Certificateless Effective Key Management Protocol (CL-EKM) Authentication for Multicast IoT Sensor Network

P. Manjula[1], Dr. S. Bagavathipriya [2]
{manjula.arunraj@gmail.com[1], baghavathipriya.s@rajalakshmi.edu.in[2]}

Assistant Professor/IT, Veltech Multi-tech Engineering College[1], Professor/CSE, Rajalakshmi Engineering College[2]

Abstract. IoT has a huge issue of security and protection because of its dynamic and heterogeneous nature. In the IoT environment, authentication is one of the most testing security prerequisites. Because a client can straightforwardly access data from the devices, given the mutual validation among client and device occurs. The research includes a CL-EKM and verified key establishment scheme has been proposed for secure communication in the IoT environment. Proposed system utilizing a multicast verification procedure which improves the adaptability of CL-EKM by empowering a delivery message from BS to an enormous cluster head hub with an acceptable delay and cost. Also, the proposed framework is contrasted with the current unicast and broadcast strategies which would cause a serious negative effect on the performance when a network size increases or when quantity of data to be communicated for a time given is enormous. The proposed results examined for security and is additionally implemented utilizing a simulator.

Keywords: IoT, Certificateless effective key management protocol, Key establishment, Multicast transmission.

1 Introduction

IoT includes an arrangement of physical items that are associated to gather information over the web. The items were equipped with an adequate communication and processing capacities and has locatable IP address. Proposed system is in need to incorporate frameworks based on PCs and also presents with economic advantage and for improving efficiency and exactness while lessening human association.

Utilizations of IoT is assorted comprising of framework administration for high-hazard situations, disaster management following ecological monitoring by offering distant administrations of medical care. IoT, offers widening to access, also comes a colossal danger to security as well as protection because of its dynamic and heterogeneous nature. Utilizing powerful security practices, particularly validation and key administration plans to ensure obscurity and protection, is required. Since cryptographic methods are needed to ensure the security benefits, a viable administration of cryptographic keys is constantly needed in an organization. Hence for addressing the security concerns, the ECM methods were presented in the earlier research as well dependent on symmetric key encryption [1], [2], [3]. This type of encryption was suitable for the sensor nodes as a result of its restricted energy and processing

I3CAC 2021, June 07-08, Chennai, India

DOI 10.4108/eai.7-6-2021.2308569

ability. Be that as it may, it shows high communication overhead which also needs enormous memory space for storing shared pairwise keys. It was additionally not adaptable and not tough in contradiction of any compromises, and unfit to help node mobility. Asymmetric key based public key cryptography or "Identity-Based Public Key Cryptography" (ID-PKC) for simplifying the establishment of key and authentication have been proposed [4], [5], [6], [7], [27], [10], [15], [18], [25].

In any case, it was discovered that the security shortcomings of the preen ECC based plans [5], [10], [25] that such methodologies were quite helpless against forgery message, attacks and key compromise. Such ECC-based plans with authentications when straightforwardly applied experience the ill effects of certificate management overhead. Subsequently, we utilize certificateless successful key management (CL-EKM) technique. In CL-PKC [12], The private key of the customer is a combination of the KGC: "Key Generation Center" unfinished private key with the hidden value of the customer. The Public/Private Key Pair together removes the credential condition and thus resolves the key problem by removing liability for the private Key of the customer.

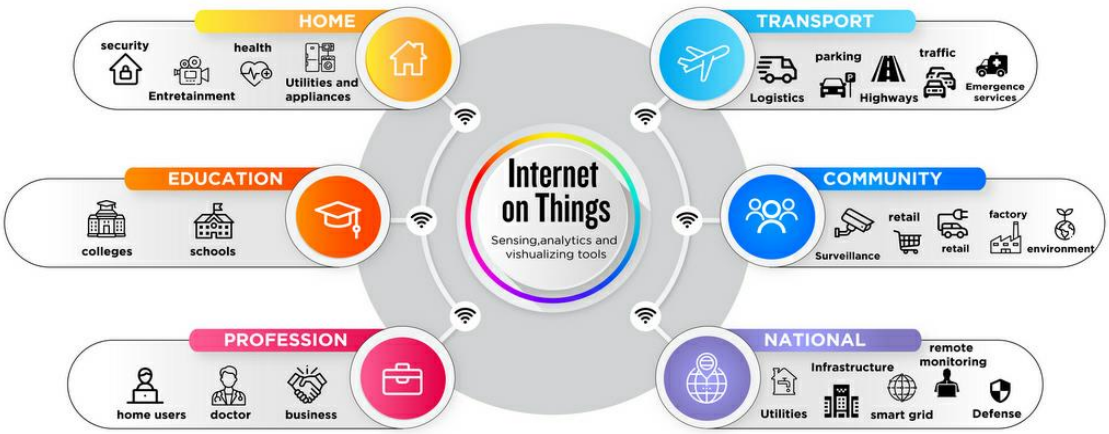
Regardless of indicating various advantages, this method shows some basic constraints as demonstrated in [R4] One of the limitations is to use the unicast mode to relay messages from the BS to all clustering heads. Since it has high cost of communication and computation and doesn't addresses a scalability prerequisite of the protected group of communication and when a system grows or in case the messages to be communicated on a time is huge, it will cause serious negative effect on its performance. Anyway, the authors in [R4] have demonstrated that broadcast transmission mode is viable and scalable to enable conveyance of messages from BS to an enormous group heads with an acceptable delay, with a satisfactory communication and computation energy, delay, data transfer capacity related with the interchanges between the BS and all its head.

This work addresses the security issues presenting multi-cast IoT application that is dissemination of information via the services of multi-cast networks, where its reliability is guaranteed for different clients. Since multicast [11] is one of the main administrations which is needed to be upheld in IoT [12, 13]. Wireless multicast [15] is one of the main services which gives profoundly productive methods for sending messages from single different source receivers [16].

In IoT [14] applications, the sending hub must have the option to affirm that this message is received by every individual from a multicast group, where at the same time guaranteeing security. In IoT applications, a significant issue is contrasted with conventional multi-cast frameworks is that it upholds the devices of end-users, yet additionally includes "Large-Scale Machine-Type Communications" (MTC) with low-power gadgets [12]. In this manner, the multi-cast needs of IoT limits the obliging of various types of gadgets and managing higher speed rates or ejected overhead.

Inclusive of all the points of interest, the multicast communication additionally has the accompanying downsides. It has higher data transfer capacity use in numerous applications and overhead of retransmission where it also grows up rapidly as a quantity of multicast objects increments [19]. In any case, the fundamental issue in the multicast system is ensuring reliable and secure transfer under different services. In this manner, the proposed framework guarantees security in the multicast transmission through the certificateless powerful key management protocol (CL-EKM) and the scheme of authenticated key network for secure communication and the experimentation is completed in an IoT network. Th rest of the research was organized under in the sectin2.

2 System Model



We think of four different scenarios in the IoT model, i.e. home, transport, communities and national ones, as seen in Fig. 1. Smart machines, for example, cameras and actuators are available for all of these scenarios. These gadgets help people to live on a daily basis. In these circumstances, any intelligent computer is linked to the internet through the Gate-way Network (GWNs). Different types of customers can access information about major IoT devices through the GWN. Customer and system authentication through GWN allow the customer to receive details [2].

Communication among the elements is carried out on a public channel. The adversary would then be able to have the occasion to snoop, adjust or erase the sent messages. It was additionally accepted that an adversary could hold at least one detecting device in IoT, and can remove all the sensitive data utilizing the power analysis attacks [4], [5].

Multicast Communication

Since accessibility and worldwide availability are the critical prerequisites of every application of IoT, this expands the accessible possibility of any risk. A heterogeneous idea of IoT raises intricacy in deploying the security methods. A wireless idea of included substances and its restricted limit were additionally a constraint. Conceivable transient and arbitrary failures are weaknesses that attackers could misuse.

ECC based Multicasting

To accomplish energy efficient secured multicasting, we propose to utilize an ECC based Multicast model. This methodology includes following issues:

- Node Deployment
- Node Scheduling based Secured Multicast model

Sensor nodes are arbitrarily deployed over the coverage area. They are self-configurable and work with a restricted energy source. For instance, to screen the war zone, a gathering of sensors can be tossed from a low-flying plane. These nodes will design themselves to frame a communication network.

In this methodology, nodes are framed into clusters of inconsistent length. A Cluster Head (CH) will lead each group. The Clusters close by the base station will have less competition range contrasted and faraway ones. CHs close to the base station need to deal with information

originating from its cluster members just as from different groups on the way to the base station. With unequal grouping, as the cluster length is less, the CH close to the base station will deal with less intra group traffic evading quick drain out of energy. Thus, the problem area issue is disposed of.

In a clustered environment, every sensor hub will detect information ceaselessly and advance it to the CH. CH will enhance information by accumulating detected information and sending it to the base station through intermediate CH nodes. To save energy, the NSSM plot works in duty cycle mode where every hub works in two modes: dynamic and static modes. Initially, the quantity of nodes adequate to cover the cluster zone are chosen and kept in dynamic mode. The excess nodes will be in static mode.

The Duty-cycle based methodologies can be synchronous or asynchronous. In Synchronous mode, nodes will be in dynamic or static mode dependent on the exchange made inside a frame. Synchronous protocols were clarified in [16-18]. In asynchronous mode, preface testing procedures are utilized to intermittently awaken nodes for a short term as clarified in [19-20].

In Proposed approach, a Tree-based multicast model is utilized. To guarantee secure communication, the Group key is created utilizing light-weight Elliptic Curve Cryptography (ECC) based calculation. ECC is most appropriate for resource constrained conditions. It is expressed that, for 128-bit message security, ECC needs a 256-bit key contrasted and 3072 bits key in RSA. A Binary tree is developed for each group, established from the cluster head. A Tree Vector (TV) is built putting away the level-wise way from root to leaf nodes. During this methodology, a secured cluster key's produced in an exceptionally conducive manner and distributed among all the individuals.

3 Key Management in Multicast Communication

For better communication, the information ought to be encoded using an assistance of a private key which is then validated. The distribution method and the key administration used in the network of safe application should give better adaptability, integrity, authenticity, as well as higher confidentiality. A single key that was shared in WSN communication is not secure as an adversary could be as it is able to undoubtedly distinguish among different key. Thus, sensors utilize diverse key administration strategies for securing a communication. In recently created key management schemes, Researchers proposed different plans such as the bilinear matching in “Dynamic Key Management” (DKM), key administration based on jobs, “Identity Based Key Management” (IBKM), “Random Seed Distribution with Transitory Master Key” (RSDTMK), irregular key circulation [11-16].

In the present research, CL-EKM: “Certificateless Key Management” plot which underpins the foundation of 4-kinds of keys. The plan likewise uses fundamental calculations of CL-HSC method [13] in determining certificateless private/public as well as the pairwise keys.

Working of Certificateless Key Management Scheme

Certificateless Public/Private Key:

1. KGC at the BS was used to generate certificateless unique public-private pair of keys which are stored in a node, before the deployment of node. Authenticated pairwise key is mutually generated.

2. Every node has its own unique key with the Base station. For instance, an L-sensor makes use of an individual key for encrypting an alert message for sending it to the BS, in case it is unable to link with the H-sensor. An H-sensor makes use of their individual key for encrypting this message which correspond to any changes in a cluster.
3. A BS could make use of a key for encrypting any type of sensitive data, like the information in a node or in the command.

Pairwise key:

Each node offers a distinctive pair-wise keys with every neighboring node to secure the communication and verification of the basestation. In case, in arrange to connect one cluster, with L-sensor ought to provide a pair-wise key with an H-sensor. At that point, it could safely disperse the cluster-key to an L-sensor with the help of a pairwise key. When using a strong Wireless Sensor network, an L-sensor could utilize a pair-wise key for safely transferring detected information to the H-sensor. Every node could powerfully set up pair-wise key with another hub and itself utilizing some particular private/public certificateless key sets.

Cluster key:

Every node connected in a cluster makes use of a key known as the cluster key. A cluster key is basically utilized to secure the cluster broadcast messages, example, the delicate commands or altering the status of the member in a cluster. As it were a cluster head could upgrade the key in case the L-sensor clears out or is joined with a cluster.

Aim of this approach is reduction in energy and delay in communications. Consider chunks holding the messages multicast from one base station to the sensor heads. This method does not follow any of the asymmetric key encryption algorithms to ensure security in the chunk as these key operation methods consume more energy. Hence, authentication in the chunk is achieved by using the individual keys of the base station and sensor heads for the encryption operation. Post this authentication, the messages could be multi-casted. The below explained algorithm depicts the process of achieving the certificateless key management during the multicast in detail.

Algorithm

Step 1: Creation of Sub-Chunks

To create a chunk, partition the n multicast messages into N sub-chunks s_1, s_2, s_3……...s_N. Every subchunk s_i with $1 \leq i \leq N$ holds m multicast messages represented as mN.

Step 2: Creation of Chunks

2.1: Concatenation

Concatenate the multi-casted messages in every sub chunk.

$s_{i(con)} = mN_{(i-1)\,(n+1)}||\ldots\ldots\ldots||mN_{i.n}$ for $1 \leq i \leq N$ (1)

2.2: Padding

Pad the concatenated messages with the authenticator. Authenticator denotes the digest which is calculated by the collision resistant hashing function such as SHA or MD5. Thus pad the concatenated message with the digest as shown in equation (2).

$P(s_{i(con)}) = s_{i(con)}||\ digest$ for $1 \leq i \leq N$ (2)

2.3: Hashing

Hash the padded message in step 2.2 using any hash function.

$digest_{i+1} = H(P(s_{i(con)}))$ for $1 \leq i \leq N-1$ (3)

Therefore, every concatenated chunk s_N should be padded with the random string $digest_{N+1}$.

2.4: Message Chunk

Decryption of every digest in the subchunk is achieved using an individual key. Subchunk s_i and the $digest_{i+1}$ form the chunk S_i.

$S_i = [s_i, digest_{i+1}]$ when $1 \leq i \leq N$

Step 3: Chunk Multicasting

Multicasting the chunk is important because every chunk waits for the authenticator (digest) from its previous chunks. Therefore, this process should follow the sequential multicast mechanism.

Step 4: Authentication of Chunks

According to step 3, the first chunk S_0reaches the receiver initially. Thus, the receiver authenticates the digest in the chunk S_0 using its individual authentication key A_{k0} for decryption of the chunk S_0. Similarly, authentication of other chunks can be performed using the hash functions such as SHA and MD5. Since, the digest of S_0 reaches initially in advance, it can also be used to authenticate S_i. Therefore, to conclude that S_i is authentic, the hashed value of the multi-casted messages and the authenticator $mN_{(i-1)\,(n+1)}||\ldots\ldots\ldots||mN_{i.n}||digest_{i+1}$ should be equivalent to the digest value $digest_{i+1}$.

4. Multicast Authentication of the nodes

Another feature of security is the Authentication which comes with a guarantee that the transmitted messages are from an authenticated source. Four kinds of authentication methods exist which can be used in the process: (a) Implicit authentication; (b) Three-way authentication; (c) Mutual or Two-way authentication; and the (d) One-way authentication.

The following authentication steps are carried out between the source and the destination.

Source Authentication

Consider a message *M* being multi-casted by a user *A* with an identity *I*.

Step 1:

The user generates a signature *S* on the message *M.*

***1.1*:** User selects a private key *R* and chooses a timestamp *T*.

1.2 - Following the sign algorithm of MR-IBS, the user generates a signature and transmits the message to the destined device. When $||M||T|| \leq$ key, the user *A* issues a signature *S* on the message $M_s = (S\ , I\ , T)$ which is further transmitted to the destination.

If $||M||T|| \geq$ key, then the user divides the message *M* into $M_1||M_2$ and generates the signature by performing the sign algorithm of PMR-IBS. In this situation, the user transmits $M_s = (S, I, M, T)$ to the destination.

Destination Authentication

On the receipt of the message, the device at the destination generates a signature S_D using the sign MR-IBS (or) PNR-IBS algorithm and transmits the message $M_D = (S_D\ , I_D\ , T_D\ )$ or $M_D = (M_D^1, S_D\ , I_D\ , T_D\ )$.

NOTE: The device receiving the messages, authenticates the signature following the MR-IBS (or) PMR-IBS algorithm. Upon verification, the algorithm either transmits (or) drops the message.

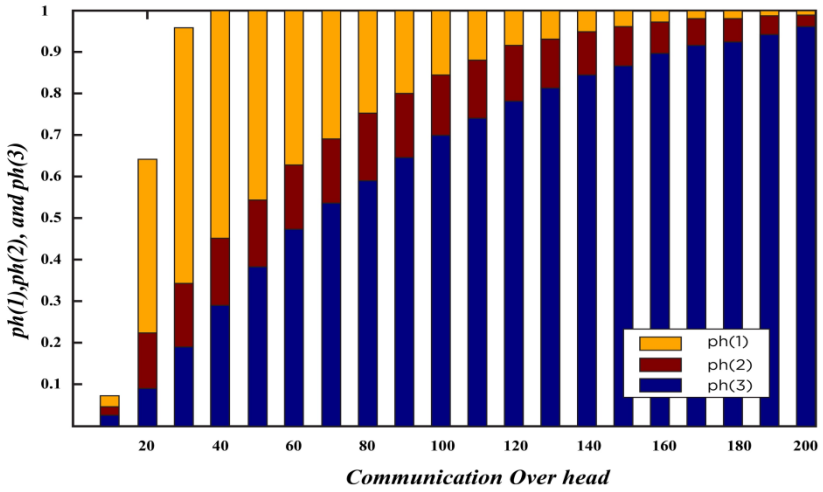
5. Performance Analysis and Results

The primary aim of the present research the performance analysis of the novel scheme proposed here. The following section includes both the simulation results and the analytical functioning. The following metrics are used to evaluate the performance.

Communication Overhead

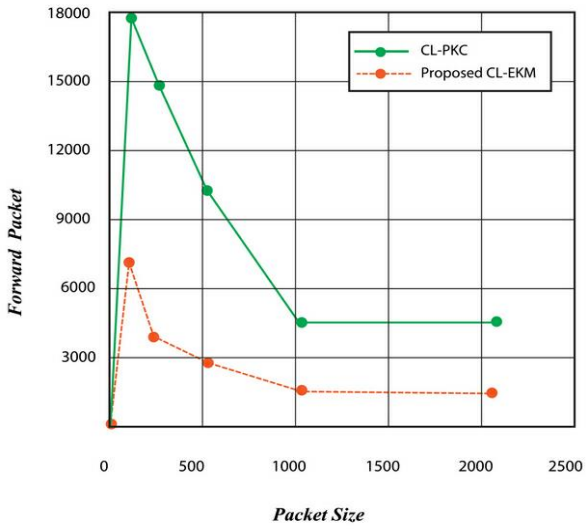
As the transmission is the major source of the battery consumption, communication required by a key management scheme must be small. In addition, transmitting the secret information over the air increases the security threats. Hence, a key management scheme should not incur high overhead during the communication. A possibility that two same neighbor nodes might share a single key is lesser than 1, when two nodes are not associated straightforwardly it ought to discover a course within the key-sharing chart to associate to one another.

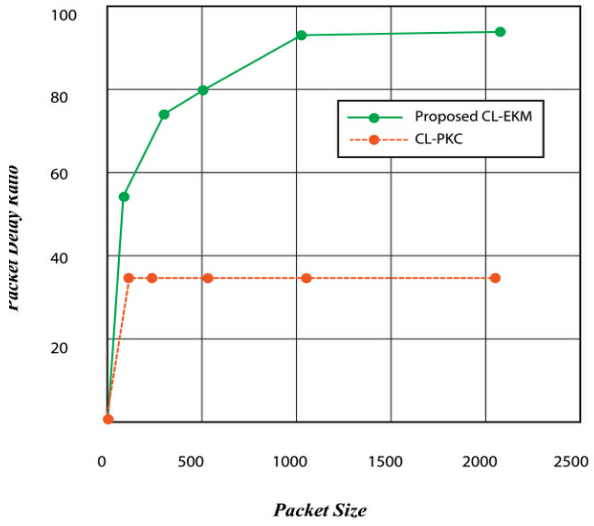
The numbers of jumps are estimates as per the requirement of this course. Clearly, if two neighbors are associated specifically, number of required bounces is 1. In case more number of jumps is required to put through a pair of nodes neighboring to each other, the overhead in the communication of setting a security affiliation among the two hub is high. The probability of lesser hops required is denoted with ph(1) which is used to connect the two nodes, and is equal to 1. Here ph(1) is equal to plocal, the local connectivity.



Connectivity

Secure connectivity shows the ratio of securely connected links to all links in the network. For a key management scheme, higher secure connectivity can be achieved by either having a large number of node pairs that share a secret key or offering an efficient and secure path key establishment method.

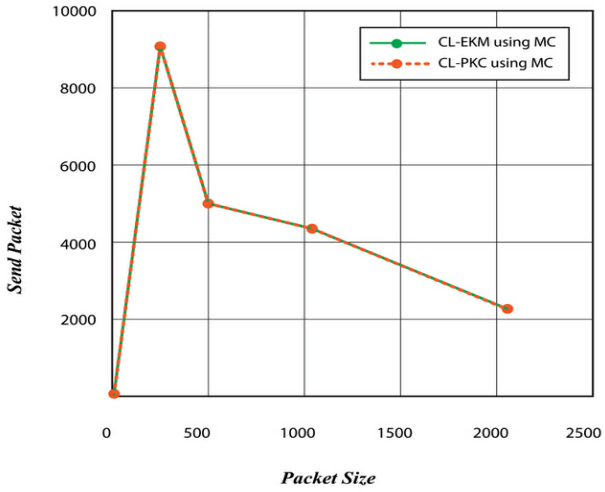


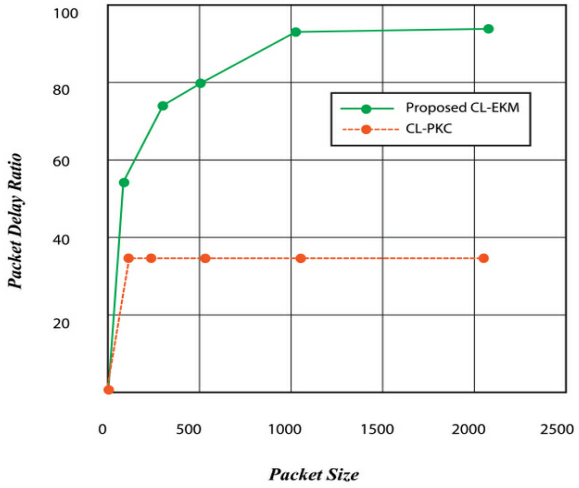


We utilize worldwide network to allude the proportion nodes within large separated elements within the final chart for measuring the total arrange. On the off chance that the proportion breaks even with 99%, it implies that maxim sensory nodes were associated, where rest of the nodes were inaccessible from biggest disconnected elements. Hence, the worldwide network metric demonstrates a rate of nodes which is squandered due its unreachability. Both local and global connectivity is affected with this scheme of pre key-distribution.

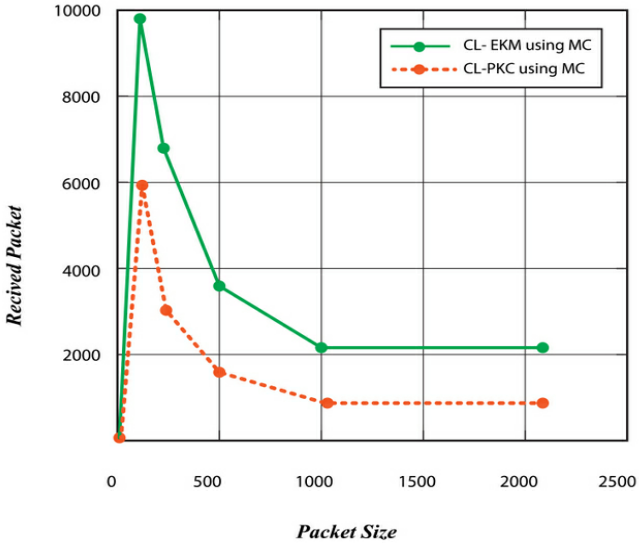
Memory overhead

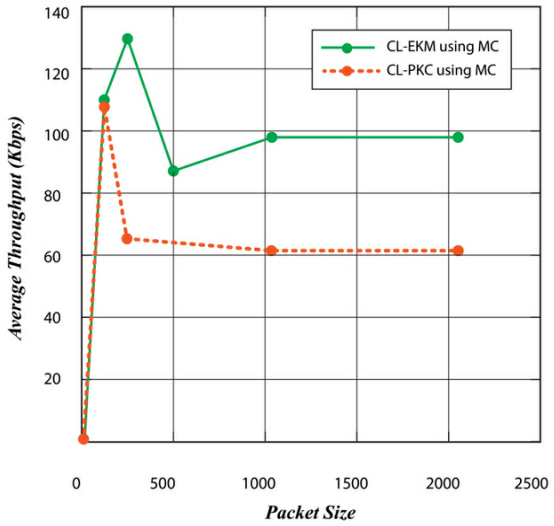
Since memory of sensor nodes is mainly occupied by operating systems and application programs, the remaining part should be used carefully. Hence, a key management scheme should be as efficient. As possible in terms of the numbers of keys that have to be stored in a sensor node.

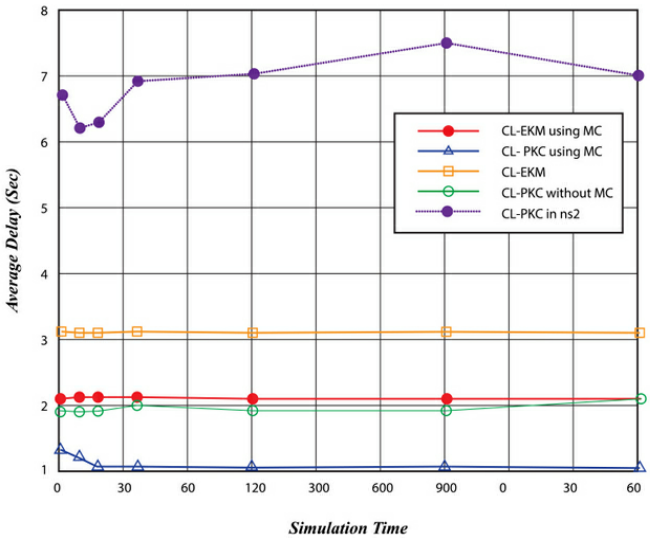

10000
8000
6000
4000
2000
Send Packet
CL-EKM using MC
CL-PKC using MC
0
500
1000
1500
2000
2500
Packet Size


100
80
60
40
20
Packet Delay Ratio
Proposed CL-EKM
CL-PKC
0
500
1000
1500
2000
2500
Packet Size

Energy and Delay Assessment







6. Conclusion

Our Proposed scheme significantly reduces the energy overhead due to the Base-station communication reaching to all the nodes of cluster head, which significantly helps making a protocol more efficient for delay, scalability as well as offers high flexibility. The proposed method provides effectiveness in terms of computation and communication when compared to other techniques used. More features of functionality, communication costs, efficient computation and high security are the few advantages of proposed technique that are suitable in IoT applications into a practical environment in comparison with other techniques.

References

[1] Anil Kumar Sutrala1, Saru Kumari2, Vanga Odelu3, Mohammad Wazid and Xiong Li4 “An efficient multi-gateway-based three-factor user authentication and key agreement scheme in hierarchical wireless sensor networks”Security Comm. Networks (2016) Published online in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/sec.1464

[2] Dieynaba Mall1 , Karim Konaté1 , and Al-Sakib Khan ECL-EKM: “An Enhanced Certificateless Effective Key Management Protocol for Dynamic WSN” NSysS 2017Department of CSE, BUET. 5-8 January, 2017

[3] Wu chunying , Li shundong , Zhang yiying , “Key Management scheme based on secret sharing for Wireless Sensor Network” 2013 Fourth International Conference on Emerging Intelligent Data and Web Technologies

[4] Amit Kumar Gautam, Rakesh Kumar. "A Comparative Study of Recently Proposed Key 8 3% 9 2% 10 1% 11 1% 12 < 10 words Management Schemes in Wireless Sensor Network" , 2018 International Conference on Computing, Power and Communication Technologies (GUCON), 2018.

[5] Suman Bala ,Gaurav Sharma and Anil K.Varma“A Survey and taxonomy of symmetric key management schemes for wireless sensor networks” Proceedings of the CUBE International Information Technology Conference ,September 2012.
[6] Sravani Challa, Mohammad Wazid, Ashok Kumar Das, Neeraj Kumar, Alavalapati Goutham Reddy, Eun-Jun Yoon, Kee-Young Yoo. "Secure Signature-Based Authenticated Key Establishment Scheme for Future IoT Applications" , IEEE Access, 2017.
[7] Ms. NimishaChunilalChaudhari , “Key Management in Wireless Sensor NetworkA Survey”, International Journal of Application or Innovation in Engineering & Management Volume 2, Issue 2, February 2013.
[8] S. Wander, N. Gura, H. Eberle, V. Gupta and S. C. Shantz, "Energy analysis of public-key cryptography for wireless sensor networks," Third IEEE International Conference on Pervasive Computing and Communications, Kauai Island, HI, 2005, pp. 324-328, doi: 10.1109/PERCOM.2005.18.
[9] Shraddha Deshmukh, Prof. A. R. Bhagat Patil, and Harshad Nakade, "Implementation of Effective Key Management Strategy with Secure Data Aggregation in Dynamic Wireless Sensor Network," International Journal of Scientific Research in Computer Science, Engineering and Information Technology, vol.4, no. 2, pp. 358-364, 2018.
[10] Laxmi, B. Prathusha, and A. Chilambuchelvan. "GSR: Geographic Secured Routing using SHA-3 algorithm for node and message authentication in wireless sensor networks." in Future Generation Computer Systems, vol.76, pp 98-105, 2017
[11] Athmani, Samir, Azeddine Bilami, and Djallel Eddine Boubiche, "EDAK: An Efficient Dynamic Authentication and Key Management Mechanism for heterogeneous WSNs," in Future Generation Computer Systems, November 2017.
[12] Ayaz Hassan Moon, Ummer Iqbal, G. Mohiuddin Bhat” Authenticated key exchange protocol for Wireless Sensor Networks” International Journal of Applied Engineering Research ISSN 0973-4562 Volume 11, Number 6 (2016) pp 4280-4287.
[13] Saraswathi, R. Vijaya, L. Padma Sree, and K. Anuradha, "Dynamic and probabilistic key management for distributed wireless sensor networks," proceedings of IEEE International Conference on Computational Intelligence and Computing Research, pp. 1-6, 2016
[14] J. S. Pan, S. C. Chu, T. K. Dao, and V. C. Do. “Improved Performance of Wireless Sensor Network Based on FuzzyLogic for Clustering Scheme.” In International Conference on Smart Vehicular Technology, Transportation, Communication and Applications, Springer, pp. 104-113, Cham, 2019.
[15] J. Wang, J. Niu, K. Wang, and W. Liu. “An energy efficient fuzzy cluster head selection algorithm for WSNs.” In 2018International Workshop on Advanced Image Technology (IWAIT), IEEE, pp. 1-4, 2018.
[16] H. AA Al-Kashoash, Z. SA Rahman, and E. Alhamdawee. “Energy and RSSI based fuzzy inference system for clusterhead selection in wireless sensor networks.” In Proceedings of the International Conference on Information andCommunication Technology, pp. 102-105. ACM, 2019.
[17] Challa, Sravani, Ashok Kumar Das, Vanga Odelu, Neeraj Kumar, Saru Kumari, Muhammad Khurram Khan, and Athanasios V. Vasilakos, "An efficient ECC-based provably secure three-factor user authentication and key agreement protocol for wireless healthcare sensor networks," Computers & Electrical Engineering, 2017.
[18] Zhongyuan Qin, Xinshuai Zhang, Kerong Feng, Qunfang Zhang, Jie Huang “An Efficient Key Management Scheme Based on ECC and AVL Tree for Large Scale Wireless Sensor Networks” International Journal of Distributed Sensor Networks, vol. 11, 9, First Published September 17, 2015.
[19] H. El Alami and A. Najid, "CFFL: Cluster formation using fuzzy logic for wireless sensor networks," 2015 IEEE/ACS 12th International Conference of Computer Systems and Applications (AICCSA), Marrakech, 2015, pp. 1-6, doi: 10.1109/AICCSA.2015.7507248.

[20] N. Saqib and U. Iqbal, "Security in wireless sensor networks using ECC," 2016 IEEE International Conference on Advances in Computer Applications (ICACA), Coimbatore, 2016, pp. 270-274, doi: 10.1109/ICACA.2016.7887964.
[21] W. Wei-hong, L. Yu-bing and C. Tie-ming, "The study and application of elliptic curve cryptography library on wireless sensor network," 2008 11th IEEE International Conference on Communication Technology, Hangzhou, 2008, pp. 785-788, doi: 10.1109/ICCT.2008.4716252.
[22] Qing Chang, Y. Zhang and Lin-lin Qin, "A node authentication protocol based on ECC in WSN," 2010 International Conference On Computer Design and Applications, Qinhuangdao, 2010, pp. V2-606-V2-609, doi: 10.1109/ICCDA.2010.5541288.
[23] M.Selvi, C.Nandhini, K.Thangaramya, K.Kulothungan, A.Kannan, "HBO Based Clustering and Energy Optimized Routing Algorithm for WSN,"in 2016 IEEE Eighth International Conference on Advanced Computing (ICoAC), 2017, pp.89-92.
[24] K. Johny Elma, Dr. S. Meenakshi, "Energy Efficient Clustering for Lifetime Maximization and Routing in WSN", International Journal of Applied Engineering Research, 2018.