International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 04 Issue: 12 | Dec-2017 www.irjet.net p-ISSN: 2395-0072

A Survey On Secure Alternate Path Selection For Enhanced Network Lifetime in Wireless Sensor Network

Kajal K.Kapoor[1], Sujata Wakchaure[2]

[1,2] *Professor, Department Of Computer Engineering Mitcoe, Pune, Maharashtra, India*

Abstract - *The main challenge of wireless sensor network is its lifetime. In this type of network, single static sink node is present, a sensor device node require more energy for estimating information packet specifically those are available in the area of the sink node. Such nodes separate the energy so fast due to the numerous tone traffic patterns and at the end they die. This uneven event is named as hot spot issue which gets more real as the numbers of sensor nodes increases. Generally, replacement of such energy sources is not feasible and cost effective solution. For this problem, there is one solution regarding to distance. If the distance between sensor and sink node is minimized; the energy consumption will be effectively reduced. This paper presents the solution for enhancing network lifetime with energy saving of sensor nodes. Here we also discuss on the limitations and advantages of previous methods. The sensors nodes consume more battery power which is at minimum distance from sink node. Therefore, energy of sensor nodes in network will quickly consumed their energy. So that, the lifetime of a sensor nodes will be produces. To overcome this drawback of this system, we propose alternate shortest path technique. To enhance the efficiency of energy along with network lifespan this approach is used. Furthermore we developed a novel technique called Energy Aware Sink Relocation (EASR) for remote base station in WSN if the energy of alternate path is going to die. This system exploit information recognized with the remaining energy of sensor nodes battery for increasing the range of transmission of sensor node and relocation technique for the sink node in network. Calculate some numerical and theoretical calculations are given to demonstrate that the EASR strategy is used to increase the network energy of the remote system essentially. ECC algorithm increases more network lifetime and transfers secure data. An improved AES-ECC hybrid encryption design has good flexibility and versatility. It has improved the speed of the digital signature generation and authentication.*

Key Words: **Wireless sensor networks; cluster head; base station; cache based system; sensor nodes.**

1.INTRODUCTION

In the wireless network of sensor, nodes are outline by heavily deployment the huge types of sensor nodes in a particular geographical area. The information captured from sensor nodes is transmitted to monitoring station. These monitoring stations worked as a sink or base station. This base station is placed far from actual sensing area. To transfer this sensed information from source to base station, concept of multi hop routing and flooding is used. With the multiple numbers of Base stations, the total number of hops can get minimized. This will results in minimized energy consumption by sensor node. The minimum energy consumption of sensor nodes will improving lifetime of sensor network along with high rate of packet transmission to base station. So the communication nodes deployment and the different sink nodes are treated as most important components in the lifetime in wireless sensor network.

The WSN have various applications such as climate observing, battlefield investigation and inventory, manufacturing progressions. Maximum time, the sensor environment needs intolerant. In the remote network system, sensor devices are not present to replace when their batteries channel. The battery exhausted from nodes can be brought several issues, for example, take coverage hollow space moreover, communication hollow space issues. Consequently, some WSN systems are busy in planning proficient approach to keep the energy of sensor nodes, as an instance, drawing schedule of cycle for sensor nodes, which is used to permit some of nodes and enters into the die state to moderate power of energy. Now sensor node does not damaging the running sensing process of the wireless network. The efficient design of energy algorithms aim at balancing the depletion of the battery exploitation strength of every sensor node or consuming a limited data aggregation technique for mixture of sensory information into a unit to decreases the number of message transmitted to prolong the wireless network lifetime. The enormous majority of such system scans coincide in the network system work. The another methodology is used for the purpose of storing energy as well as utilizing remote sensors to maintain the locations of region with aggregating lifetime network energy of nodes.

For enhancing the lifespan of network as well as efficiency of energy we propose a shortest alternate path mechanism in this paper. For transmitting data from source to sink node safely use alternate path and ECC algorithm. Elliptic curve cryptography (ECC) is a kind of public key cryptosystem like RSA. But it differs from RSA in its quicker evolving capacity and by providing attractive and alternative way to researchers of cryptographic algorithm. The security level which is given by RSA can be provided even by smaller keys of ECC (for example, a 160 bit ECC has roughly the same security strength as 1024 bit RSA).

When energy level is less than given threshold for alternate path, we trigger the relocation of sink. Scheme for sink relocation is explored here, which decide when and where to relocate the position of sink. The mathematical performance evaluations are calculated to determine the proposed sink relocating scheme which is beneficial for enhancing the network lifetime of a system. The simulation of technique used in project to check out the precaution of the EASR technique. This type of approach can work to improve the lifetime of a WSN system. The sink node relocation will be prolonging the battery usage of nodes.

The existing symmetric encryption schemes, such as AES, provide a strong security solution but maintenance of keys is difficult. When asymmetric schemes could be used, maintenance of keys become easier but they provide a lesser degree of security when compared to symmetric encryption schemes. To cope with these shortcomings, the use of a new version of the hybrid encryption system is proposed which is a combination of Advanced Encryption Standard and Elliptical Curve Cryptography with cross encrypted keys for secure key exchange. Hence we proposed the AES-ECC hybrid encryption system targeted to Wireless Sensor Networks (WSNs) to increase lifetime of network.

Section II illustrates the related work studied for our new topic. Section III demonstrate the details of project implementation, definitions of terms and in addition the documentation can be expressing the proposed system undertakings in this paper. Section IV includes conclusions and represents future work of project.

2. LITERATURE SURVEY

In this part we illustrate the previous techniques proposed by the authors for WSN system.

G. S. Sara and D. Sridharan [2], represents a survey of routing schemes in remote sensor nodes networks. In WSN's author review the challenges for routing protocol designs. The comprehensive research of individual routing technique classified into three stages depend upon the structure of network like as flat, hierarchical, and location-based routing etc.
Somasundara et al. [3] investigate a network system which depends on the utilization of mobile components and to reduce the utilization of the energy constrained nodes at the time of communication and enhance useful network. Similarly, their approach gains the advantages in sensor networks and inadequately deployed sensors in network. They demonstrate how their procedure supports to reduce energy utilization at energy controlled nodes. After that, for enhancing the performance of energy author illustrate their framework model which uses their proposed way.

Sensor network deployment is highly challenging because of the aggressive as well as volatile nature of utilization environments. Mousavi et al., [4] implemented two routines for the self-deployment of mobile sensors. Basically author developed a randomized way that offers both simplicity and applicability to different environments.

Akyildiz et al. [5] describe idea of network formed by sensors. These sensors have combined micro electro mechanical technology, wireless communication and digital physics. First, the sensing tasks and applications of sensor networks are examined, and a comparative analysis of things influencing the look of sensor networks is given.

The main benefit of sensor node networks is there self-organizing nature as well as autonomous process and possible architectural alternatives suitable for a different types of data centric driven applications. During this article N. Jain and D. P. Agrawal [6], deal with the present an outline of this state of the art inside the field of wireless sensor networks.

D. Tian and N. D. Georganas [7], has introduced, an inclinations to a node scheduling scheme, which can reduced the energy utilization of complete system, therefore growing network time period, by characteristic redundant nodes with respect of sensing coverage of network, moreover distributing them an offline operation mode. This offline mode has minimum energy consumption than the online mode.

Hong et al. [8], implemented a capable route set up for distributed sensing element network utilizing the similar process between the wireless and multi hop communications network concerning instruments and rovers and therefore the packet radio network utilized as a typical ad hoc networking surroundings.

S. C. Huang and R. H. Jan [9], for enlarge the lifetime of network's presented an Energy Aware Cluster Based Routing Algorithm (ECRA) in WSN's. This algorithm chooses some nodes as cluster heads to construct Voronoi outlines, move the cluster head load balancing in every cluster of nodes. To improve the execution of the ECRA a two tier architecture (ECRA-2T) is designed. The reproductions demonstrate that both the ECRA-2T as well as ECRA algorithm perform better than other routing schemes such as direct communication, static clustering, and LEACH.

R. C. Shah and J. Rabaey [10] developed a energy aware routing mechanism, that is depend upon sub optimal paths which gives substantial gain. Additionally the experimental results are shown that increment in lifetime of network over practically similar plans like directed diffusion routing. The more elegant degradation of service with time in a fairer manner to overcome the burning energy of nodes.

In planning sensor networks Sensor deployment is a primary problem. Wang et al. [11], they review and makes use of disseminated self deployment protocols for mobile sensors. The protocols are proposed to estimate the target positions

of the sensors after finding coverage of hole in network where the sink is ready to move.

3. IMPLEMENTATION DETAILS

In this field, we illustrate the overview of system, algorithmic steps of system, and mathematical formulation of the proposed system.

3.1 System Overview

Figure 1 represents that architecture of the proposed system. System works as following way:

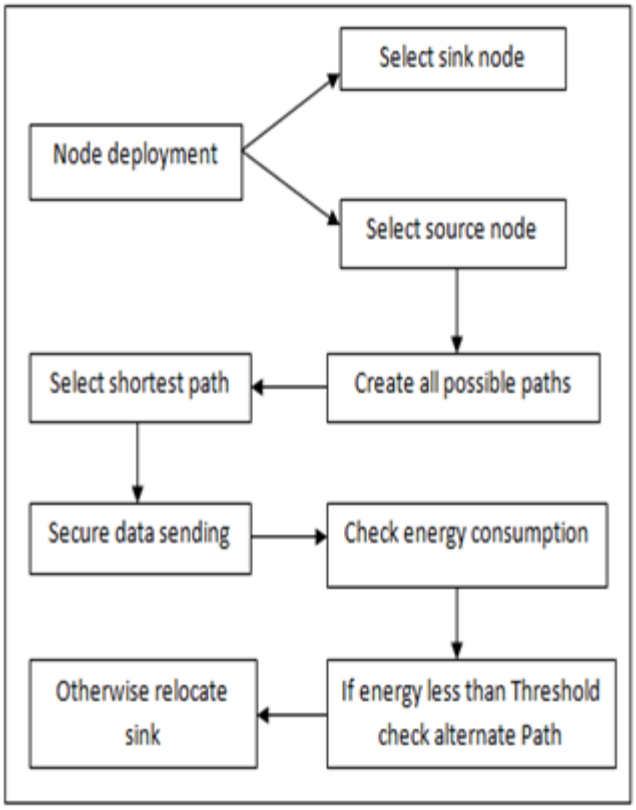

Fig -1. Proposed System Architecture

- Network Generation

  In this phase, user can generate vertices or nodes. These nodes are connected by edges.

- Path Generation:

  It creates all possible routes from source to sink node after creating source as well as sink.

- Shortest Path Selection:

  After generation of all possible paths from source to destination node, shortest path is selected on the basis of minimum weight of edge.

- Generation and distribution of Keys:

  At key generation center, keys are generated and distributed to all nodes belongs to shortest path.

- Encryption of data:

  At every node, collected data is encrypted by using ECC algorithm for security purpose.

- Estimation of Energy Consumption:

  After collection of data or sending of data or any type of action, consumed energy is calculated at each node.

- Data Authentication:

  Sink node check the authenticated data after determining the hash value at source node.

- Data Decryption:

  After receiving the data from source node, sink node decrypt the data for further processing. For decryption sink node has the decryption key.

3.2 Mathematical Model

System S is represented as
S= {N, S, D, P, Sp, K, d}

1. Deployment of nodes

   N = {n1, n2. . ..nn}
   Where,
   N is set of n umber of deployed nodes.

2. Source node selection

   S = {s1, s2,… ,sn}
   Where, S is a set of Sources selected at each run time.

3. Sink Node selection

   D = {d1, d2, ...,dn}
   Where, D is a set of sink nodes selected at each run time.

4. All Paths from source to destination

   P = {p1, p2,....,pn}
   Where, P is a set of all n number of paths from source to destination.

5. Shortest Path Slection

   Sp = {sp1, sp2, sp3, ...,spn}
   Where Sp is the set of all possible shortest path from source to destination at each run time.

6. Authentication with keys

   K = {k1, k2,....,kn}
   Where, k is a set of n number of Keys generated and distributed to each node for authentication.

7. Data sending from source to destination.

   d= {d1, d2, d3, ...,dn}
   Where, d is the set of all data packets securely routing through shortest path.

3.2.1 Algorithm

The proposed scheme works as:

- **Algorithm 1: EASR Algorithm**

1. Generate a network graph Graph such as g(v,e)
   Where, V is the set of vertices and e is the set of all connecting edges to vertices.
2. Choose source and destination node among all sensor nodes.
3. Produce all possible paths from selected source to destination node.
4. Among all generated possible path, select the one shortest path based on weight factor.
5. Generate and distribute public-private key pair for source and destination node.
6. Perform data sending at source node through selected shortest path.
7. Encrypt the data with the private key before actual sending.
8. Estimate energy consumed by each node belongs to shortest path.
9. Decrypt the private key and authenticate received data at destination.
10. If energy node in path is going to die then select Alternate path among shortest path.
11. Resend the data from source to destination node through alternate path and also calculate energy consumed by path.
12. Again energy may expire of alternate path.
13. When energy is minimize, use energy-aware sink relocation technique (EASR) to relocate sink node at other place.

Explanation: Algorithm 1 describes primarily, with sensor nodes, source and sink node network is created. Then generate all routes from source to sink node and for data sending purpose choose the shortest path. Sensor nodes are not working properly if energy utilization is greater. Therefore systems choose optional communication path between source and destination node also estimate energy consumed by each node in network. By using the ECC algorithm encrypt the data with the secret key. With the help of its hash value data is validated. Only verified data is accepted by sink node. Decrypt the received data with the appropriate public key. If again energy is evacuate and path is expired, then repeat the procedure of sink relocation.

- **Algorithm 2: ECC Algorithm**

  Elliptic Curve Cryptography (ECC): Elliptic Curve Cryptography (ECC) [14] is a public key cryptography developed independently by Victor Miller and Neal Koblitz in the year 1985. In Elliptic Curve Cryptography we will be using the curve equation of the form

  $$y2 = x3 + ax + b$$

  which is known as Weierstrass equation, where a and b are the constant with

  $$4a3 + 27b2 = 0$$

  Algorithm:

1. Sender and Receiver node Calculate edB = S =(s1, s2).
2. Sender node sends a message M E to Receiver node as follows:
3. Compute L such that, (s1 * s2) mod N = L.
4. Compute L * M = C.
5. Send C to sender node.
6. Receiver node receives C and decrypts as follows:
7. Compute (s1 * s2)modN = L.
8. Compute (L-1)mod N, Where N = E
9. L-1*C = L-1*L*M = M.

- **Algorithm 3:AES-ECC Hybrid Encryption Model Implementation Algorithm**

ECC signature and verification process: Using the Hash function which was selected to process messages first, Signature Scheme Based on Elliptic Curve follows: The signer A has a private key d and a public key Q, making known to the public the public key Q, the selected Hash and other necessary information; A will send B signature-messages, B can verify the legitimacy of signatures based on public news, n is the order of point G. The signature generation process is as shown in Fig. 2 [13].

- To sign a message m, the sender performs the following steps:

1. kε[1, n-1], u = [k]G = (x_1, y_1); K is a random selection
2. Compute r = x_1 mod n, if r = 0, return to step 1
3. According sk = sha-1(m)+dr mod n, we would calculate s. If s = 0, return to step 1
4. (u, s) is the signature information, then, we sent m and (u, s) to B as (m(u, s))

5. To verify the signature, the receiver performs the following steps:

    - If s ∉[1.n-1], the signature is forged, reject the signature
    - Verify the equation:
      [s]u = [sha-1(m)]G+[r]Q

Validation passes if and only if equality holds, otherwise, the signature is forged, reject the signature proving the equation:

- Because $s = k^{-1}(sha\text{-}1(m)+dr)$ and u = [k]G
- Compute $[s]u = [k^{-1}(sha\text{-}1(m)+dr)k]G$
  $= [sha\text{-}1(m)]G+[dr]G$
  $= [sha\text{-}1(m)]G+[r]Q$

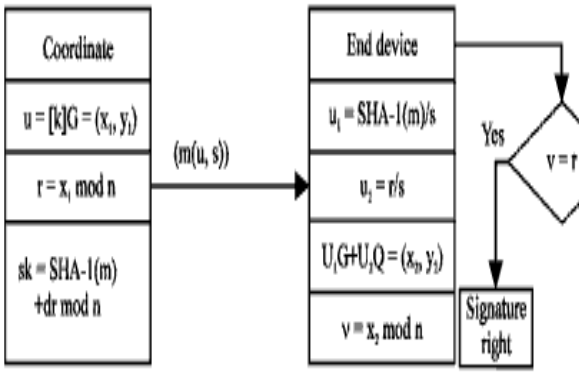

Fig -2 Digital signature software process

- **AES-ECC Hybrid Encryption Model Implementation Algorithm:**

1. Data is collected by the sensor data acquisition system
2. Using SHA-1 function to generate the data summary
3. Using the sender's private key K and ECC digital signature module to generate Digital Signatures
4. According to AES encryption module (the private key is KAES), encrypting digital signature and encrypting data which need to be sent. Then, getting data-ciphertext and signature-ciphertext
5. Encrypting the private key KAES by ECC encryption module, then, generating key-ciphertext
6. Packing all ciphertext and sending it by means of wireless sensor networks
7. The sender upload that ciphertext to the internet by the sink node, the users can use the mobile terminal to receive data
8. When the receiver receives the ciphertext, receiver uses his private key to decrypt the key KAES, then, decrypting the data-ciphertext and signature-ciphertext by KAES. Using the sender's public key to verify the signature and get the summary B; then we can get the summary A by using SHA-1 algorithm. Comparing summary A with summary B, if they are the same, then the data is valid and available; otherwise, it represents invalid data

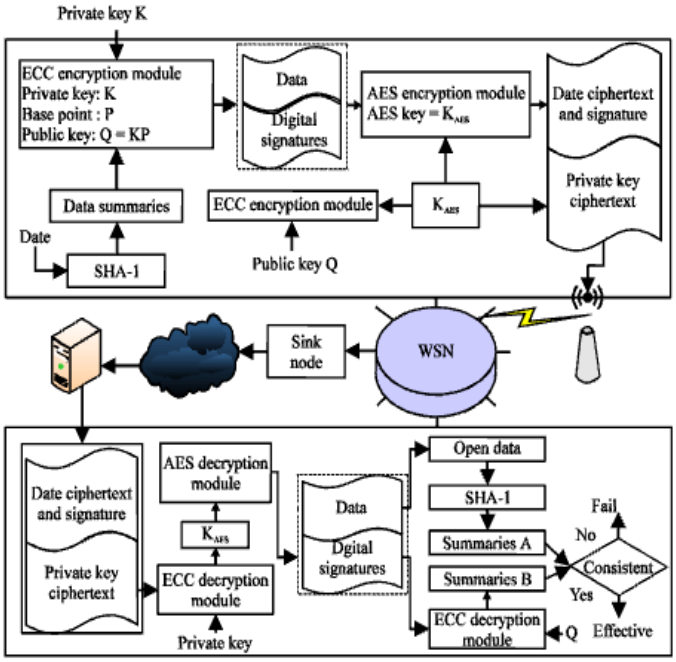

Fig -3 AES-ECC hybrid encryption system

The existing framework of the hybrid encryption scheme allows for only one way key encapsulation. That is, the AES key is protected by encrypting it with the ECC key. This necessitates periodic updation of AES key and ECC public key without increase in complexity and also cross encryption of AES and ECC keys with one another. The improved AES-ECC Hybrid encryption scheme is shown in fig 3.

4. CONCLUSIONS

This paper implemented the different method to improve the lifetime of network. A relocate-able sink is one approach to enhance the lifetime of network but still it have its own limitations as sink relocation involves more energy so we have proposed alternate shortest path technique which optimizes all nodes in the network system also enhances lifetime of network by limiting the number of sink relocating actions. In addition, we also proposed secure data sending and node authentication for communication purpose. In future, we can increase lifetime of a network. Also can secure the network by providing security.

REFERENCES

[1] G. S. Sara and D. Sridharan, Routing in mobile wireless sensor network: A survey, Telecommun. Syst., Aug. 2013.

[2] A.A. Somasundara, A. Kansal, D. D. Jea, D. Estrin, and M. B. Srivastavam, Controllably mobile infrastructure for low energy embedded networks, IEEE Trans. Mobile Comput., vol. 5, no. 8, pp. 958973, Aug. 2006.

[3] H. Mousavi, A. Nayyeri, N. Yazani, and C. Lucas, Energy conserving movement-assisted deployment of ad hoc sensor networks, IEEE Commun. Lett., vol. 10, no. 4, pp. 269271, Apr. 2006.

[4] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E.Cayiric, Wireless sensor networks: A survey, Comput.Netw., vol. 38, no. 4, pp. 393422, Mar. 2002.

[5] N. Jain and D. P. Agrawal, Current trends in wireless sensor network design, Int. J. Distrib. Sensor Netw., vol.1, no. 1, pp. 101122, 2005.

[6] D. Tian and N. D. Georganas, A node scheduling scheme for energy conservation in large wireless sensor networks, Wireless Commun. Mobile Comput., vol. 3, no. 2, pp. 271290, Mar. 2003.

[7] X. Hong, M. Gerla, W. Hanbiao, and L. Clare, Load balanced energyaware communications for Mars sensor networks, in Proc. IEEE Aerosp. Conf., vol. 3. May 2002, pp. 11091115.

[8] S. C. Huang and R. H. Jan, Energy-aware, load balancedrouting schemes for sensor networks, in Proc. 10th Int.Conf. Parallel Distrib. Syst., Jul. 2004, pp. 419425.

[9] R. C. Shah and J. Rabaey, Energy aware routing for lowenergy ad hoc sensor networks, in Proc. IEEE WirelessCommun. Netw. Conf., vol. 1. Mar. 2002, pp. 350355.

[10] G. L.Wang, G. H. Cao, and T. L. Porta, Movement-assistedsensor deployment, in Proc. IEEE Inf. Commun. Conf.,Aug. 2004, pp. 24692479.

[11] Bing Ji, Liejun Wang and Qinghua Yang, 2015. New Version of AES-ECC Encryption System Based on FPGA in WSNs. *Journal of Software Engineering, 9: 87-95.*

[12] A Arjuna Rao1 , K Sujatha1 , A Bhavana Deepthi1 , L V Rajesh1 1 Miracle Educational Society Group of Institutions, Bhogapuram, Vizianagram, India , Survey paper comparing ECC with RSA, AES and Blowfish Algorithms, IJRITCC | January 2017, http://www.ijritcc.org

BIOGRAPHIES

Kajal K. Kapoor received the B.E. and M.Tech. degrees in Computer Science and Engineering from Yeshwantrao Chavan College of Engineering and Bapurao Deshmukh College of Engineering, Wardha in 2009 and 2014, respectively. She is currently working as assistant professor in Computer Engineering Department in MITCOE,Pune.

Sujata S. Wakchaure received the B.E. and M.E. degrees in Computer Science and Engineering from Amrutvahini College of Engineering, Sangamner and JSPM College of Engineering, Pune in 2009 and 2014, respectively. She is currently working as assistant professor in Computer Engineering Department in MITCOE,Pune.