Lightweight & Energy Efficient Secure Data Transmission in WSN

Sangamesh J.Kalyane
Department of Computer Science, Bheemanna Khandre Institute of Technology,
Bhalki-585328 Email: kalyanesangamesh@gmail.com
Dr.Nagaraj B.Patil
Principal, Government College of Engineering, Gangavati - 583227
Email: nagrajbpatil1974@gmail.com

ABSTRACT

In current days an effective design of WSN has became a leading area of research with the wide application of WSN, data transmission in network becoming a more hot research topic. The biggest challenge is to transmit the data from source to sink node securely. The main disadvantage in WSN is they have limited resources, cluster network have been proposed by many researchers to reduce the energy load & reduces the overhead in the network to increase the network life time.

The SLEACH is the modified version of LEACH is a clustering selection method that provides an effective way to minimize the energy utilization along with providing security to the WSN, but still energy efficient for SLEACH is not up to the mark and it doesn't guarantee confidentiality, availability and secure transmission of data from one end to another end. This paper introduces a lightweight Secure data authentication scheme (LWSDAS) which is based on Elliptic curve cryptography (ECC) to provide integrity, confidentiality, authentication & data aggregation and it is also capable to protect against attacks .The proposed work is more energy efficient over SLEACH. The results of simulation shows that the proposed work is more advantageous than SLEACH, considering parameter like end to end delay ,energy overhead, packet delivery ratio and overall it is up to 7-10% far better than SLEACH algorithm.

Keywords - WSN, SLEACH, Clustered, Elliptic curve cryptography (ECC), Lightweight polynomial secret key (LWPK).

Date of Submission: Sep 11, 2019 Date of Acceptance: Sep 26, 2019

I. INTRODUCTION

WSN are highly distributed, lightweight and low powered devices called motes. WSNs are spatially appropriated self- governing sensors to screen physical or ecological conditions like, temperature, sound, weight, etc. Sensor network consist of sensor nodes which consist of sensor sub system, processing system and communication system.WSN provides bridge between physical & virtual world. Sensors are energy efficient multi functional wireless devices, sensors are communicated with each other through transceivers. In much live application the sensor nodes are achieving different functions like discovery of neighbor node, smart discover, storage of data, assembling of data, target trace, controlling & checking node location, & routing.

WSN are playing major job in multiple applications such as [2]. Battle field surveillance and target tracking, Patient diagnosis and monitoring, Environmental monitoring such as Air pressure, temperature, humidity level, Smart Home Appliances, Noise level for finding in particular area, Forest fire detection, Water quality checking, Commercial Applications.WSN consist of some characteristics includes: Sensor nodes are low power devices and it consist of limited memory and energy constraints due to small in size and ability to handle extreme environmental conditions and it is simple to use.

WSN provides some Advantages and Disadvantages. Why peoples liking WSN might be abbreviate as the following [3]:

1. Arrangement of network should be possible without fixed infrastructure. 2. It is fit for the remote area, for example, past the ocean, crest, profound backwoods. 3. Execution cost is less. 4. It keeps away from huge number of wirings. 5. WSN can suit new gadgets whenever. 6. WSN can be operate by a centralized monitor.

The drawback of WSN can be condensed as pursues [3]: 1.Not that much safe since the attackers may enter the access point and access all the data. 2. It is less slowness contrasted with a wired network. 3. It is progressively hard to set up contrasted with a wired network. 4. Communication of speed is comparatively low. 5. Cost is too high

In WSN providing security is one of the toughest job and care also be taken that they should not be traditional security techniques and along with security they should restrict power, communication and computation capability [4][5].

WSNs are insecure to different categories of attacks. These types of attacks are classified in WSN are [6]: Attacks on confidentiality, authentication & attack on network availability it is also called as denial-of-service(DOS) attacks. In WSN security is must to provide services like confidentiality of data, data integrity, data freshness, self- organization, and secure localization [7][8].

In WSN sensor nodes are communicate to BS station through single hop or multi hop transmission. The data is passed through intermediate nodes using verities of routing protocols.[1] These protocols for routing are split in to two types: Flat routing & Cluster based routing. Since sensor nods are energy constrained, so that cluster based is best routing protocol to boost the network life time rather than flat routing. In cluster based network nodes are assembled into clusters, the CH is assigned and its work is to send the messages from each node in the cluster to BS. A big challenge is how to provide better security to the data that can be send from one node to another node (CH to BS).The proposed technique is based on Low Energy Adaptive Clustering Hierarchy (LEACH) protocol.

LEACH is an energy-preserve routing protocol for WSNs. In LEACH sensor nodes design clusters and the cluster heads and these cluster head act as a routers for sink. This will rescue energy since the transmission will be complete by only CHs [9].

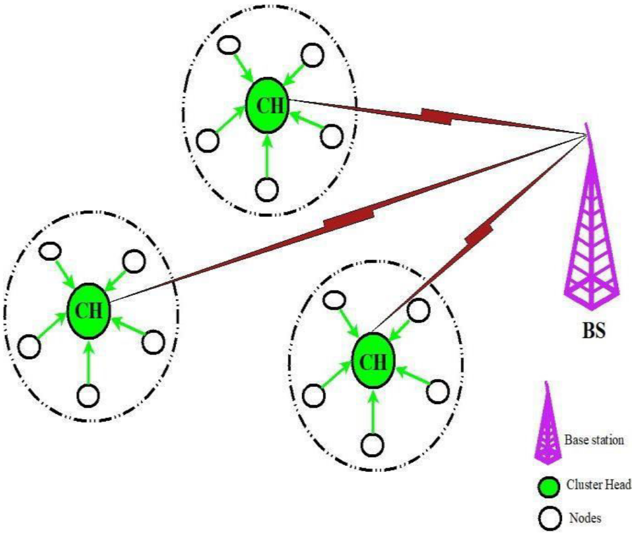


Fig 1.Cluster Formation

The selection of cluster head in LEACH protocol is done by two phases: 1. Setup phase. 2. Steady phase.

In setup phase if the number selected is less than predefined threshold than that node become cluster head (CH).

The threshold T can be determined as

$$\mathbf{T}(\mathbf{n}) <= \frac{(p+E0)}{(1=p*mod(r,round(\frac{1}{p}))},$$

where r is the number of rounds ,E0 initial energy value in network, p is the probability of selecting CH & in steady phase, nodes in cluster can send their data to the cluster head using a time division multiple access (TDMA) schedule. This TDMA allot time slots to every node. The CH gathers the data from cluster node and send it to the BS. In this paper providing better security to the LEACH for secure transmission of data over existing method (SLEACH) using Light weight secure data authentication Scheme (LWSDAS). The paper is organized as follows: Related work describes in section II. Section III describes the proposed work. Section IV shows results of simulation and comparison. Finally we conclude this paper in section V.

II. RELATED WORK

In WSN issue with security is the big challenge especially topic of network availability. Wireless sensor network can be secure from different attack that is related with confidentiality, integrity & availability. In [10] authors have come up with dynamic solution to recognize DoS attack. This Clarification acquires the plan of LEACH protocol and includes a new node. The network consist of three nodes namely sensing, analyzing & CH. The work of sensing nodes is to perform only sensing and work of cluster head is to perform the data collection, new nodes for analyzing nodes or control the congestion in cluster. In the event that action is unusual, at that point it is recognized, and makes a report to the CH by the controlling nodes. Controlling nodes can be choosing based on Multiplicative Linear Congruential Generators.

In [11] author discussed about some energy efficient protocols like data centric routing or flat type routing protocols. In case of data centric power utilization is restricted in many of the protocols where as in hierarchical routing power utilization is high, like LEACH, APTEEN, PEGASIS & TEEN.

In [12] author enhanced LEACH by proposed algorithm i.e. LEACH-I by reduce the energy usage of the network to expand the network life time.

W.Xiao-yun.[13] proposed Secure-Low Energy Adaptive Clustering Hierarchy (SLEACH) Protocol for WSN, to improve the security on cryptography based scheme to provide authentication, integrity.

Dong Chen. [14] Proposed a secrete sharing scheme based on congruence equations to move data securely from source node to the sink node .

Fares Mezrag.[15] proposed a modern stable protocol named as HCBS, which is based on LEACH. This stable protocol is constructed on the combination of cryptography method which is based on the Elliptic Curves to exchange the keys which uses symmetric keys for encryption of data and operations of MAC.

In [16] present the model of Secure LEACH, expansion of the LEACH protocol. By partitioning SLEACH into four stages and fit efficient cryptographic to create an effective protocol, then provided security review of SLEACH.

Some of Researchers [21] recommend that, to generate a several message authentication codes (MACs) for message authentication by utilizing the hash functions. These plans are extra powerful than the plan which depends on the public key cryptography (PKC), due to every secret key is mutual by different nodes. These plans turn into insufficient or even unusable if countless nodes are settlement with one another. Moreover these plans can't satisfy non-repudiation. The proposed technique is likewise computationally viable and disparate from these plans and also it can permit a huge number of node are compromises and it can also satisfy non repudiation.

III. PROPOSED WORK

We proposed a Lightweight Secure data authentication scheme (LWSDAS) which is based on improved polynomial (ECC) scheme required to eliminate scalability problem that is SDAS technique is used. SDAS transmit an unlimited data securely to reach the destination and provide sufficient security along with data aggregation and it is capable to protect against attacks. The main concept is to authenticate each message ‘m’ which is released by the source node and the authentication can be done at message sender.

The generation is based on the Modified Elgamal Signatures on Elliptic curves [17]. In ring signature, every ring member is needed to examine a fake signature for further members of the Anonymous set (A S). In proposed design, the complete SDAS generation requires three stages, which is connection to every non-senders and message sender to SDAS. SDAS is authenticate over a single equation without independently authenticate the signature.

A. System Model

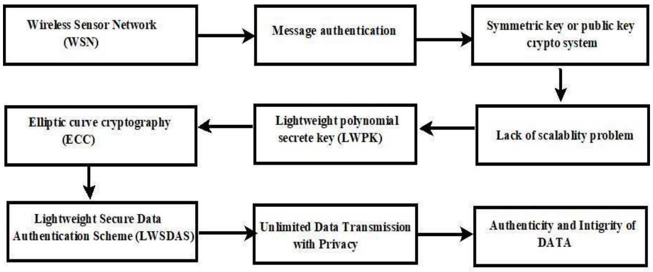

Wireless Sensor Network (WSN)
Message authentication
Symmetric key or public key crypto system
Lack of scalablity problem
Lightweight polynomial secrete key (LWPK)
Elliptic curve cryptography (ECC)
Lightweight Secure Data Authentication Scheme (LWSDAS)
Unlimited Data Transmission with Privacy
Authenticity and Intigrity of DATA

Fig 2.System Model of message authentication scheme

A Lightweight SDAS based on improved polynomial ECC scheme provides privacy to message sender. SDAS to provide message authentication. SDAS scheme is used. In order to provide message authentication for hop-by-hop without losing built in threshold of the polynomial-based method. A SDAS scheme is proposed which is as shown in fig 2. Every message is transmitted including digital signature using the private key of sender’s of the message generated in public-key based scheme. Forwarder of each intermediary node and receiver of last node can authenticate the message with the sender’s public key [18].

The new improvement in Elliptic curve cryptography shows that the public-key is stronger in terms of complexity, security and memory utilization and also it is very simple and pure key management.

B. Design Goals Secure Data Authentication Scheme (SDAS).

Authentication: In authentication process the receiver can check the messages which are retrieved by the corresponding sender. The adversary act as an innocent node, so the node can inject the fake messages.

Integrity: The integrity of messages being checked out whether the message is modified or not.

Hop-by-Hop message authentication: The routing path is provided to check the integrity and authentication. Communication is carried out by inserting the strong cryptography to involve the above discussed methods. These goals can be recovered through the symmetric, public key algorithm.

C. Advantages of Secure Data Authentication Scheme (SDAS).

- SDAS can be applied on any messages for authentication.

- Messages authentication can be provided without threshold limit.

- It is Energy efficient

- Reduce computational complexity

D. Formation of Network

If there should arise an occurrence of huge scale WSN the key administration is one of the real downsides for keeping up a secret key based authentication plans. As we definitely realize that few plans are projected to give node authentication where they can offer end to end node authentication by utilizing the secret key mutual between two nodes. The intermediary nodes may require to forward a controlled message for several hops earlier than the message is authenticated by the receiving node. In above case it expends additional sensor power and furthermore expands impact in the network and diminishes the message delivery ratio. Hence to improve performance advancement and empowering intermediary node authentication to safe guard from Daniel of service (DOS) attacks through massage controlled, which consumes power and communication resources in WSN. Therefore it is required to develop a protocol to give hop by hop node authentication is a major investigation work. Fig.3 show the network formation.

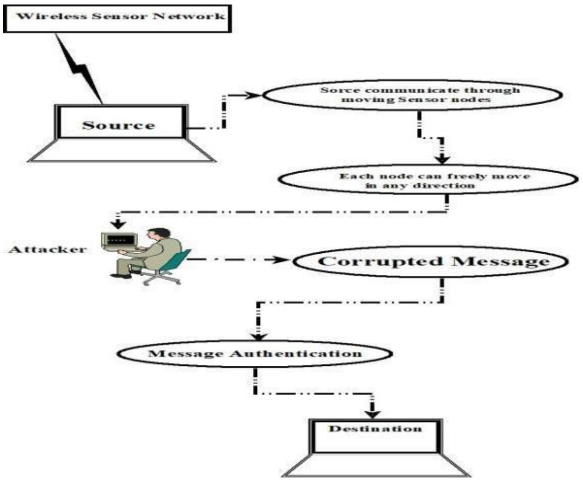

Wireless Sensor Network
Source
Sorce communicate through moving Sensor nodes
Each node can freely move in any direction
Attacker
Corrupted Message
Message Authentication
Destination

Fig 3. Formation of Network for message authentication

E. Algorithm for proposed scheme

Nomenclature: E1, E2...En: public key, m: message, C1, C2, C3:Anonymous Set(AS), t: time, g: generator or primitive root, St: intended message sender, Pk: private key of sender
,S(m): signed message.

1. Generate (m; E1; E2; . . .; En). Given a message ‘m’ and E1, E2...En of the AS (C1; C2; ….Cn) g, the intended message sender. St:1_t_n produces S(m) using its Pk.

2. Verification S(m): From message ‘m’ and S(m), which consist En of all members in the AS. Verification is done by the verifier to check S(m) is actually generated by the AS or not.

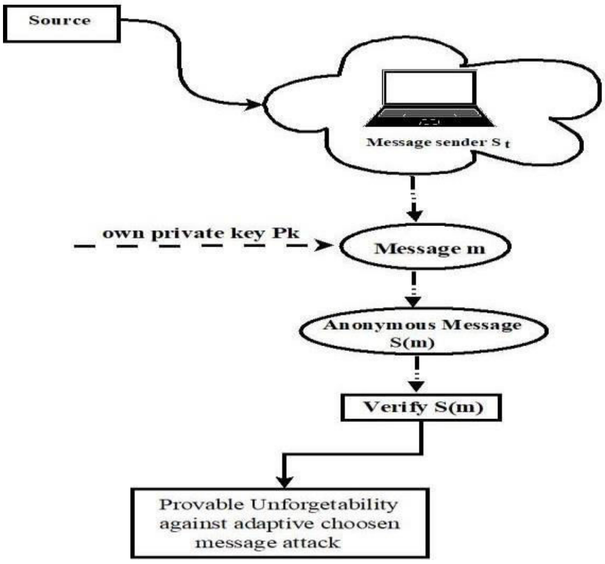


Fig 4. Secure data authentication scheme

F. Modified ElGamal signature (MES) scheme on Elliptic curve cryptography

Elliptic Curve cryptography Key Exchange:

Nomenclature: nA: sender private key, PA: sender public key, nB: receiver private key, PB: receiver public key, G:point on elliptic curve, q: prime number, n: large value, k secrete key of sender & receiver.

Let q > 3 is an odd prime. Now E is defined by a mathematical function called cubic function:

E: y2 = x 3 + ax + b

Let Eq (a b) elliptic curve with parameters a b & G.

Sender key generation:

1. Select nA: nA<n

2. Calculate PA: nA*G

3. Secret key calculation by sender: k= nA*PB

Receiver key generation:

1. Select nB: nB<n

2. Calculate PB: nB*G

3. Secret key calculation by receiver: k= nB*PA.

In this way key exchange is done using ECC.

G. **Modified ElGamal signature (MES) Scheme**:

Nomenclature: p: prime number, Pk:private key, e:public key, α:generator, h:one way hash function,(r s):is a pair of digital signature, m:message, k:random number

1. Key generation process. Select d with gcd(d,p-1)=1,then compute e.

e=αPk mod p

2. Signing process: To sign a message m, randomly choose k,0<k<p with(k,p-1)=1 , then compute r=αkmod p ,then solve “s” from equation: **s=Pkr+ks mod (p-1)** where four variables i’e, m,d,r and k are known and s is unknown.

s = k-1(m-Pkr)

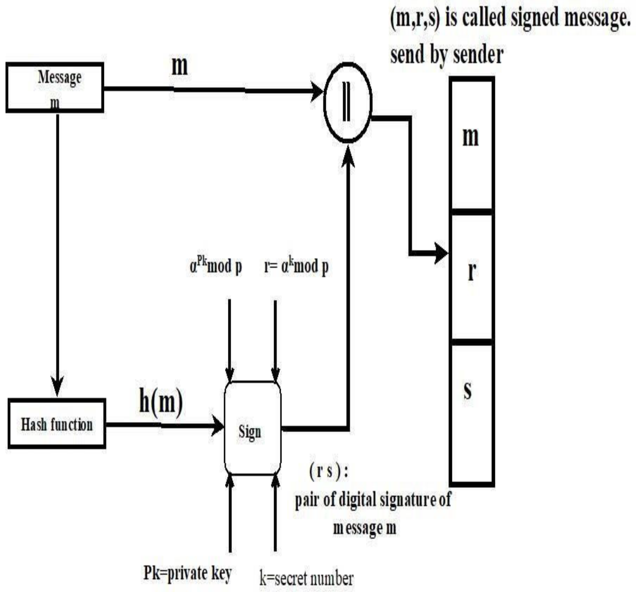
mod (p-1) s

=rPkh(m,r)+ k

mod (p-1)

3. **Verification process**: In verification process the verifier examines whether the signature (αs =rerh (m, r)) mod p, is holding equivalence or not. If yes then signature is accepted or else rejected.

Fig 5: Signing process



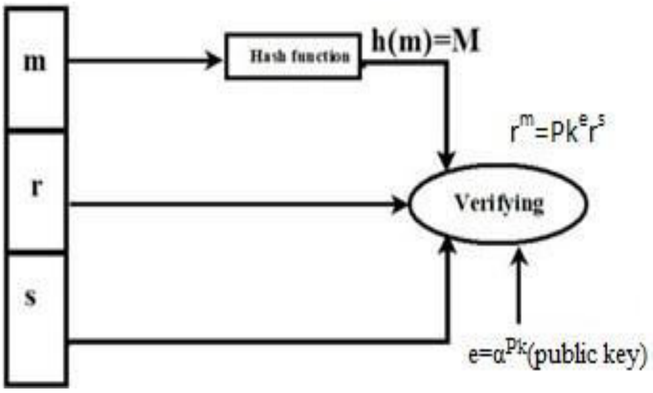


Fig 6: Verification Process

IV. SIMULATION RESULTS & COMPARISION

The simulation results show that energy consumption and message transmission delay are very low by the proposed work. The proposed scheme has performance parameters in terms of packet delivery ratio, transmission overhead and computation delay. Simulation were carried on discrete event tool, results were analyzed and compared with existing SLEACH .The disadvantage of SLEACH is, it does not provide guarantee of availability ,confidentiality and secure transmission of data [20]. Hence the proposed work is far better than SLEACH and it is energy efficient. On Table 1 shows the simulation parameters and proposed scheme is analyzed and table.2 shows comparison between LEACH, SLEACH & proposed work with respect to security aspect.

Simulator	NS-2
Propagation	Two Ray Ground
Number of Nodes	80
Simulation Area	1000 x 1000
Routing	LEACH
Antenna	Omni Antenna
Queue	DropTail
Queue Length	100
Nodes in a Cluster	20
Simulation Time	100 sec
Node Input power	2j
CSThresh	1 nW
RXThresh	6 nW

Table 1. Simulation parameters

Security	LEACH	SLEACH	Proposed
Integrity	NO	Medium	High
Authentication	NO	Medium	High
Confidentiality	NO	Medium	High
Computation overhead	High	High	Less
Efficiency	Low	Medium	High

Table 2. Comparison with others protocol

A. Security analysis

In our proposed scheme, if it is found that when a Cluster Head is compromised, the other keys related to sensor nodes are not revealed. As compared to the SLEACH, This scheme provides strong proof for Cluster Head which does not provide to retrieve keys when the attacker tries to retrieve keys. As shown in Figure 5, we can see the network successful rate when the nodes are attacked. Hence our proposed scheme provides better performance compared to SLEACH.

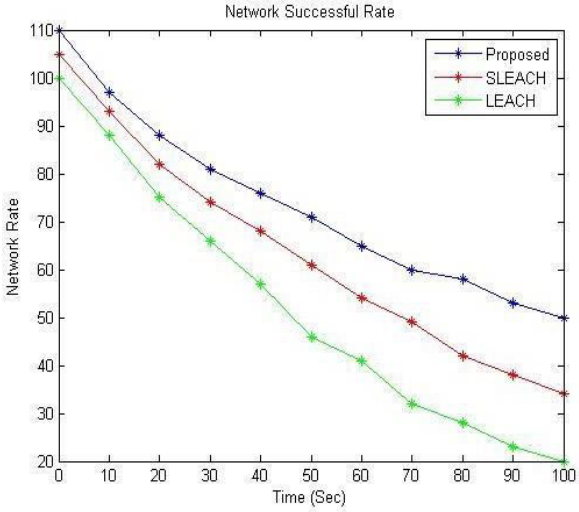


Fig 5. Network Successful Rate

B. Energy Consumption and Computation Overhead

In figure 6. Shows the energy consumption of proposed scheme, the energy equation is given as

From simulation result it is observed that our method consumes less energy for searching the key compare to existing scheme, where the Cluster Head consumes more energy in searching and authenticating keys which does not extend network life time. In this scheme we also evaluated computation overhead in generating, authenticating and verifying keys. The proposed scheme has less overhead than SLEACH because of using symmetric keys for authentication. Fig 6 and 7 shows energy consumption, computation overhead.

$$\text{Energy used} = \frac{\text{Consumed}}{\text{Initial Energy}} * 100\ \%$$

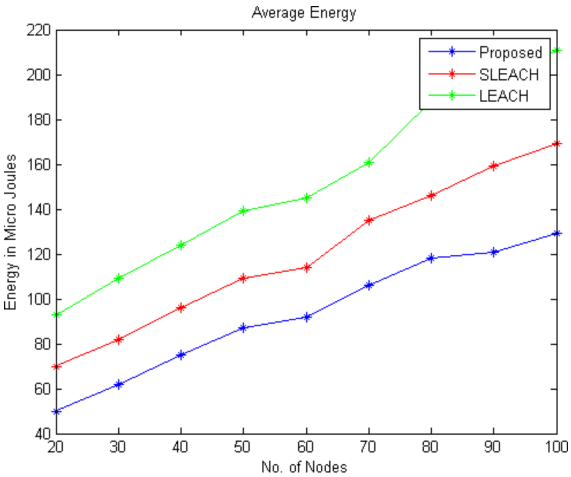


Fig 6. Average Energy Consumption

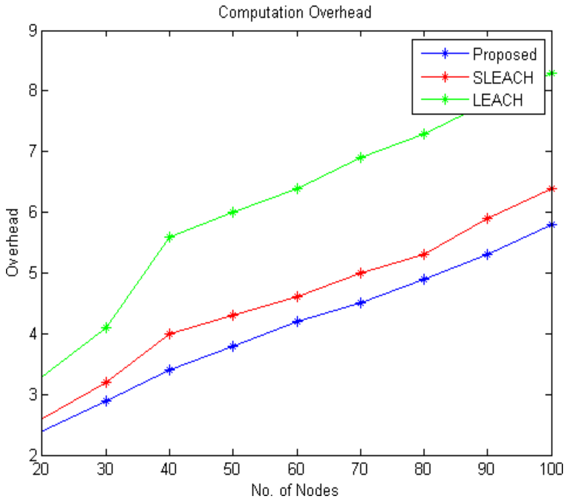


Fig 7. Computation Overhead

C. Packet Delivery Ratio

As per simulated results with Figure 8, we see the packet delivery ratio. We observe that shows when the malicious activity tries to packet drop in the network. Our proposed scheme has capability to prevent any malicious activity and reduces the packet drop ratio than existing scheme. In the below figure our proposed scheme achieves more PDR and delivers more authentic packets.

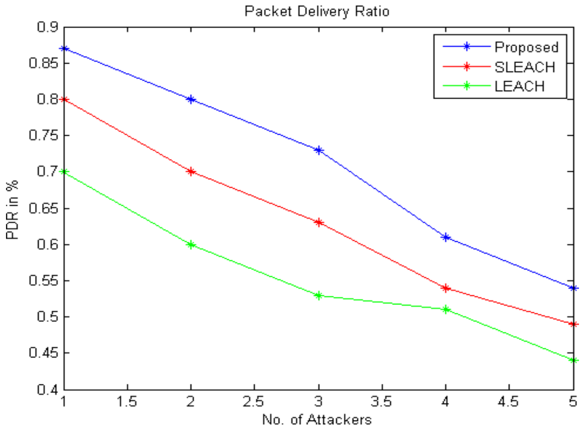


Fig 8. Packet Deliver Ratio

D. End to End Delay

Fig.9 Shows average end to end delay results, by our simulation results we observe that the delay is less in our proposed scheme compared to existing scheme. We analyze delay in terms of cryptographic operation in generating and verifying keys.

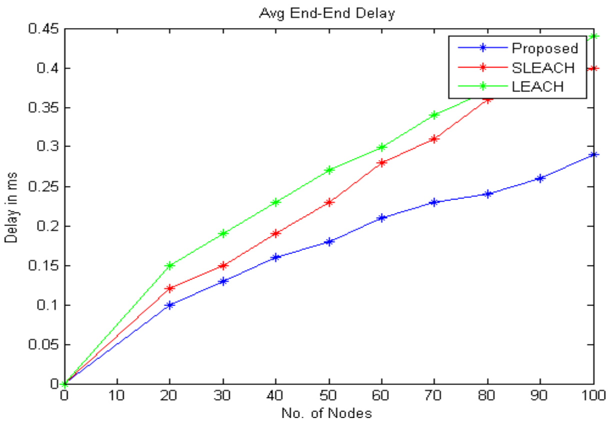


Fig 9. Average end to end Delay

IV. CONCLUSION

This paper concentrates on giving better security for transmission of data. The Lightweight Secure Data Authentication Scheme (LWSDAS) is proposed to increase the security of WSN. This scheme is based on Elliptic curve cryptography to protect against attacks and it is done by hop by hop authentication. An intermediate nodes are authenticated and allowed to transmit a data and it is free from threshold problem, mean unlimited data canbe authenticated and sent to the destination. Proposed scheme ensures better security and it can be robust against malicious attacks. The proposed work is compared with existing LEACH and SLEACH and evaluated performance in terms of overhead, end to end delay, packet delivery ratio and energy consumption. Simulation results show that proposed methodology is better in terms of security and energy efficient transmission compared to existing schemes.

ACKNOWLEDGEMENTS

We would like to thank Visvesvaraya Technological University, Belagavi for providing the required facility to complete the project within stipulated time.

REFERENCES

[1]. A. Nayyar, and A. Gupta, “A comprehensive review of cluster-based energy efficient routing protocols in wireless sensor networks”, IJRCCT, vol. 3, no. 1, pp. 104-110, 2014.

[2].Othman, M.; Shazali, K. Wireless Sensor Network Applications: A Study in Environment Monitoring System. Procedia Eng. 2012, 41, 1204–1210.

[3]. A Comparative Study of Wireless Sensor Networks and Their Routing Protocols, Debnath Bhattacharyya , Tai-hoon Kim , and Subhajit Pal, Sensors 2010, 10.

[4]. Sora, D. Security Issues in Wireless Sensor Networks. International Journal of Online Engineering (iJOE). 6(4): 26- 30 (2010). ISSN: 1861- 21216, 2010.

[5].Perrig, A., Stankovic, J., & Wagner, D. Security in Wireless Sensor Networks, In Communications of the ACM (CACM), Vol. 47, No. 6, June 2004.

[6].Shi E., and A. Perrig. “Designing Secure Sensor Networks.” Wireless Communication Magazine, 11 (6): 38-43, . December 2004.

[7].Akyildiz, F., W. Su, Y. Sankarasubramaniam, and E. Cayirci. “A Survey on Sensor.Networks.” IEEE Communications Magazine 40 (80): 102 – 114, August 2002.

[8].Mohamed Elhoseny, Hamdy K. El-minir, A. M. Riad and Xiaohui yuan, "Recent Advances of Secure Clustering Protocols in Wireless Sensor Networks", International Journal of Computer Networks and Communications Security, Vol. 2, No. 11, November 2014.

[9]. Heinzelman, Wendi Rabiner, Anantha Chandrakasan, and Hari Balakrishnan. "Energy-efficient communication protocol for wireless microsensor networks." In System Sciences, 2000.

[10].M. Guechari, L. Mokdad, and S. Tan, "Dynamic solution for detecting denial of service attacks in wireless sensor networks," in IEEE ICC Ad- hoc and Sensor Networking Symposium, Ottawa, ON, Canada, pp.173-177,2012.

[11]. Ali Abdul-hussian Hassan, Wahidah Md Shah,” Clustering Methods for Cluster-based Routing Protocols in Wireless Sensor Networks: Comparative Study”, International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, pp. 11350-11360, Number 21 (2017).

[12].Monika , Sneha Chauhan , & Nishi Yadav ,” LEACH-I Algorithm for WSN”, International Journal of Innovative Research in Computer and Communication Engineering Vol. 4, Issue 3, March 2016.

[13]. W.Xiao-yun, Y.Li-zhen, C.Ke-fei, SLEACH Secure Low Energy Adaptive Clustering Hierarchy Protocol for Wireless Sensor Networks, Wuhan University Journal of Natural Sciences, Volume 10, , PP.127-131,Number 1 2005.

[14]. Dong Chen , Wei Lu , Weiwei Xing and Na Wang ,” An Untraceable Data Sharing Scheme in Wireless Sensor Networks”, 31 December 2018.

[15]. Fares Mezrag, Salim Bitam, Abdelhamid Mellouk. "Secure Routing in Cluster-Based Wireless Sensor Networks", IEEE GLOBECOM 2017.

[16]. WANG Xiao-yun ,” SLEACH : Secure Low-Energy Adaptive Clustering Hierarchy Protocol for

Wireless Sensor Networks ",Vol.10 No. 1 2005.

[17].Wensheng Zhang , Subramanian, N.Guiling Wang, "lightweight And Compromise Resilient Message authentication In Sensor Networks",IEEE 27th Conference on Computer Communications on 2008.

[18]. H. Wang, S. Sheng, C. Tan, and Q. Li, "Comparing Symmetric-Key and Public-Key Based Security Schemes in Sensor Networks: A Case Study of User Access Control", Proc. IEEE 28th Int‟l Conf. Distributed Computing Systems (ICDCS), pp. 11-18, 2008.

[19]. Haodong Wang , Bo Sheng , Tan, C.C., Qun Li , " Comparing Symmetric-key and Public-key Based Security Schemes in Senso Networks A Case Study of User Access Control" 28th International Conference on Distributed Computing Systems, 2008.

[20]. Ibrihich Ouafaa, Esghir Mustapha, Krit Salah-Ddine, El Hajji Said," Performance Analysis Of Sleach, Leach And Dsdv Protocols For Wireless Sensor Networks (Wsn)", Journal of Theoretical and Applied Information Technology, Vol.94. No.2, 31st December 2016.

[21].W. Zhang, N. Subramanian, and G. Wang, "Lightweight and Compromise-Resilient Message Authentication in Sensor Networks," Proc. IEEE INFOCOM, Apr. 2008.

[22]. S.Ganesh,Dr.R.Amutha,"Real Time and Energy Efficient Transport Protocol for Wireless Sensor Networks", Journal Of Advanced Networking and Applications Vol. 01 No. 01 pages: 40-44 (2009).

[23]. S. S. Sonavane, Dr. B. P. Patil,"Experimentation for Packet Loss on MSP430 and nRF24L01 Based Wireless Sensor Network", Journal Of Advanced Networking and Applications Vol. 01 No. 01 pages: 25-29 (2009).

Biographies and Photographs

Mr. **Sangamesh J.Kalyane** Received the Bachelor's degree in Computer Science and Engineering from Visvesvaraya Technological University Belagavi, Karnataka 2002, M. Tech. degree in Computer Science and Engineering from JNTU Hyderabad, Andhra Pradesh in 2011.

From April 2012 to till date working as an Assistant professor in Department of Computer Science and Engineering at Bheemanna Khandre Institute of Technology Bhalki- Karnataka. His research interests areas are, Wireless Sensor Networks, Network Security, Computer Network and Management &presently pursing Ph.D under VTU, Belagavi, from 2015.

Dr. Nagaraj B. Patil Received the B.E degree from The University of Gulbarga Karnataka 1993, M. Tech. degree the AAIDU University of Allahabad in 2005,and the Ph.D. degree from University of Singhania Rajastan India in 2012.He is having teaching experience of 27 years including 7 years research, from 2010 to 2018. He worked as a Associate professor and HOD Dept. of CSE & ISE at Government College of Engineering, Raichur Karnataka. Presently he is working as a Principal of Govt Collegeof Engineering Gangavati Karnataka. His research interest's areas are Image Processing and Wireless sensor network.