Implementation of Secure Energy Efficient Network Priority Routing (SEENPR) Protocol with Secure Key Management in WSN

Anil.G.L, J L Mazher Iqbal

Abstract*— *Wireless sensor networks (WSNs) consist of sensor nodes, which act as source and link nodes through which the data forward to sink node. However, the nodes in network have limited computation complexity, transmission capability and restricted battery life. Several routing protocols are available to improve the performance of network but very few concentrates on security issues. The performance of routing and security protocol in WSN affect due to unreliable low power links, insecure communication, threats, and resource limitations which limits the design of an efficient routing and security algorithm in wireless sensor networks. In this paper, we propose a secure energy efficient routing protocol with effective data collection and key management in dynamic WSN. The routing protocol prolongs network lifetime and minimizes energy consumption. The routing protocol implement with A* algorithm and security improve with EECLDSA (Enhanced Elliptic Curve Logic Discrete Algorithm). The combined Secure Energy Efficient Network Priority Routing (SEENPR) apply for effective data collection and key management in WSNs. SEENPR uses k-means algorithm to improve cluster head (CH) selection using Euclidean distance. The SEENPR implement in testbed to evaluate performance with respect to security and key management.

Keywords* –*Secure Energy efficiency, K-means clustering, Key management, Security, EECLDSA

I. INTRODUCTION

Wireless Sensor technology plays a vital role in industrial automation processes, surveillance and various real time applications. Thus, Wireless sensor networks (WSN) generates a growing interest in industrial and research perspectives. In general, WSN consists of a collaboration of sensor nodes with high computation, distributed sensing and effective communication in a secured way. WSN networking enables communication between two remote nodes and shares information about surrounding environment with an objective of collecting and routing information through link nodes to base station (BS). In WSN, nodes organize in cluster form to gather data from sensor nodes in its cluster. The cluster head then transmits data to adjacent cluster head node, to be delivered to sink [1]. In addition, sensor nodes relay information received from neighbor nodes and transmits data to sink node following some routing decisions. Thereby, sensor nodes act as data originators and data routers. Unreliable data, power links and resource limitations place a constraint in designing an efficient routing algorithm for wireless networks [2]. Hence, optimum care needs to be taken in designing routing protocol, which reduces computation complexity, resource utilization and data loss. Hence, Multi path routing is devised to improve throughput and reliability of data transmitted in network.

Routing procedures depend on design objectives and differ among various applications of WSN. WSN nodes have constriction with respect to energy, computation complexity and memory. Routing protocols were designed to enhance energy efficiency with minimal sacrifice to network parameters such as throughput, end-to-end delay [3]. Energy is a crucial factor which determines network lifetime in WSN. Many routing protocol focuses on energy reduction and lifetime maximization of the network [4]. Proper protocol selection is a key in minimizing unnecessary energy consumption in the network and to make secure data transmissions from the sensor nodes to the base station.

The Architecture of WSN is shown in figure 1. In the wireless sensor network, each sensor node possesses a sensing element, an ADC converter, processing unit, transceiver unit and power unit. Energy expenditure is distributed over various operations such as message reception, message transmission and idle listening [5]. Hence, the designed protocol should consider the energy levels of active nodes or a successful way of utilizing the energy of sensor nodes in the network. Most of the sensor nodes are battery operated and have limited lifetime. Prolonging the lifetime of the sensor nodes is highly crucial. Moreover, sensor nodes may be in hostile environments where replacement of failed nodes is a big task. Therefore, routing protocol has to be designed with an idea of extending the lifetime of the network and energy saving. In the proposed method, the sensor nodes are gathered to form clusters. The data from each node is encrypted with EECLDSA and K-means clustering algorithm. The cluster head is elected for each cluster with K-means clustering algorithm, which considers distance between nodes in cluster. The keys are generated by EECLDSA algorithm to encrypt data flowing between nodes in network clusters.

Revised Version Manuscript Received on 10, September 2019.

Anil.G.L, Research scholar, Department of ECE, Veltech Rangarajan, Dr Sagunthala R&D Institute of Science and Technology Chennai, Tamil Nadu, India.(Email: anilluciageorge@gmail.com)

Dr.J L Mazher Iqbal, Professor, Department of ECE, Veltech Rangarajan, Dr Sagunthala R&D Institute of Science and Technology Chennai, Tamil Nadu, India.(Email: mazheriq@gmail.com)

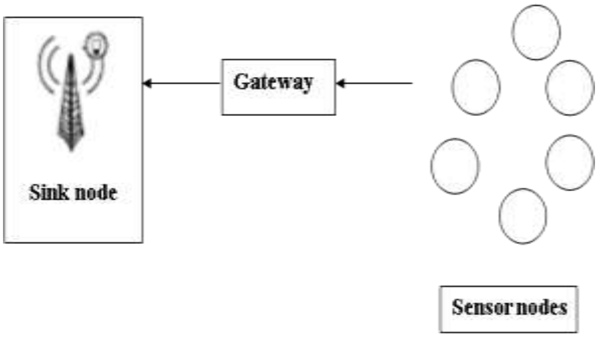


Figure 1: Architecture of Wireless Sensor Network

The paper is organized as follows, Section 2 reviews about the related works. Section 3 describes the problem statement. Section 4 illustrates the proposed method, which also presents network model and radio energy dissipation model. Section 5 depicted the proposed algorithm, simulation and hardware setup. Comparison results with existing methods are graphically represented in section 6 and concluded the paper in section 7.

II. RELATED WORKS

The transmission power level and size of data packet are factors, which influence life time of network [6]. The reduction in packet size transmission minimizes bit error rate and minimizes number of retransmissions in network there by improving network lifetime. Fragmenting the packet size into several packets increases energy dissipation However a tradeoff exist between size of data packet and energy efficiency. When transmission power level increases, the probability of packet loss decreases. Hence, appropriate selection of packet size and transmitting power overcomes the difficulty in optimization and increases network lifetime. WSN link layer with Mica2 nodes energy dissipation features is used in design of Mixed Integer Programming (MIP) system to optimize transmission power level and packet size. The lifetime of network in wireless sensor networks reduces due to communication load and overhead in sensor nodes [7]. Furthermore, the lifetime of network improves with appropriate Topology implementation in Cluster based WSN. The hierarchical design conserves energy in WSN in which node with more residual energy accumulates and route the data. Many of the nodes work on two-layer hierarchy but only few work with three-layer hierarchy. The semi-distributed clustering technique combines central gridding and distributed clustering to select upper –level and lower-level cluster head (CH) respectively. The lifetime of WSN depends on sensor node's operation with respect to communication range, computation complexity and size of data transmission [8]. Clustering approach improves network lifetime and energy efficiency [9]. A fuzzy based energy-aware clustering approach carried was used to carry out cooperative communication to overcome the issue of energy consumption. In cooperative communication, selection of cluster head is based on SNR, residual energy, trust and load. Intra-cluster routing uses network coding based on probabilistic routing system.

Energy efficiency compressive sensing based clustering algorithm (EECSR) was proposed by [10]. It possesses the merits of clustering and compressive sensing protocols. EECSR is used to maintain optimum size of the cluster and also maintains relationship between adjacent layers. Hot spot problem can be overruled by randomly modifying the functions of cluster head and to change cluster head into backup cluster head. Performance of EECSR is compared with the conventional clustering protocols. Data aggregation function wasw used to collect sensed data from sensor nodes in intermedicate location [11]. The technique helps in reducing data packets transferred in network. The data aggregation was perfomed with various protocols. Cluster chain mobile agent routing protocol (CCMAR) was developed by merging merits of LEACH and PEGASIS protocol. CCMAR also breaks network into smaller clusters and execute in two phases. The simulated results show that (CCMAR) provides higher efficiency than existing routing protocols. The lifetime of network improve by maintaining higher energy efficiency [12]. Usually, the sensor nodes collect sensed data and route it to sink node. The main motive in developing new routing algorithm is to minimize transmission delay and power consumption in network. Clusters are created and CH select based on energy consumption and delay. So, routing algorithm was developed to maintain low cost communication link between the cluster head and the sink node. The performance parameters of hybrid routing were compared with the conventional techniques. Two clustering protocols implement [13] to maximize lifetime of Wireless Sensor Network. Cluster head was selected based on remaining energy of nodes in cluster and mean power of cluster in Single-hop energy efficient clustering protocol (S-EECP). Node with maximum residual energy select as CH than minimum residual energy node. However, CH route data packets to BS by multiple hops in Multi-hop energy efficient clustering protocol (M-EECP). A Regional Energy Aware Clustering (REAC-IN) technique with isolated nodes was implemented to select CH on the basis of weight [14]. Weight calculation was done on basis of residual and regional mean energy of all nodes in all clusters. REAC-IN performance was compared with the existing methods such as Low Energy Adaptive Clustering Hierarchy (LEACH), Hybrid Energy Efficient Distributed Clustering (HEED) and Distributed Energy Efficient Clustering (DEEC) using various simulation parameters. A delay-constrained energy multi-hop (DCEM) routing apply in WSNs [15]. Trade-off between two goals in the design of reducing energy consumption and delay was examined. Distributed clustering algorithm defines best CH for every cluster was used. Multi-hop routing algorithms apply to route sensed data from CHs to BS at low energy cost. Simulation parameters were compared with existing protocols dealing with delay and energy consumption. A PEGASIS-DSR enhanced Routing Protocol (PDORP) combines features of routing protocols such as Power Efficient Gathering Sensor Information System (PEGASIS) and Dynamic Source Routing (DSR) [16]. Further, hybridization of Genetic Algorithm (GA) and Bacterial Foraging Optimization (BFO) was used to discover an energy efficient optimum route. The parameters of existing method such as PEGASIS, LEACH, DSR and OD-PRRP were compared in terms of delay, bit error rate, energy consumption and throughput.

III. PROBLEM STATEMENT

In WSN, lifetime of network determine by total energy consumed by nodes. Therefore, nodes are grouped into clusters, in which CHs collect the data. Security is one of the most important issues in WSN. Security is mostly used feature, which incorporates the features of authentication, integrity, privacy, nonrepudiation and anti – playback which is important in hospital wireless data management system. The proposed method EECLDSA algorithm applies for security purpose in cluster head**.**

IV. PROPOSED METHODOLOGY & RESULTS

The flow chart of Secure Energy Efficient Clustering Protocol is shown in Figure 2. Several clusters are formed and then a cluster head (CH) is assigned for each cluster. Nodes in the network are grouped into clusters by calculating distance of each node from centroid position of cluster head. EECLDSA algorithm is applied to each cluster head for security. Each time a key is generated for each cluster and the data is transmitted from one CH to other CH and then it is forwarded to the base station till it reaches the sink. The objective of the proposed approach is

1. To design Secure Energy Efficient Clustering protocol using K-means and EECLDSA Key management protocol.
2. To reduce energy consumption and end-to-end delay in network.

4.1. Network Model With Radio Energy Dissipation Model

WSN comprises lower number of high-end nodes and large number of low-end nodes, which act as CH and sensor nodes respectively. CH performs more computation than the sensor nodes with limited capability. The static base station receives data from cluster heads and aggregates them. Sensor node transmits the sensed data to CH, which accumulates the received data and forwards it to BS using EECLDSA algorithm. Every sensor nodes is identified by a unique ID and key, which will get updated for each transmission using key management technique.

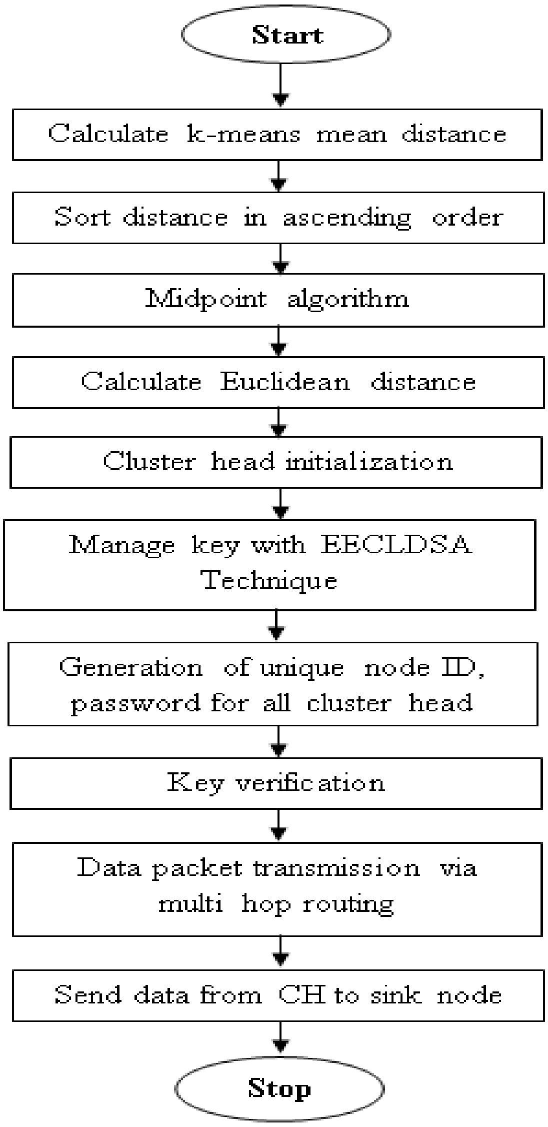

Start
Calculate k-means mean distance
Sort distance in ascending order
Midpoint algorithm
Calculate Euclidean distance
Cluster head initialization
Manage key with EECLDSA Technique
Generation of unique node ID, password for all cluster head
Key verification
Data packet transmission via multi hop routing
Send data from CH to sink node
Stop

Figure 2: Flow chart of the proposed model

V. SEENPR –LEACH WITH SECURE KEY MANAGEMENT USING EECLDSA

The SEENPR involves two algorithms such as K-means Clustering algorithm and EECLDSA. K-means Clustering algorithm is used to select CH for each cluster based on distance from the origin whereas EECLDSA helps in key generation for each cluster to ensure security of the network and for key updating for each transaction of data.

5.1. k-means clustering algorithm

According to K-means clustering algorithm, Clusters rely on selection of initial cluster centroids. The clustering algorithm classifies data set as K number of disjoint clusters. This clustering algorithm comprises of two separate stages. The initial stage is to describe K centroid and then second stage is to take every point belonging to a given node and links to adjacent centroid node. The distance is calculated between nodes by Euclidean distance formula. Data elements having fewer distances to centroids are moved to suitable cluster. The Euclidean distance is calculated as follows,

$$D(M,N) = \sqrt{(m_1 - n_1)^2 + (m_2 - n_2)^2 + \ldots + (m_x - n_x)^2} \quad (1)$$

Where, D(*M*,*N*) represent Euclidean distance between two nodes

K-means clustering algorithm performs as follows:

K-means clustering algorithm is performed by selecting an integer from the clusters of interest. Then, K preliminary points selected to estimate cluster centroids to act as initial starting values. Every point in the dataset analyzed to assign it to various cluster groups based on the nearest centroid value. After assigning all the points in the dataset to a cluster, new centroids calculated and it is repeated till the centroid remains static or if there is no obligation in cluster formation.

Initialize the number of nodes to be N and number of cluster head to be CH. The distance from origin to every node in a particular region calculated. Mean value sorted to divide into equal groups. For each group one centroid is assumed and the Euclidean distance calculated from the selected centroid to each node. If the Euclidean distance exceeds threshold, then it is considered as cluster head otherwise again the mean value will be sorted to form new groups.

5.2. key management with eecldsa algorithm

Secure key management is ensured by EECLDSA algorithm. The security key is generated and maintained between the nodes throughout the lifetime of wireless sensor network. Data authentication, integrity, digital signature involves the use of key to transmit data in a secured way.

Each CH carries out EECLDSA algorithm. The CH sends request, which comprises of key and CH node ID. BS validates ID received from all CHs with the database to avoid any fraudulent user. CH always stores a database of its ID and centroid distance of every sensor network. A key generated for each transaction and it will get updated each time a data crosses one CH to other and the change in the node status will be updated to BS.

It is essential to generate a public key Q and it entirely depends on the trust value generated at the initial stage i.e. Q=K to authenticate the system. An important rule is that Q should lie on the elliptical curve. If Q is found invalid then the node will be skipped or it goes for another check. Where m represents maximum number of bits in public key Q. XOR operation is performed between the bits m and k, using SHA-1 a 160 bit hash function. Convolution operation carried out to generate a private key, s to restrict unauthorized access if the key doesn't match with the public key.

Algorithm: 2 EECLDSA

Step 1: Node 'A' generates parameters from elliptic curves.

Step 2: Node 'A' uses elliptic curve parameter to produce cipher text with division polynomial multiplication as below.

[Input text] [elliptic curve parameter] mod c = encoded message.

```
Encrypt(){
        plaintext = document.getElementById("p").value.toLowerCase().replace(/[^a-z]/g, "");
        k = document.getElementById("k").value.toLowerCase().replace(/[^0-9 ]/g, "");
        keys = k.split(" ");
        // do some error checking
        if(plaintext.length < 1){ alert("please enter some plaintext (letters and numbers only)"); return; }
        if(plaintext.length % 2 == 1){ plaintext = plaintext + "x"; }
        if(keys.length != 4){ alert("key should consist of 4 integers"); return; }
        for(i=0;i<4;i++) keys[i] = keys[i]%26;
        ciphertext="";
        for(i=0; i<plaintext.length; i+=2){
        ciphertext += String.fromCharCode((keys[0]*(plaintext.charCodeAt(i)-97) + keys[1]*(plaintext.charCodeAt(i+1)-97))%26 + 97);
        ciphertext += String.fromCharCode((keys[2]*(plaintext.charCodeAt(i)-97) + keys[3]*(plaintext.charCodeAt(i+1)-97))%26 + 97);
        }
        document.getElementById("c").value = ciphertext;
```

Step 3: The encoded message decode with inverse elliptic curve parameter as below

[elliptic curve parameter] $^{-1}$ mod c = decoded message.

```
Decrypt(){
    ciphertext = document.getElementById("c").value.toLowerCase().replace(/[^a-z]/g, "");
    k = document.getElementById("k").value.toLowerCase().replace(/[^0-9 ]/g, "");
    keys = k.split(" ");
    // do some error checking
    if(ciphertext.length < 1){ alert("please enter some ciphertext (letters only, numbers should be spelled)"); return; }
    if(ciphertext.length % 2 == 1){ alert("ciphertext is not divisible by 2 (wrong algorithm?)"); return; }
    if(keys.length != 4){ alert("key should consist of 4 integers"); return; }
    for(i=0;i<4;i++) keys[i] = keys[i]%26;
    // calc inv matrix
    det = keys[0]*keys[3] - keys[1]*keys[2];
    det = ((det%26)+26)%26;
    di=0;
    for(i=0;i<26;i++){
```

```
if((det*i)%26 == 1) di = i; }
        if(di == 0){alert("could not invert, try different key"); return; }
        ikeys = new Array(4);
        ikeys[0] = (di*keys[3])%26; ikeys[1] = (-1*di*keys[1])%26;
        ikeys[2] = (-1*di*keys[2])%26; ikeys[3] = di*keys[0];
        for(i=0;i<4;i++){ if(ikeys[i] < 0) ikeys[i] += 26; }
        plaintext="";
        for(i=0; i<ciphertext.length; i+=2){
          plaintext += String.fromCharCode((ikeys[0]*(ciphertext.charCodeAt(i)-97) + ikeys[1]*(ciphertext.charCodeAt(i+1)-97))%26 + 97);
          plaintext += String.fromCharCode((ikeys[2]*(ciphertext.charCodeAt(i)-97) + ikeys[3]*(ciphertext.charCodeAt(i+1)-97))%26 + 97);
        }
        document.getElementById("p").value = plaintext;
    }
```

5.3. hardware setup

The Secure Energy Efficient Network Priority Routing (SEENPR) Algorithm, which comprises of Enhanced Elliptic Curve Logic Discrete Algorithm implement in hardware to evaluate algorithm performance in testbed. The test bed is implemented with PIC16F877A microcontroller and Tarang wireless transceiver module. The module is built with 8-bit microcontroller, 9V battery and Tarang transreceiver. PIC microcontroller has 2k words of program memory and 128 bytes of RAM. PIC 16F877a has a maximum operating frequency of 20 MHz to drive the microcontroller and to produce clock pulses which in turn is connected to the tarang transreceiver through a Max232 level converter. Max232 makes TTL logic CMOS compatible for tarang module. Tarang modules are designed with low to medium transmit power for wireless networks with high reliability. Modules need less power to deliver the data efficiently between devices. The interfaces between modules are applicable in several industrial applications. The modules work within ISM 2.4-2.4835 GHz frequency band with IEEE 802.15.4 baseband.

VI. TESTBED PERFORMANCE ANALYSIS

6.1. Energy consumption

Energy Consumption of node is the total energy utilized for data transmission and node operation. The total energy utilization is related to aggregate number of packets delivered in WSN. The energy consumption for SEENPR algorithm in network is low compared to other algorithm such as reputation-based trust management framework (RFSN), dynamic trust management system (DTMS) an Efficient and Secure Routing Protocol (ESRPSDC). The energy consumption in the network was measured for different number of nodes in network. Figure 3 shows the proposed algorithm consumes less energy than existing methods. The energy consumption was measured by increasing the number of nodes in the network. The network evaluate for energy consumption with 5 nodes. The energy consumption of network was 35 joules whereas the network operating under RFSN, DTMS and ESRPDC consumed 30, 28 and 25 joules respectively.

In RFSN, DTMS and ESRPSDC algorithms, the energy level decreases when the time taken to transmit a packet decreases. But in A*SEENPR algorithm, the energy level increases when the time taken to transmit a packet decreases.

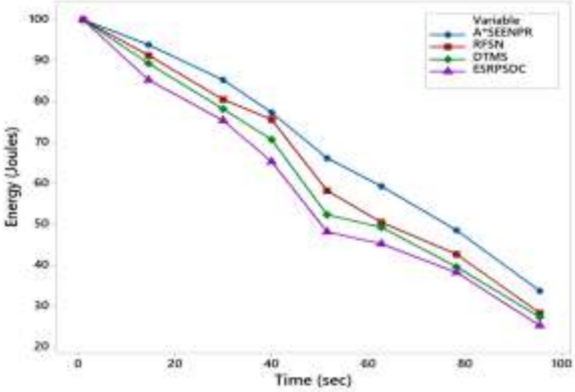


Figure 3: Energy Level for A*SEENPR algorithm Vs RFSN, DTMS and ESRPSDC algorithms

6.2. End To End Delay

Delay is the total time taken for transmission of data packets and it is a crucial factor in WSN. Delay may be caused due to transmission delay, queuing delay, propagation delay and processing delay. From the clustering technique, all the packets were easily transmitted to their respective cluster head within short period. It is confirmed that the SEENPR has minimum end to end delay when compared to existing approach as shown in figure 4. The delay is reduced in SEENPR algorithm as it transmits data to destination node based on Euclidean distance instead of transmitting the data via adjacent nodes in other algorithm. The SEENPR algorithm generates maximum delay of 20 ms but the existing protocols like RFSN, ESRPSDC and DTMS generates delay about 32, 80 and 90 ms delay in the WSN respectively. The delay measure for different number of nodes as shown in figure 4. The delay calculates with

delay[i] = receiving time[i] – sending time[i] (9)
Total Delay = Total Delay + delay[i] (2)
Average Delay = Total Delay / count

Where,
i = packet sequence number
count = Total packet count

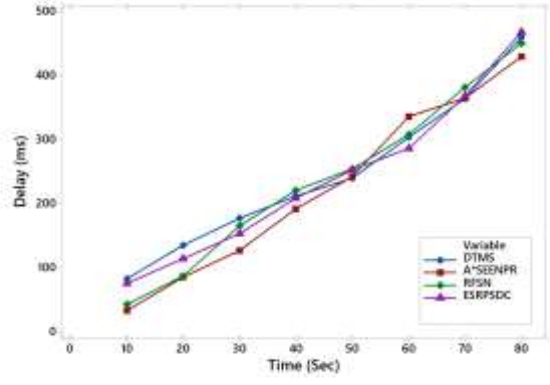


Figure 4: End-To-End Delay for A*SEENPR algorithm Vs DTMS, RFSN and ESRPSDC algorithms

6.3 Packet Delivery Ratio

PDR is well-defined as ratio of successfully delivered data packets to destinations. The packet delivery ratio estimates with

Packet delivery ratio = received packets/generated packets*100 (3)

Figure 5 shows the packet delivery ratio for DTMS, RFSN and ESRPSDC algorithms compared to A*SEENPR algorithm. SEENPR algorithm achieves a packet delivery ratio of 9.8% whereas the existing algorithms like RFSN, DTMS, ESRPDC achieves around 8% of the delivery ratio. In this technique, huge number of packets was received, which is used to achieve maximum throughput. So, it has a highest packet delivery ratio than existing methods.

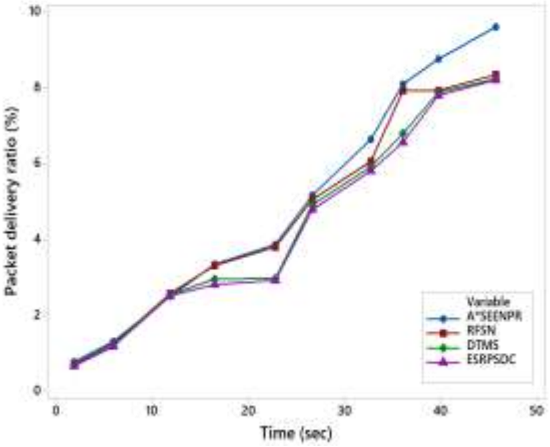


Figure 5: Packet Delivery Ratio for A*SEENPR algorithm Vs DTMS, RFSN and ESRPDC algorithms

6.4 Packet Loss Ratio

Packet loss is the failure of one or more transmitted packets to arrive at their destination. Packet loss minimizes the Packet Delivery Ratio. Packet loss cause due to number of factors including signal degradation over the network medium and multi-path fading. Figure 6 shows Packet Loss Ratio for RFSN, DTMS and ESRPSDC algorithms compared to A*SEENPR algorithm. SEENPR algorithm achieves 8% of packet loss ratio but existing techniques such as RFSN, ESRPDC and DTMS achieves 9.5%, 10% and 11% packet loss ratio. In RFSN, DTMS and ESRPSDC algorithms, the packet loss ratio increases with respect to packet size in network. However, in A*SEENPR algorithm, the packet loss ratio decreases marginally with respect to data packets in network.

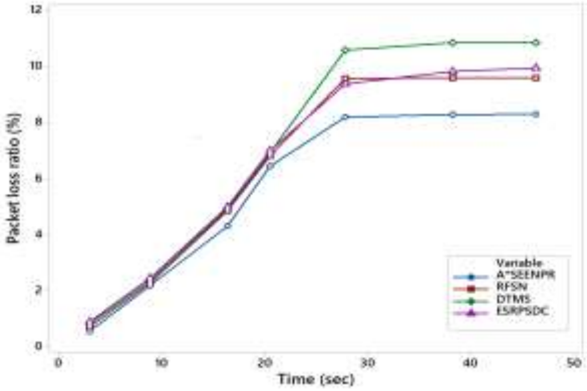


Figure 6: Packet Loss Ratio for A*SEENPR algorithm Vs RFSN, ESRPSDC and DTMS algorithms

6.5 Throghput

Network throughput, a performance metric use to measure the number of packets per second received at the destination. Throughput measures the effectiveness of a protocol which is often of great concern for researchers in measuring maximum data throughput in bits per second of a link. Throughput is intended as average rate of successful messages delivered over the network. The throughput increases since, the packet loss in network is minimized due to clustering of nodes in network. In cluster all the nodes wait for the cluster head request signal to transmit data. Hence, the data collision and packet loss among nodes in cluster is eliminated resulting in increased throughput. The throughput calculates with

Throughput = received data*8/Data Transmission Period (4)

Figure 7 shows throughput for RFSN, DTMS and ESRPSDC algorithms compared to A*SEENPR algorithm. From figure 7, the SEENPR algorithm achieves maximum throughput of 1900 kbps when time taken to transmit a packet increases. But in RFSN, DTMS and ESRPDC throughput is 1800, 1600 and 1500kbps. In RFSN, DTMS and ESRPSDC algorithms, the throughput decreases as the number of transmitted packets increase. But in A*SEENPR algorithm, the throughput increases with respect to packet size.

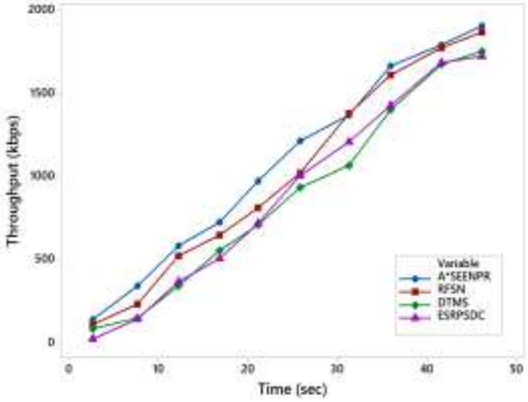


Figure 7: Throughput for A*SEENPR algorithm Vs RFSN, DTMS and ESRPSDC algorithms

6.6 Computation Overhead

The amalgamation of excess or indirect computation time is known as Computation

Overhead, this includes memory and bandwidth of networks. It is the main problem of heterogeneous network. The A*SEENPR offers low computation overhead than existing methods. The computation overhead is minimized since; the computations are performed by cluster head instead of all the nodes in network. The overhead calculates with

Routing Overhead = Routing Packets Count (5)

Figure 8 shows the Overhead for DTMS, RFSN and ESRPSDC algorithms compared to A*SEENPR algorithm. In SEENPR algorithm, the overhead is about 0.85 kb. The same overhead is achieved in DTMS also but in RFSN and ESRPDC, overhead is only 0.6 kb. In DTMS, RFSN and ESRPSDC algorithm, the overhead is low compared to other algorithm. The overhead increase in network during data transmission.

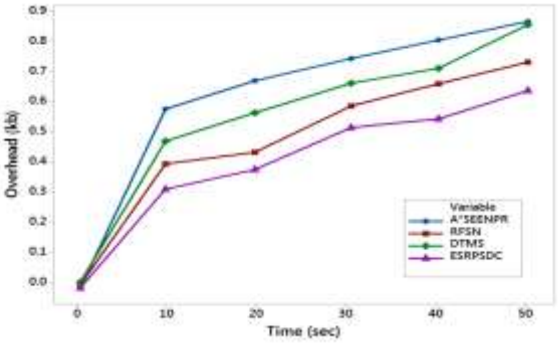
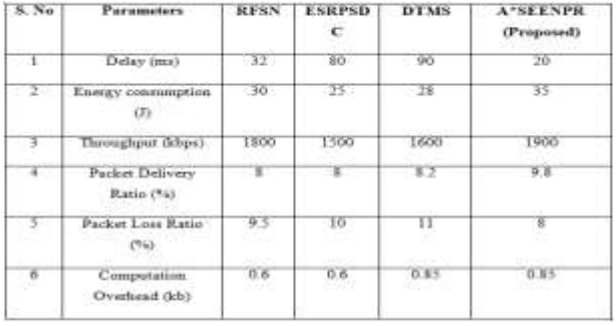


Figure 8 Overhead for A*SEENPR algorithm Vs DTMS, RFSN and ESRPSDC algorithms

The proposed SEENPR protocol is compared with existing protocol such as RFSN, DTMS and ESRPSDC as shown above in the graphical representation.

Table 1 shows the performance comparison of proposed A*SEENPR with RFSN, DTMS and ESRPSDC with respect to parameter such as delay, energy consumption, throughput, PDR and overhead. Similarly, the algorithm implement for different number of nodes for performance evaluation is shown in table 2.

Table 1. State-of-Art Performance Comparison.



S. No	Parameters	RFSN	ESRPSDC	DTMS	A*SEENPR (Proposed)
1	Delay (ms)	32	80	90	20
2	Energy consumption (J)	30	25	28	35
3	Throughput (kbps)	1800	1500	1600	1900
4	Packet Delivery Ratio (%)	8	8	8.2	9.8
5	Packet Loss Ratio (%)	9.5	10	11	8
6	Computation Overhead (kb)	0.6	0.6	0.85	0.85

Table 2: EECLDSA performance comparison.

No of nodes	Parameters	RFSN [17]	ESRPSDC [18]	DTMS [19]	A*SEENPR (Proposed)
100	Delay (ms)	**462**	**952**	**1038**	**325**
	Energy consumption (J)	**80**	**67**	**73**	**94**
	Throughput (kbps)	**4238**	**3958**	**4135**	**4452**
	Packet Delivery Ratio (%)	**75**	**78**	**82**	**95**
200	Delay (ms)	**752**	**1184**	**1388**	**579**
	Energy consumption (J)	**157**	**132**	**165**	**188**
	Throughput (kbps)	**8135**	**7254**	**8267**	**7515**
	Packet Delivery Ratio (%)	**142**	**164**	**168**	**184**

VII. CONCLUSION

The study presents a A*SEENPR algorithm with secure key management using Enhance Elliptic Curve Logic Discrete Secure Algorithm. The algorithm performance was evaluated via testbed implementation and network parameters such as energy consumption, end to end delay, packet delivery ratio, packet loss ratio, overhead and throughput were compared with the existing techniques such as DTMS, RFSN and ESRPDC. The algorithm minimizes overhead and increase throughput in network. The finding shows overhead of A*SEENPR algorithm was low compared to other existing techniques and throughput of network has increased compared to other algorithms.

REFERENCES

1. Waltenegus Dargie, Christian Poellabauer. Fundamentals of Wireless sensor Networks: Theory and Practice, Wiley series on Wireless communication and Mobile computing.
2. Deepti Gupta. (2015). Wireless Sensor Networks ‘Future trends and latest research challenges’. IOSR Journal of Electronics and Communication Engineering, e-ISSN 2278-2834, p-ISSN: 2278-8735, 10(2) Version II. 41-46.
3. Prabhat kumar (2012). ‘A review of routing protocol in Wireless Sensor Network’, International Journal of Engineering Research & Technology (IJERT), ISSN: 2278-0181, 1(4).
4. P.Hurni T.Braun (2008). ‘Energy-efficient multi-path routing in wireless sensor networks’ Proceedings of the 7th international conference on Ad-hoc, Mobile and Wireless networks, Springer-Verlang, 72-85.
5. Y.M.Lu and V.W.S. Wong (2007), ‘An energy-efficient multipath routing protocol for wireless sensor networks, International journal of communication systems, 20(7), 747-766.
6. Akbas, A. *et al.* (2016) ‘Joint Optimization of Transmission Power Level and Packet Size for WSN Lifetime Maximization’, *IEEE Sensors Journal*, pp. 5084–5094.
7. Lee, J. S. and Kao, T. Y. (2016) ‘An Improved Three-Layer Low-Energy Adaptive Clustering Hierarchy for Wireless Sensor Networks’, *IEEE Internet of Things Journal*, pp. 951–958.
8. Karakus, C., Gurbuz, A. C. and Tavli, B. (2013) ‘Analysis of energy efficiency of compressive sensing in wireless sensor networks’, *IEEE Sensors Journal*, pp. 1999–2008.
9. Akila, I. S. and Venkatesan, R. (2016) ‘A fuzzy based energy-aware clustering architecture for cooperative communication in WSN’, *Computer Journal*, pp. 1551–1562.
10. Wang, Q. *et al.* (2019) ‘An Energy-Efficient Compressive Sensing-Based Clustering Routing Protocol for WSNs’, *IEEE Sensors Journal*. IEEE, pp. 3950–3960.
11. Sasirekha, S. and Swamynathan, S. (2017) ‘Cluster-chain mobile agent routing algorithm for efficient data aggregation in wireless sensor network’, *Journal of Communications and Networks*, pp. 392–401.
12. Lee, J. S. and Kao, T. Y. (2016) ‘An Improved Three-Layer Low-Energy Adaptive Clustering Hierarchy for Wireless Sensor Networks’, *IEEE Internet of Things Journal*, pp. 951–958.
13. Kumar, D. (2014) ‘Performance analysis of energy efficient clustering protocols for maximising lifetime of wireless sensor networks’, *IET Wireless Sensor Systems*, pp. 9–16.

14. Santar Pal singh, SC Sharma. (2015). A survey on Broadcasting Routing Protocol in Wireless Sensor Networks. Procedia Computer science. 687-695.
15. Seo, S. H., Won, J., Sultana, S., &Bertino, E. (2015). Effective key management in dynamic wireless sensor networks. *IEEE Transactions on Information Forensics andSecurity*, *10*(2), 371-383.
16. Khan, T. F., &Sivakumar, D. (2014, July). Performance of AODV, DSDV and DSR protocols in mobile wireless mesh networks. In *Current Trends in EngineeringandTechnology (ICCTET), 2014 2nd International Conference on* (pp. 397-399). IEEE.
17. Xie, G., & Pan, F. (2016). Cluster-based routing for the mobile sink in wireless sensor networks with obstacles. *IEEE Access*, *4*, 2019-2028.
18. Poornima, A. S., &Amberker, B. B. (2011). Secure data collection using mobile data collector in clustered wireless sensor networks. *IET wireless sensor systems*, *1*(2), 85-95.
19. Z. Ye, T. Wen, Z. Liu, X. Song, and C. Fu, "An Efficient Dynamic Trust Evaluation Model for Wireless Sensor Networks," *J. sensors*, vol. 1, no. 2, pp. 1–17, 2017.
20. R. A. S.Ganesh, "Efficient and Secure Routing Protocol for Wireless Sensor Networks through SNR based Dynamic Clustering Mechanisms," *J. Commun. Networks*, vol. 15, no. 4, pp. 422–429, 2013.
21. X. Dai, C. Zhu, and Y. Guo, "P2P Dynamic Trust Management System Based on Trust Network," *2012 Int. Conf. Cyber Secur. Cyber Warf. Digit. Forensic*, vol. 1, no. 2, pp. 165–170, 2012.