Received: July 17, 2018

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

A Novel Technique for Improving the Security of WSN Using Random Key Pre-Distribution Scheme

Vijay Kumar Nadipinayakanahalli Krishnappa [1]* **Suresh Hosahalli Narayanagowda [2]**

[1] *Department of Computer Science & Engineering, Bangalore Institute of Technology, India*
[2] *Department Electronics & Instrumentation Engineering, Bangalore Institute of Technology, India*
* Corresponding author's Email: vkumargptcs@gmail.com

Abstract: Secure mechanisms are widely in Wireless Sensor Networks (WSNs), not only for improving the network energy consumption and lifetime, it also improves the security between the networked Sensor Nodes (SNs). Key management is a fundamental security mechanism which is equipped in WSN. In this paper, a Random Key Pre-distribution (RKP) scheme is used in Low-Energy Adaptive Clustering Hierarchy (LEACH) based clustered network. LEACH divides the network into a number of clusters and also it elects the optimum Cluster Head (CH) from each cluster. Then RKP scheme provides the common keys to each SN of the network to improve the secrecy of the network. Combination of LEACH and RKP scheme is named as LEACH-RKP-WSN. After performing key distribution, the data packets are sent from the source (anyone of SN) to Base Station (BS). The performance of LEACH-RKP-WSN was compared with Adequate Sparse Secure and Minkowski distance based Location Privacy (ASSMLP). Thus the result shows energy consumption, packet delivery ratio, throughput and delay and it achieves 12.1%, 2.25%, 6.5% and 2.25% better performance than ASSMLP. The lifetime of the network increased by minimizing the energy consumption of the LEACH-RKP-WSN.

Keywords: Wireless sensor networks, Security, Leach, Random key pre-distribution, Energy consumption.

1. Introduction

Wireless Sensor Networks (WSNs) are the wireless networks which comprise of hundreds or thousands of networked SNs. These SNs is deployed in an unattended, harsh and hostile environment. Key management is a main core for providing the secure communication inside the network and the network scalability is improved by unital-based key pre-distribution scheme [1-3]. A suitable encryption key protocol like certificate less effective key management protocol is introduced to support an effectively updates a key while a SN left or joins with in a cluster [4]. In heterogeneous WSNs, the single lightweight protocol is introduced for both the dynamic authentication and key management scheme. Dynamic keys are generated by the previous information [5]. The time division secret key protocol is equipped to identify the denial of service attack through the network [6]. The amount of communications and computations are decreased by the combination of Lightweight Kerberos and Elliptic Curve Menezes–Qu–Vanstone protocols and also it improves the network security and the energy consumption [7]. A secured decentralized data transfer is enabled to minimize the effects of the node capture attacks, and then an augmented tree based routing is equipped to generate the path from the source to the destination (BS) [8].

There are three protocols are used in tree-based key management scheme such as time stamp protocol (TSP), polynomial points sharing protocol (PPSP) and secret sharing protocol (SSP). The TSP protocol makes encryption and decryption operation over the CH for authenticating the Mobile Data Collector (MDC), and then PPSP and SSP uses a polynomial construction and estimation for authenticating MDC [9]. Communication security of WSN is achieved by a data encryption and mutual authentication of multilevel dynamic key management system, it is a

coordination centre for asymmetric keys and each SN built a various asymmetric keys in neighbours [10]. Depends on the geometry of simplistic, the deterministic key pre-distribution scheme is introduced over the network and it has three basic operations such as key pre-distribution, shared key discovery and path key establishment [11]. Resource efficient authentic key establishment (RAKE) is used in the clustered heterogeneous WSN for exploiting the clustering characteristics of WSN which is used for delivering a hierarchy of initial symmetric keys. If L-sensors are present in the tamper-resistant hardware, the information stored in the network becomes insecure [12]. The gateway node is issued the temporal credential to each user and SN by a password based authentication. This WSN network gives good performance only when the gateway node is being as a centralized node [13]. Based on multifunctional data aggregation schemes (MODA) two enhanced and complementary schemes are introduced such as random selected encryption based data aggregation and compression based data aggregation is introduced in WSN to improve the communication cost. The MODA provides the results with the higher communication cost [14]. The above methods have some constraints such as insecurity, reliability, etc. In order to overcome these constraints, the LEACH-RKP-WSN is used to enhance the security among the network. Then the performance is improved by using the RKP in a cluster based network with the use of LEACH. The major contributions of this LEACH-RKP-WSN is stated as follows:

- To save energy of this desired network, a single hop routing technique such as LEACH clustering is introduced to improve the lifetime of this LEACH-RKP-WSN.
- LEACH algorithm does not require any control information from the BS.
- Here the node to node communication security is improved by RKP without involving BS.

This research work is composed as follows, Section 2 presents a survey of recent papers based on security related WSN. The section 3 briefly described the random key pre distribution using LEACH clustering. The section 4 and section 5 describes about an experimental setup and results and discussion of the LEACH-RKP-WSN method with comparative analysis. The conclusion of this research work is given in the section 6.

2. Literature survey

H. Fakhrey, R. Tiwari, M. Johnston, and Y.A. Al-Mathehaji [15] has presented location-dependent key management protocol with random selected cell reporters (LKMP-RSCR) in a wide area of network. The security of a network is enhanced by the existence of cell reporters. Based on the virtual grid, the terrain which is provided by the WSN is separated into a lot of cells. Based on the node location and cell centre location, both a node key and cell key are derived in each cell respectively. This LKMP-RSCR requires only a less computations. The authenticity of the system is improved only up to 35%.

F. Gandino, R. Ferrero, B. Montrucchio, and M. Rebaudengo [16] has introduced a new key management scheme which is depends on the transitory master key and this scheme is named as a hierarchic scheme with transistor master key. Pairwise keys are computed by the formula of LEAP+. The efficiency of this method is improved by minimizing the key setup time. If all nodes know the initial key value, then it degrades the performance of the security system.

S. Ruj, A. Nayak, and I. Stojmenovic [17] has presented the pairwise and trible key distribution scheme in WSN. The trades (combinatorial structures) are used in the pairwise key generation and then the trible key distribution shared a common key in each three nodes. This method improved the security and bandwidth requirements. It is difficult to generate a secure routing using trible key and this scheme is broken when the nodes are compromised more than c (i.e., security parameter of trible key distribution).

F. Zhan, N. Yao, Z. Gao, and G. Tan [18] has improved the key connectivity with the help of the novel key generation methods which depends on the system of equations. If the system has one and only one solution, then the system is considered as an eligible system. The equations are applied to the eligible system to generate a secret key that is called as associate keys. The Computational complexity of this desired system is small and it requires only an arithmetic operation. If t then again the path key establishment is happened. The establishment of path key happened again when the nodes does not have the common keys and it leads to disconnect the intersections among nodes.

N. Suganthi and V. Sumathy [19] designed an efficient key establishment scheme named as traditional cryptographic technique. In this technique, three types of keys are established such as individual key, pairwise key and the group key. The keys at initialization, membership change and key compromise are analysed by polynomial function. This method needs less memory, even the number of

nodes of the system increases and also the communication overhead is less. The immunity of the WSN towards the several attacks is decided by the algorithm complexity.

Uma Meena and Anand Sharma [20] has presented the ASSMLP to overcome the location privacy and security protection issues. This method comprises of two different phases. The fake source and fake sink technique is used in the first phase to concentrate on the location privacy. In second phase, the security and confidentiality of the transmitted message is mad by sparse matrix and the one-time key is created by using extended euclidean algorithm. An energy of each SNs need to be considered while clustering the network.

The existing algorithms has some disadvantages like complex routing, less security and high energy consumption. Due to overcome these drawbacks, a key management scheme such as RKP is introduced in a cluster based routing (LEACH) network. The detailed description of this proposed methodology is given in the following section 3.

3. LEACH-RKP-WSN methodology

In LEACH-RKP-WSN, the LEACH is used for dividing the network into a number of clusters. Then the CH is elected from each cluster based on the threshold value of LEACH and it serves the equal chance to all nodes to be a CH. Additionally, the random key pre-distribution scheme is developed for providing the keys to each nodes for making the secured network. The overall schematic for the LEACH-RKP-WSN is given in the following Fig. 1.

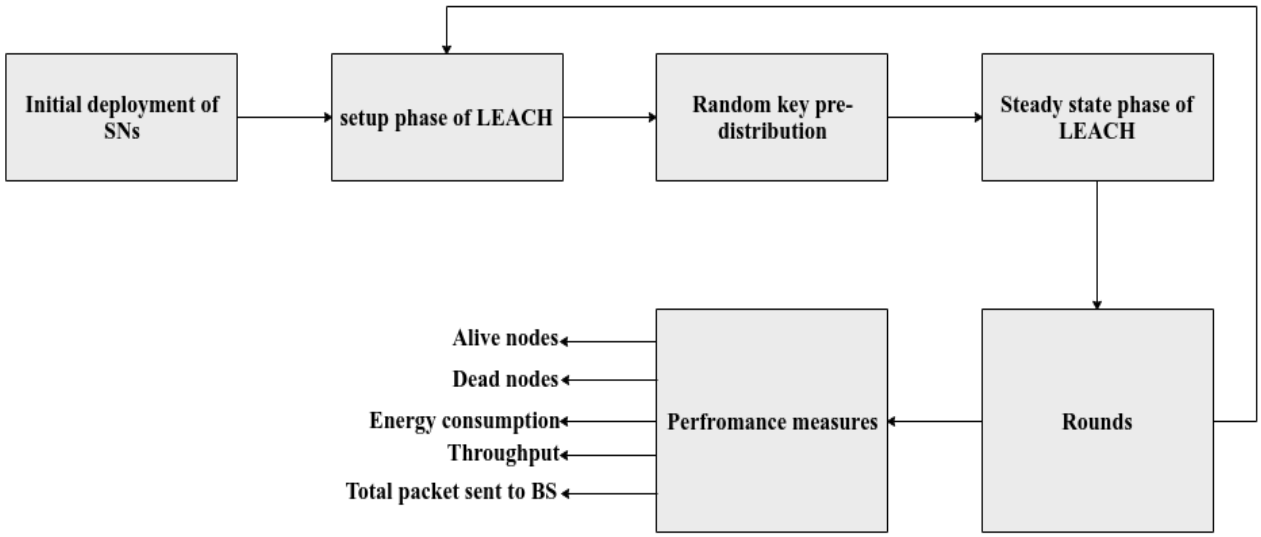


Figure.1 Block diagram for LEACH-RKP-WSN

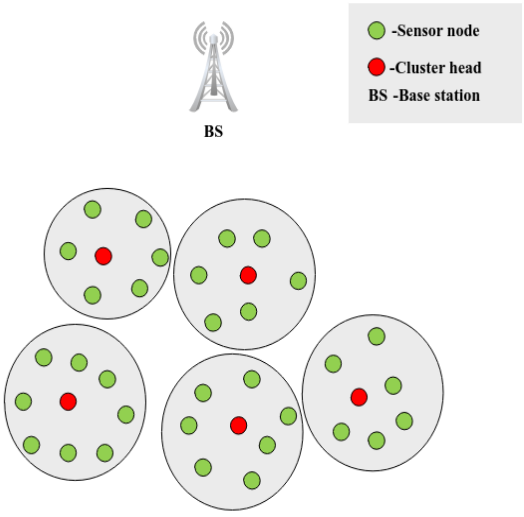


Figure.2 Cluster formation of LEACH

3.1 LEACH based clustering

Initially the SNs are randomly deployed in an interested area to develop the communication between the source and the destination. Then LEACH is applied in this node. LEACH is one of the hierarchical clustering algorithm which is used in the WSN and this LEACH performs self-organizing and re-clustering functions for each round. LEACH is classified into two phases such as set-up phase and steady state phase. In set-up phase, the SNs of LEACH-RKP-WSN is categorized into clusters. In that clusters any one of the node acts as a CH and remaining nodes are normal nodes. The data are transmitted from the nodes to CH and CH to the sink (BS) and there is no direct communication from the

nodes to the sink. In this LEACH clustering CH gathers the data form the nodes and this data is aggregated and it is directly transferred to the BS. The additional responsibilities of the CH are to avoid the draining of their energy in fewer iterations by randomized rotation of the CH. The node is elected as the CH based on the suggested percentage (P) and also by the earlier record as a CH. The nodes which are not a CH of past (1/P) rounds generate a number between 0 and 1. The respective node act as a CH when the generated value is less than a threshold $T(n)$ and the formula for the threshold calculation is given in Eq. (1).

$$T(n) = \begin{cases} \frac{P}{1-P\times rmod(1/P)} & if n \epsilon G \\ otherwise & 0 \end{cases} \quad (1)$$

Where, the set of nodes which is CH for a previous $1/P$ rounds is represented as$G$, suggested percentage of a CH is represented as P and the current round is r. After the selection of CH, it acts as a CH for next $1/P$ rounds. Because, it serves the equal chance to all nodes to be a CH and the selected CH transmits its own status by CSMA MAC protocol. From this advertisement, the non-cluster head selects its CH by comparing the RSSI of multiple CH. TDMA schedule is created by CH for its related members in a cluster. The following Fig. 2 shows the cluster formation of LEACH.

3.2 Random key pre-distribution scheme

After performing the LEACH based clustering, the RKP scheme is used for assigning the key for each node of the network. RKP is such kind of probabilistic approach and it achieves enhanced the security over the small scale attack and the keyset up security is improved. So, that to eavesdrop communication among nodes the attackers have to compromise a lot of nodes. The network is fully secured when some of the nodes are compromised and these nodes are complicated. This RKP is divided into three phases such as key pre-distribution, shared key discovery and path key establishment.

3.2.1 Key pre-distribution

3.2.1.1 Generation of the key pool

Each sensor node of network holds k amount of different keys that are randomly selected from a big key pool. The key pool comprises two kinds of parameters such as key chains L and key pool size K. A different key chains are present in the key pool that is represented in the following Eq. (2).

$$K = jc_j \ \ (j = 0,1, L-1) \text{ and } \ \ C_j \cap C_k = \phi (j \neq k) \quad (2)$$

The unique generation key g_i and the publicly known $seed$ is used for generating the each key chain C_i by applying a keyed hash algorithm in a frequent manner. The l-th key of the key chain $C_i$is calculated by Eq. (3).

$$k_{c_j} = H^l(seed, g_j) \quad (3)$$

Where, $H^l(seed, g_j) = H(H^{l-1}(seed, g_j), g_j)$. The $g_i$is allocated to each sensor node and it is must be kept as a secret to improve the secrecy of the desired network. The corresponding key is indexed by the pair$(C_i, l)$and it is given in the following Eq. (4).

$$C_j = l = 1\, K/L\, k_{c_j}, l \quad (4)$$

The graphical illustration of the key pool and key chains are shown in Fig. 3.a.

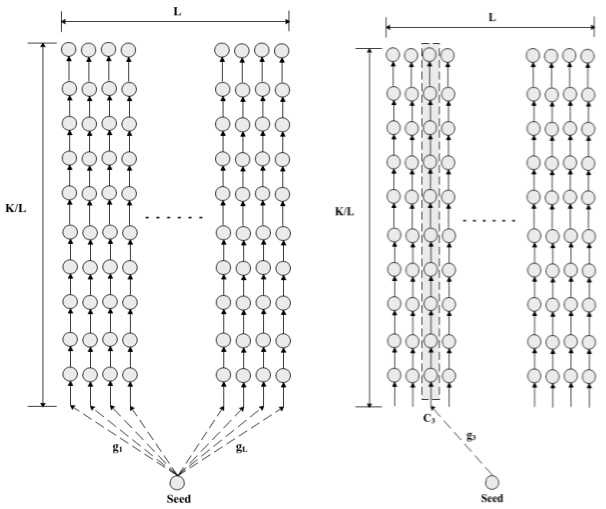
3.2.1.2 Key Ring Loading

In this key ring loading phase, each node holds it allocated key rings R. This key ring R comprises of two main parts such as $R1$ and $R2$. The generation knowledge of amount of key chains and the set of individual random keys from the different key chains are represented as $R1$ and $R2$ respectively. To be more specific, for node j has some key ring value that is given in the Eq. (5).

$$R_j = R_{j,l} \cup R_{j,2} \quad (5)$$

The assignment of rule of each node is given as follows.

Initially, the node j is allocated with the randomly elected key chains r_0 . To reduce the storage requirement of each node, the nodes are stored only the corresponding key chain generation keys like one key per one chain. In this part it stores the $r_0$keys which is $|R_{j,1}| = r_0$. The random keys $r_0 \times (K/L)$is effectively calculated by key generation r_0 . Furthermore the node j is allocated with randomly selected keys r_1 each from a different key chain ($|R_{j,2}| = r_1$), it is shown in Fig. 3.b.



(a) (b)

Figure.3 (a) Key pool generation, (b) Sample key ring

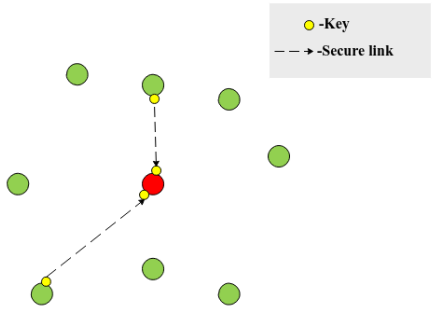


Figure.4 Secure link establishment

3.2.2 Shared key discovery

The process of shared key discovery starts when the SNs of the network is deployed in the specific network. Then these SNs searches for its neighbours nodes and it shares the common keys. The list of key identifier is broadcasted by nodes to other nodes. The secure communication between the nodes happens by key only when the nodes are known it can share a common key with a particular node and this communication happen within a specific communication range. If two nodes identify one or more common keys, a secure link is generated between them and the communication is done over the link of two nodes. The following Fig. 4 shows the secure link establishment.

3.2.3 Path key establishment

In path key establishment process, a link between the two nodes are generated even the nodes does not have the capacity to share a common key. For example, the node A needs to communicate with the rest of the nodes and those nodes do not have a common key between the nodes. The node A transmits the message to node C like node A wants to communicate with node B. The node A common key encrypts the message and this message is transmitted among the node A and node C. Pairwise key for node A is created when the node C has its own common key to node B. The amount of unused keys holds in the sensor key ring. Each sensor node uses the unused keys of the sensor key ring for improving the path key establishment.

3.3 Steady state phase

The steady state phase is started when the keys of RKP is distributed to each node. Based on the key values, the node to node communication is performed. In this phase nodes communicate to cluster-head during allocated time slots otherwise nodes keep sleeping. Due to this attribute LEACH minimize energy dissipation and extend battery life of all individual nodes. When data from all nodes of the cluster have been received to cluster-head, it will aggregate, compress and transmit to sink. The steady state phase is longer than setup phase. The following Fig. 5 shows the routing of CH to BS.

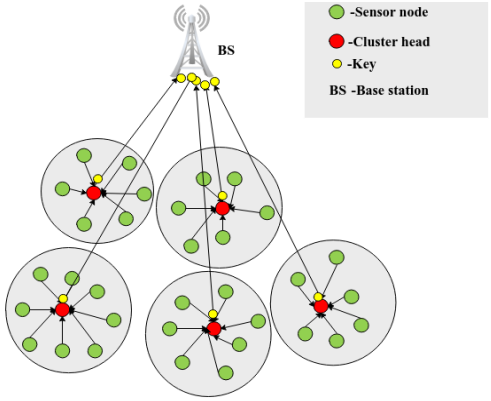


Figure.5 Route from CH to BS

Table 1. Specifications

Clustering algorithm	LEACH
Area	100m×2000m
Security algorithm	RKP
Simulator used	NS3
Simulation start time	0.0000
Simulation end time	500.0000
Number of nodes	100
Base station location	(50,50)
Antenna model	Omni antenna
Minimum speed	30 ms
Network interface type	Wireless
MAC type	MAC/802_11
Initial energy	1J

4. Experimental setup

LEACH-RKP-WSN system has implemented by using Network simulator 3 software tool (for the simulation purpose). In that LEACH-RKP-WSN, the clustering among SNs is provided by the LEACH and the security is developed by RKP. The following Table 1 shows the specifications which is used in the LEACH-RKP-WSN methodology. For knowing the performance of this LEACH-RKP-WSN method, it is compared with ASSMLP [20].

5. Results and discussions

The LEACH-RKP-WSN has implemented with 100 SNs. Assume each sensor node has the initial energy up to 1J. The LEACH-RKP-WSN algorithm is verified greatly and described the experimental results for both security and clustering. The coverage area of the entire network 100m×2000m and the position of the base station is 50,50 that is x and y co-ordinates. For knowing the performance of the LEACH-RKP-WSN, it is compared with ASSMLP [20].

5.1 Energy consumption

The total quantity of energy required for each node to deliver the message through the path is extracted in the LEACH based clustering and the total energy consumption is given in Eq. (6).

$$E_c = E - (E_T + E_R) \tag{6}$$

Where energy consumption of the WSN is represented asE_c,E is defiend as the total amount of energy, the transmitting and receiving energy is represented asE_T and E_R respectively.

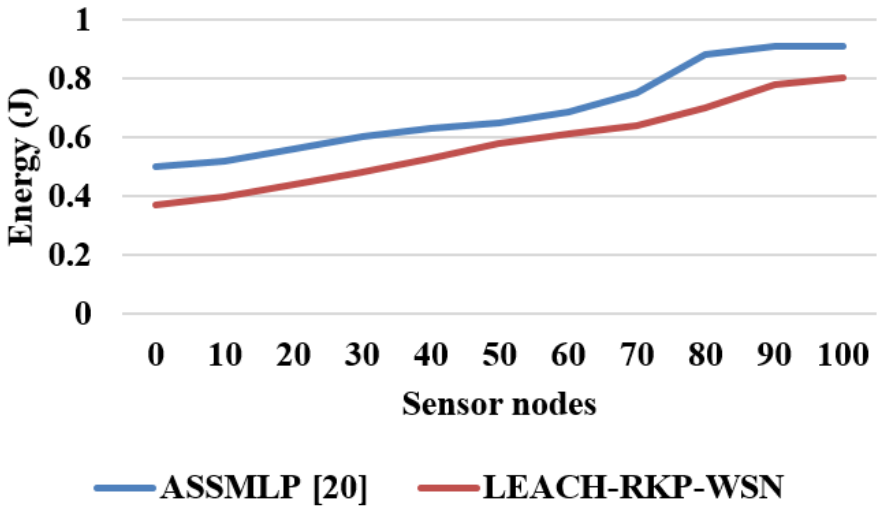


Figure.6 Comparison of energy consumption

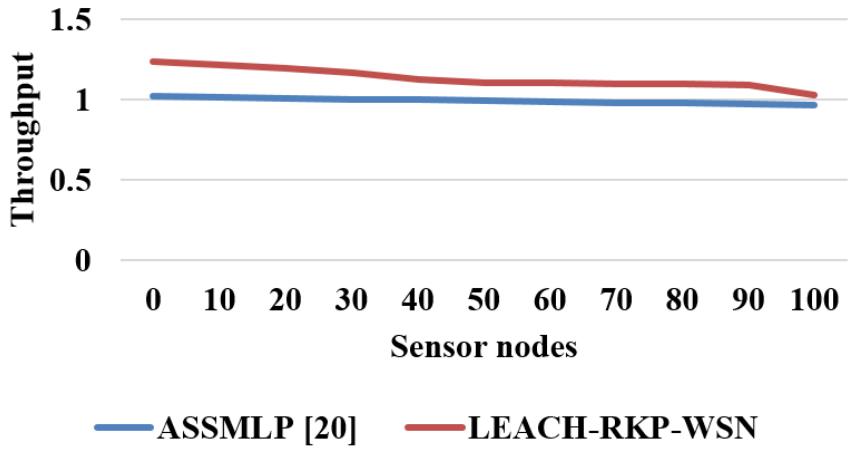


Figure.7 Comparison of throughput

Fig. 6 shows the energy consumption of two methods LEACH-RKP-WSN and ASSMLP [20]. Energy consumption of the LEACH-RKP-WSN is less compared to the ASSMLP [20] method. Energy consumption is more when the distance among the source to the destination becomes high.

5.2 Throughput

Throughput is described as a number of successful messages delivered to the destination in a particular point of time.

Fig. 7 shows the comparison of two methods LEACH-RKP-WSN and ASSMLP [20] in terms of throughput. From the analysis, it is concluded that the throughput of the LEACH-RKP-WSN is increased when compared to the ASSMLP [20]. The throughput of the entire network is maximized by making the successful transmissions without any packet loss.

5.3 Packet Delivery Ratio (PDR)

The data transmission reliability is shown by the PDR. PDR is the ratio between number of packets received by the BS to number of packets generated by the source node. The PDR is given in the Eq. (7).

$$PDR = \frac{Packetsdelivered}{Packetsgenerated} \quad (7)$$

Fig. 8 shows the comparison of total packet sent to the BS for LEACH-RKP-WSN to ASSMLP [20]. By considering the energy of each SN, the transmission rate of delivering the successful messages of LEACH-RKP-WSN becomes more.

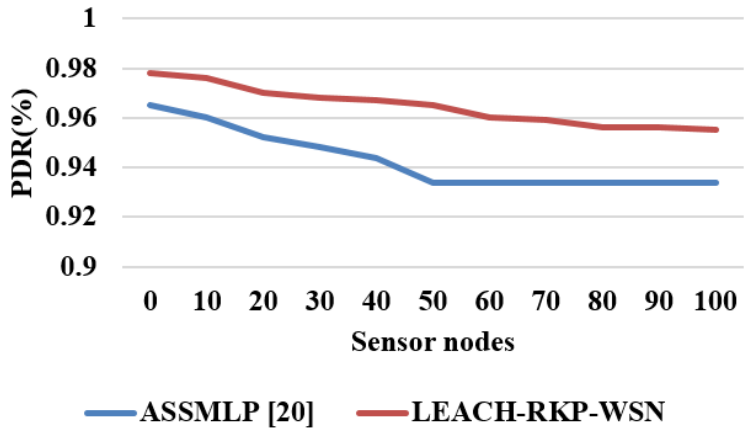


Figure.8 Comparison of packet delivery ratio

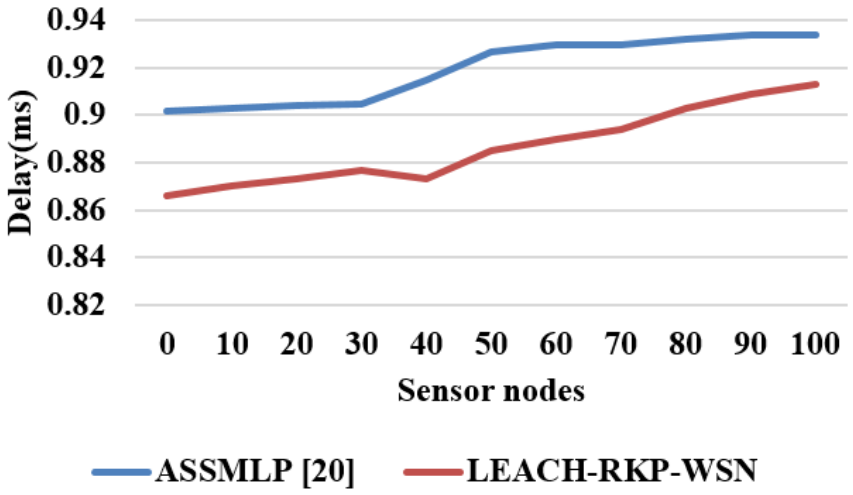


Figure.9 Comparison of end to end delay

5.4 End to end delay

The end to end delay is described as the amount of time taken by packet transmitted from the source node to the BS.

Fig. 9 shows that the end to end delay comparison of LEACH-RKP-WSN and ASSMLP [20]. From the Fig. 10 concluded that the LEACH-RKP-WSN takes less amount of time for transmitting the desired information from the source to the destination.

From the analysis, it concluded that the LEACH-RKP-WSN consumes less energy when compared to the existing ASSMLP [20]. Because, the ASSMLP mainly depends on the security, it doesn't consider the shortest path for transmitting the data from the source to the destination. But, in LEACH-RKP-WSN both the security and energy efficient based clustering is considered, during the data transmission from the source to the destination (BS).

6. Conclusion

This paper presented a secured clustering network which is the combination of LEACH algorithm and the random key pre-distribution scheme (LEACH-RKP-WSN). LEACH algorithm is used for dividing the network into clusters and elects the CH from each cluster and this clustering is improves the energy consumption of the desired network. Then the provided RKP improves the security over the clustered network by sharing the key to each node of the desired network. The probability of key shared between the cluster head to the sensor nodes are increased by RKP. This LEACH-RKP-WSN gives the better performance when compared to ASSMLP. The efficiency of this LEACH-RKP-WSN is improved by decreasing the amount of energy utilized by each transmission. The energy consumption of LEACH-RKP-WSN is reduced at 12.1% when compared to the ASSMLP. This leads to enhance the lifetime of the network. Furthermore, the energy consumption and security of WSN can be minimized by using effective clustering and authentication mechanisms.

References

[1] J. Zhang and V. Varadharajan, "Wireless sensor network key management survey and taxonomy", *Journal of Network and Computer Applications*, Vol.33, No.2, pp.63-75, 2010.

[2] X. He, M. Niedermeier, and H.D. Meer, "Dynamic key management in wireless sensor networks: A survey", *Journal of Network and Computer Applications*, Vol.36, No.2, pp.611-622, 2013.

[3] W. Bechkit, Y. Challal, A. Bouabdallah, and V. Tarokh, "A highly scalable key pre-distribution scheme for wireless sensor networks", *IEEE Transactions on Wireless Communications*, Vol.12, No.2, pp.948-959, 2013.

[4] S.H. Seo, J. Won, S. Sultana, and E. Bertino, "Effective key management in dynamic wireless sensor networks", *IEEE Transactions on Information Forensics and Security*, Vol.10, No.2, pp.371-383, 2015.

[5] S. Athmani, A. Bilami, and D.E. Boubiche, "EDAK: An Efficient Dynamic Authentication and Key Management Mechanism for heterogeneous WSNs", *Future Generation Computer Systems*, In Press, 2017.

[6] J.L. Chen, Y.W. Ma, X. Wang, Y.M. Huang, and Y.F. Lai, "Time-division secret key protocol for wireless sensor networking", *IET communications*, Vol.5, No.12, pp.1720-1726, 2011.

[7] N.S. Fayed, E.M. Daydamoni, and A. Atwan, "Efficient combined security system for wireless sensor network", *Egyptian Informatics Journal*, Vol.13, No.3, pp.185-190, 2012.

[8] E. Kohno, T. Okazaki, M. Takeuchi, T. Ohta, Y. Kakuda, and M. Aida, "Improvement of assurance including security for wireless sensor networks using dispersed data transmission", *Journal of Computer and System Sciences*, Vol.78, No.6, pp.1703-1715, 2012.

[9] A.S. Poornima, and B.B. Amberker, "Secure data collection using mobile data collector in clustered wireless sensor networks", *IET wireless sensor systems*, Vol.1, No.2, pp.85-95, 2011.

[10] O.K. Sahingoz, "Large scale wireless sensor networks with multi-level dynamic key management scheme", *Journal of Systems Architecture*, Vol.59, No.9, pp.801-807, 2013.

[11] C. Shangdi, and W. Jiejing, "New key pre-distribution scheme using symplectic geometry over finite fields for wireless sensor networks", *The Journal of China Universities of Posts and Telecommunications*, Vol.24, No.5, pp.16-76, 2017.

[12] Q. Shi, N. Zhang, M. Merabti, and K. Kifayat, "Resource-efficient authentic key establishment in heterogeneous wireless sensor networks", *Journal of parallel and distributed computing*, Vol.73, No.2, pp.235-249, 2013.

[13] K. Xue, C. Ma, P. Hong, and R. Ding, "A temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks", *Journal of Network*

and Computer Applications, Vol.36, No.1, pp.316-323, 2013.
[14] P. Zhang, J. Wang, K. Guo, F. Wu, and G. Min, "Multi-functional secure data aggregation schemes for WSNs", *Ad Hoc Networks*, Vol.69, pp.86-99, 2018.
[15] H. Fakhrey, R. Tiwari, M. Johnston, and Y.A. Al-Mathehaji, "The optimum design of location-dependent key management protocol for a WSN with a random selected cell reporter", *IEEE Sensors Journal*, Vol.16. No.19, pp.7217-7226, 2016.
[16] F. Gandino, R. Ferrero, B. Montrucchio, and M. Rebaudengo, "Fast Hierarchical Key Management Scheme with Transitory Master Key for Wireless Sensor Networks", *IEEE Internet of Things Journal*, Vol.3, No.6, pp.1334-1345, 2016.
[17] S. Ruj, A. Nayak, and I. Stojmenovic, "Pairwise and triple key distribution in wireless sensor networks with applications", *IEEE Transactions on Computers*, Vol.62, No.11, pp.2224-2237, 2013.
[18] F. Zhan, N. Yao, Z. Gao, and G. Tan, "A novel key generation method for wireless sensor networks based on system of equations", *Journal of Network and Computer Applications*, Vol.82, pp.114-127, 2017.
[19] N. Suganthi and S. Vembu, "Energy efficient key management scheme for wireless sensor networks", *International Journal of Computers Communications & Control*, Vol.9, No.1, pp.71-78, 2014.
[20] U. Meena and A. Sharma, "Adequate Sparse Secure and Minkowski Distance Based Location Privacy Approach in Wireless Sensor Network", *International Journal of Intelligent Engineering and Systems*, Vol.10, No.3, pp.280-289, 2017.