set of all probable next hop nodes and furthest node determine the FTA (i).

2) Next evaluate FTA (j) and $S_{FTA}(j)$ for all possible hop node. It can be designed as that of FTA (i) and $S_{FTA}(i)$

$$S_{FTA}(i)=\frac{1}{2}\pi d_2^2-d_2\sqrt{d_1^2-\frac{1}{4}d_2^2}+(d_1^2-\frac{1}{2}d_2^2)$$

$$\times\arccos\left[1-\frac{1}{2}\left(\frac{d_2}{d_1}\right)^2\right] \qquad (6)$$

The communication launch node can calculate the weight of edge between neighbors. Neighbors can get its individual FED. It avoids the communication launch node doing all of the algorithms. Thus, each and every node's memory should storage its individual ID, real time energy, distance to the Sink, and FED at any instant, which could be feed back to launch node quickly.

C. Reconstruction Mechanism

In the actual routing process, nodes with greater signal strength will have more communication link and result in aster energy consumption. The whole network cannot always work under these topology structures. A topology reconnecting method of the cluster head rotation algorithm like LEACH is needed.

The whole WSN information is limited, and global topology alteration may affect the information perception, the global change caused by energy unbalanced area is a waste of power to energy balanced area, thus a local topology reconstruction mechanism is necessary. This paper proposes a point strength-driven local topology reconstruction mechanism based on forward aware factor in the energy balanced reconstruction mechanism (FAF-EBRM).

The stages of the algorithm as given here.

1) In FAF-EBRM, every time node i finishes transmission, check the point strength of the next-hop node j . If it is fewer than the average value of all of the sensors' strengths in FTA, the local topology reconfiguration mechanism should be launched in node i ' s FTA.

2) Before the topology reconfiguration mechanism is launched, remove the link between i and j , remove j from FTA(i) , and get a new set FTA' (i) Then, reconnect in, and the function of connect possibility is given as

$$P_{i\to j}=s_j/\sum_{j\in FTA'(i)}S_j \qquad (7)$$

The node removed in 2) may be the possible next-hop node when the next transmission is finished, and the revocation of the edge does not change the possible reconnection. The node's real-time strength is needed to calculate the sum of strengths.

D. Performance Evaluation

1) *Simulation Parameters:* At present agent based modeling and simulation is the only pattern which allows the simulation of complex behavior in the environment of WSNs. Agent based simulation of WSN is new paradigm. It is based on social simulation. Simulation shows the comparison between energy balanced routing protocol with LEACH by five parameters: throughput, energy consumption, end to end latency, packet drop, packet delivery ratio. Simulation results shows that the performance of energy balanced routing protocol can be much better than the LEACH protocol in terms of below parameters.

2) *Performance Metrics:* The metrics used to evaluate performance of proposed approach:

3) *Packet Delivery Ratio (PDR):* It can be defined as the ratio of number of packets received to the number of packets sent.

©IJRASET: All Rights are Reserved

Volume 5 Issue V, May 2017
ISSN: 2321-9653

4) *Throughput:* It can be defined as rate of successful message transferred over a communication channel.
5) *End to end latency:* It refers to the time taken for a packet to reach source to target over a network.
6) *Packet drop:* It means difference between packets sent and packets received.
7) *Energy consumption:* It can be defined as average energy consumed on ideal sleep transmits and received to total energy consumed.
8) *Simulation results:* We utilized the performance metrics to validate the proposed algorithm against black hole attack and the results obtained are shown in Figure4-8.

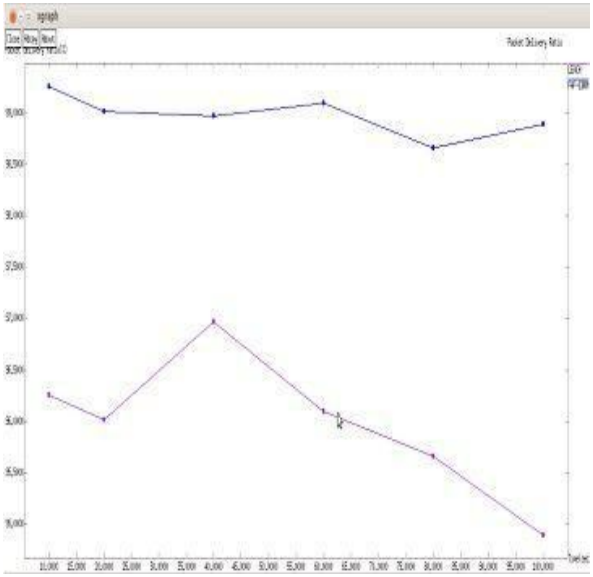


Figure 4: Comparison of Packet Delivery Ratio

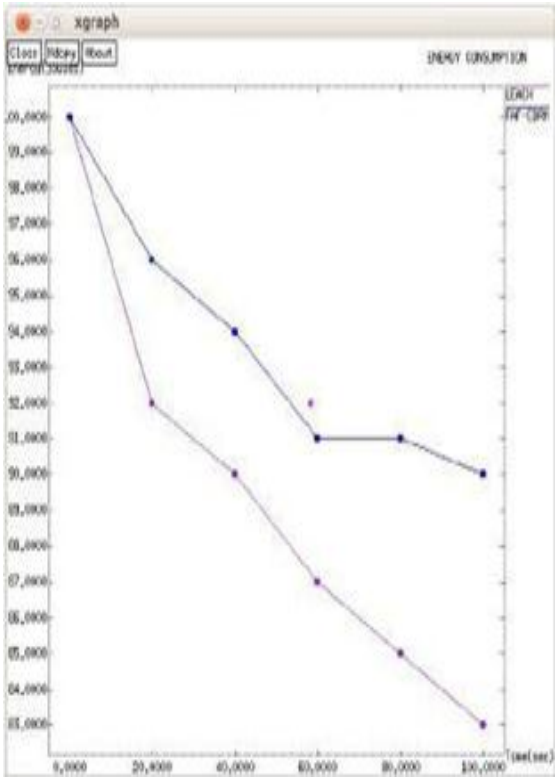


Figure 5: Comparison of Energy Consumption

©IJRASET: All Rights are Reserved

Volume 5 Issue V, May 2017
ISSN: 2321-9653

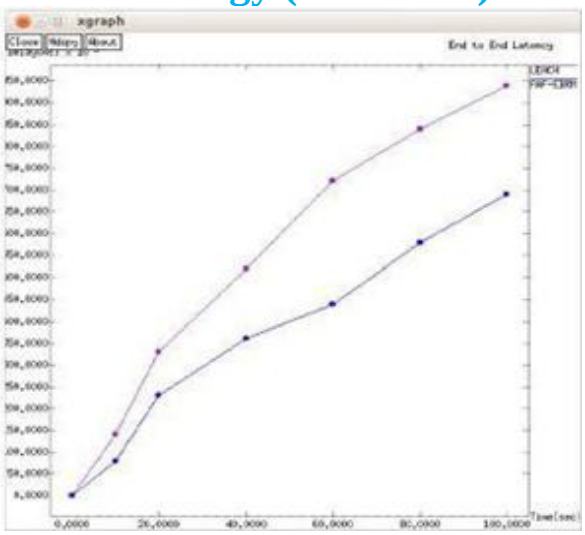


Figure 6: Comparison of End to End Latency

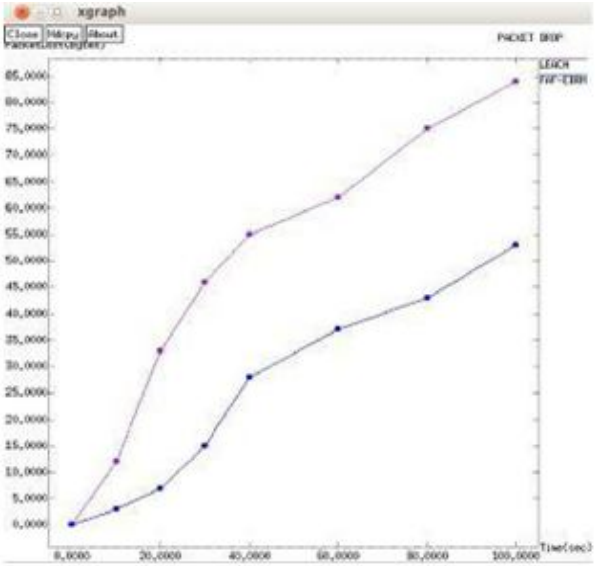


Figure 7: Comparison of Packet Drop

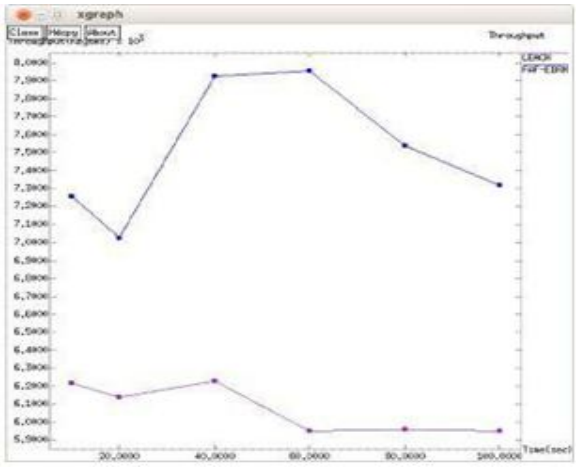


Figure 8: Comparison of Throughput

©IJRASET: All Rights are Reserved

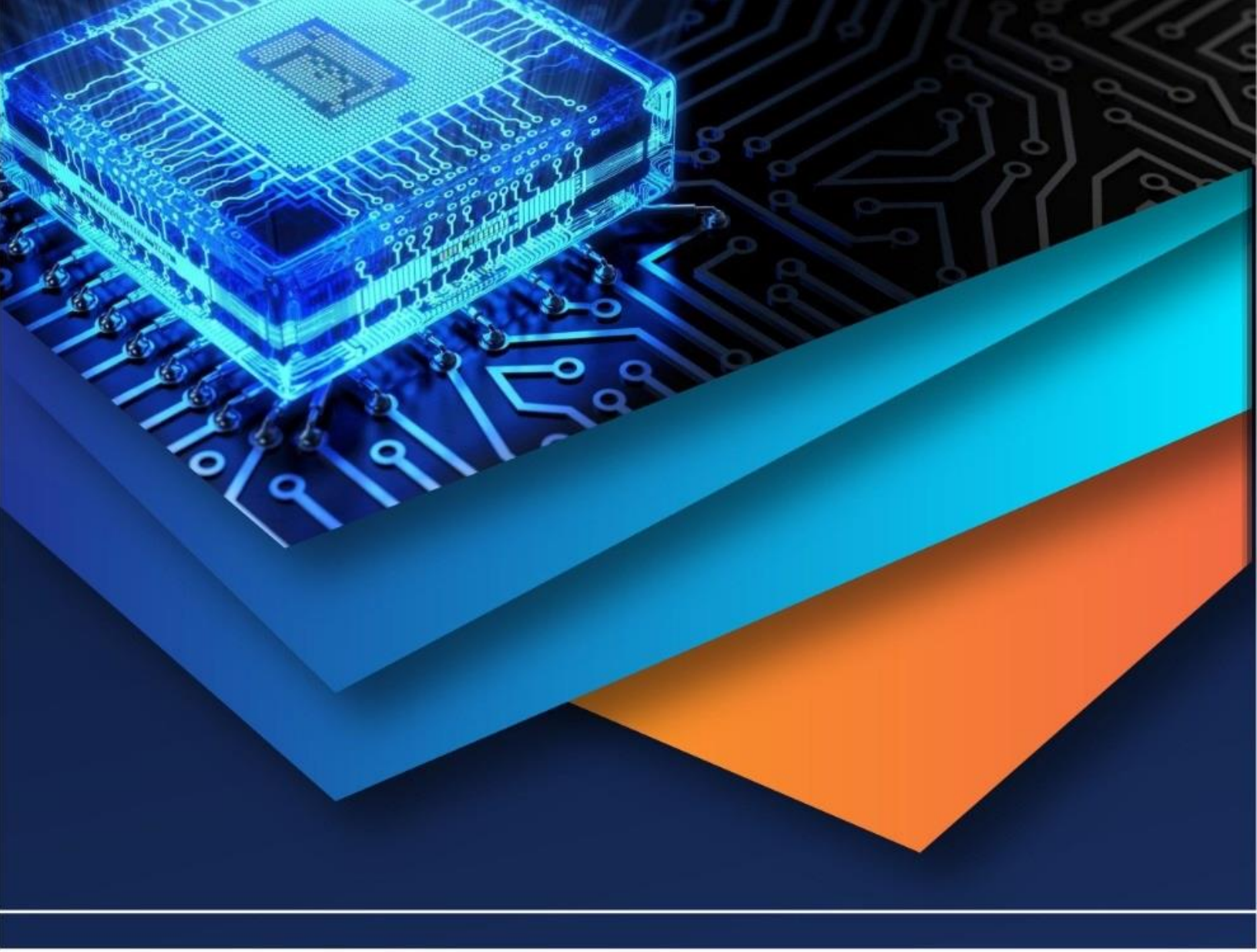
IV. CONCLUSION

An energy-balanced routing technique FAF-EBRM based on forward-aware factor and certificateless-effective key management (CL-EKM) is proposed in this paper. In FAF-EBRM, the next-hop node is selected according to the awareness of link weight and forward energy density. In addition, a spontaneous reconstruction mechanism for local topology is designed. In the experiment, FAF-EBRM is compared with LEACH and experimental results show that FAFEBRM outperforms LEACH, which balances the energy utilization, packet delivery ratio, end to end latency, packet drop and throughput prolongs the function lifetime, and guarantees high QoS of WSN. Also, they show that the distributions of node degree, strength, and edge weight follow power law and represent "tail," so the topology has robustness and fault tolerance, reduces the probability of successive node failure, and enhances the synchronization of WSN of IA.

REFERENCES

[1] S. Aeron, V. Saligrama, and D. A. Castanon, (2008)"Efficient Sensor Management Policies for Distributed Target Tracking in Multihop Sensor Networks," IEEE Transactions Signal Processing, vol. 56, no. 6, pp. 2562-2574.
[2] H. Liu, P. Wan, and X. Jia, (2007) "Maximal Lifetime Scheduling for Sensor Surveillance Systems with K Sensors to One Target," IEEE Transactions Parallel and Distributed Systems, vol. 15, no. 2, pp. 334-345.
[3] W. R. Heinzelman, A. Chandrakasan, and Balakrishnan, (2002)"An Application-Specific ProtocolArchitecture for Wireless Micro-sensor Networks," IEEE Transactions Wireless Communications, vol. 1, no.4, pp. 660-670.
[4] Fengyuan Ren, Jiao Zhang, Tao He, Chuang Lin, and Sajal K. Das, (2011) "EBRP: Energy-Balanced Routing
[5] Protocol for Data gathering in Wireless Sensor Networks," IEEE Transactions on Parallel and Distributed Systems, vol. 22, no. 12.
[6] S. Olariu and I. Stojmenovi, (2006) "Design Guidelines for Maximizing Lifetime and Avoiding Energy Holes in
[7] Sensor Networks with Uniform Distribution and Uniform Reporting," Proceedings IEEE INFOCOM.
[8] D. G. Zhang, "A new medium access control protocol based on perceiveddata reliability and spatial correlation in wireless sensor network," Comput, Electr. Eng., vol. 38, no. 3, pp. 694–702, 2012
[9] Chan H, Perrig A, Song D. Random key pre distribution schemes for sensor networks, 2003 Symposium on Security and Privacy. IEEE, pp. 197-213, 2003.
[10] Zhou R, Yang H. A hybrid key management scheme for Heterogeneous wireless sensor networks based on ECC and trivariate symmetric polynomial, 2011 International Conference on Uncertainty Reasoning and Knowledge Engineering (URKE). IEEE, Vol.1, 251-255, 2011.
[11] J. Li and Y. Zhou, "Target Tracking in Wireless Sensor Networks", Wireless Sensor Networks: Application - Centric Design, pp. 1-20, December 2010.
[12] D. Du, H. Xiong, and H. Wang, "An efficient key management scheme for wireless sensor networks," Int. J. Distrib. Sensor Netw., vol. 2012, Sep. 2012, Art. ID 406254.
[13] S.Zhu, S.Setia, and S.Jajodia,"LEAP+ : Efficient security mechanisms for large-scale distributed sensor networks," ACM Trans.Sen.Netw., Vol.2, no.4, pp.500 528, (2006).
[14] X He, M Niedermeier and H Meer," Dynamic Key Management in Wireless Sensor Networks: A survey," Journal of Network and Computer Applications, pp.611-622, 2012.
[15] Bo Chang and Xinrong Zhang, (2010) "An Energy-Efficient Cluster-Based Data Gathering Protocol for Wireless
[16] Sensor Networks," Wireless Communications Networking and Mobile Computing (WiCOM).
[17] Rui Wu, Kewen Xia,Yanjun Zhang, and Guodong Li, (2013)"Optimal Design on Clustering Routing Protocol for Wireless Sensor Network," Journa lof Computational Information Systems,.
[18] M.Bayat and M.R.Aref,"A Secure and efficient elliptic curve based authentication and key agreement protocol suitable for WSN," IACR Cryptology ePrint Archive 2013,(2013).
[19] F. V. C. Martins and E. G. Garrano, "A hybrid multiobjective evolutionary approach for improving the performance of wireless sensor networks," IEEE Sensors J., vol. 11, no. 3, pp. 545–554, Mar. 2011.

©IJRASET: All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)