EAI Endorsed Transactions
on Internet of Things
Research Article EAI.EU

Key Management for Hierarchical Wireless Sensor Networks: A Robust Scheme

Anubrata Chanda[1], Pampa Sadhukhan[1,*], Nandini Mukherjee[2]

[1]School of Mobile Computing & Communication, Jadavpur University, India - 700032.
[2]Dept. of Computer Sc. & Engineering, Jadavpur University, India - 700032.

Abstract

Secure data transmission within the wireless sensor networks (*WSNs*) is a critical issue as they are mostly deployed in the open areas. Moreover, the communication between the cluster head (*CH*) and the base station (*BS*) in a hierarchical *WSN* is required to be more secure since the *CH* is responsible for data collection, aggregation and its forwarding to the *BS*. Thus, this paper aims to design a hybrid key management scheme (*KMS*) for the hierarchical *WSNs* for enhancing security between the *CH* and *BS* by using some asymmetric cryptographic technique while applying the secret key based communication among the member nodes to reduce their computational overheads. The security analysis of our proposed scheme exhibits its robustness against the node capture attack and its ability to support the node revocation. The performances of proposed scheme are also evaluated in term of data freshness, average number of keys established, throughput and computational cost to demonstrate its efficiency.

Received on 29 April 2020; accepted on 27 September 2020; published on 02 October 2020

Keywords: wireless sensor network (*WSN*), key management scheme (*KMS*), hierarchical, symmetric, asymmetric, robust

doi:10.4108/eai.2-10-2020.166541

1. Introduction

Low-cost and small sensor nodes which are equipped with radio transceiver and low-power batteries can be effectively used in collecting various kinds of data like temperature, pressure, motion etc. On the other hand, wireless sensor networks (*WSNs*) is a collection of sensor nodes communicating via the wireless medium and deployed in a specific area in order to collect data and forward it to the *base station* (*BS*) or server for further processing it [1]. Thus, *WSNs* have significant usage in various domains such as environment monitoring, patient monitoring, military operations and so on. Since the nodes within the *WSNs* communicate through the wireless channel and mostly deployed in the open areas, an adversary can easily eavesdrop on the messages exchanged between the nodes or can alter the data carried by these messages and even the adversary can compromise some node. Thus, *WSNs* are highly vulnerable to various kinds of security attacks and threats.

The communication among two or more parties, in general, can be made secured by applying some cryptographic protocol that uses either some symmetric key (single secret key) or asymmetric keys (pair of public and private key) [2]. Managing such cryptographic keys by the resource-constrained sensor nodes is a major issue to securing communication among the nodes within a *WSN*. Various key management issues related to *WSNs* and also the requirements for key management by the *WSNs* have been pointed out in [3]. Although the asymmetric key based cryptographic techniques provide stronger security, but they require more buffer space and computations compared to the symmetric key based cryptographic techniques. Therefore, symmetric key based various key management schemes (*KMS*) for distributed *WSNs* [4–8] have been proposed in the literature in the last decade. However, such *KMSs* cannot be effectively applied to the hierarchical or cluster-based *WSNs* which are partitioned into several subsets (clusters) in order to carry out in-network

[*] Corresponding author. Email: pampa.sadhukhan@ieee.org

data processing in an efficient way. Various clustering algorithms proposed for *WSNs* have been reviewed in [9]. Thus, this paper focuses on designing some suitable *KMS* for hierarchical *WSNs*.

In a cluster-based *WSN*, the cluster head (*CH*) is responsible for aggregating the data received from other member nodes belonging to its cluster and then forwarding it to the sink node or base station (*BS*). For this reason, any adversary is more interested in attacking the *CH* or eavesdropping on the communication link between the *CH* and the *BS*. Hence, the *CHs* in a cluster-based *WSN* are more vulnerable to various kinds of security attacks compared to the ordinary member nodes, whereas the former are usually more powerful nodes compared to the latter if the *CHs* of a hierarchical WSN are selected based on maximal residual energy of the ordinary nodes. To address the above-mentioned issue, we aim to design a robust KMS based on the hybrid model, i.e., a combination of both symmetric and asymmetric cryptography, for the hierarchical WSNs in this paper. Our proposed scheme applies some asymmetric key based cryptographic technique on the communication link between the *BS* and the *CH* in order to make it more secure whereas it uses symmetric key based communication between any two member nodes or the *CH* and any other member node within a cluster in order to reduce the resource consumptions of the ordinary nodes. Therefore, the main contribution of this paper lies in designing a robust *KMS* based on the combination of symmetric as well as asymmetric cryptography for the hierarchical *WSNs* in order to provide stronger security to the communication link between the *CH* and the *BS* and also reduce the computational overhead and storage requirement of the ordinary sensor nodes. The robustness of our proposed scheme against the node capture attack and its ability to support the node revocation have been proved via the security analysis given in Section 4, whereas the effectiveness of our proposed scheme is demonstrated via its performance evaluations in term of the data freshness, average number of keys established and throughput using NS-3 [27] along with its performance analysis in terms of the computational cost provided in Section 5.

This paper is organized as follows. Section 2 reviews several key management techniques proposed for hierarchical or cluster-based *WSNs* in the literature over the past few decades. Our proposed *KMS* for hierarchical *WSNs* is described in detail in Section 3. The security analysis of our proposed scheme is given in Section 4. Section 5, at first, defines several performance metrics and then evaluates the performances of our proposed scheme in terms of those metrics. Finally, we conclude in Section 6.

2. Related Work

This section briefly reviews various key management schemes proposed for the hierarchical *WSNs* in the literature over the past few decades. The researchers in [10] have investigated the problem of designing secure communication protocols for cluster-based homogeneous *WSNs* and also proposed a solution for adding security to LEACH [11], a well-known protocol to create the clusters dynamically and periodically, by using some symmetric key based cryptographic technique. A *KMS* that can create secure communication link between the sensor nodes and the gateways based on public key cryptography within the cluster-based *WSNs* has been proposed in [12]. The proposed scheme does not need to pre-deploy a large number of keys into the sensor nodes rather it enables the ordinary sensor nodes to receive session keys from the gateway for establishing secure communication link with their neighbors. A secret sharing based *KMS* that has paid special attention to keys revocation and protection issues for hierarchical *WSNs*, has been proposed in [13]. The authors in [14] have proposed two secure protocols for data transmission within the cluster-based *WSNs* based on identity-based digital signature (IBS) as well as identity-based online/offline digital signature (IBOOS) technique. Another *KMS* proposed for *WSNs* uses a hierarchical network topology in terms of generating the keys and their distribution in order to distribute the tasks of key management among various levels of nodes and also to minimize each node′s storage for the keys [15].

An efficient key management scheme that can establish three types of keys to enable secure communication among the sensor nodes for a hierarchical *WSN* has been proposed in [16]. Apart from the key establishment, the proposed *KMS* also includes key transportation and dynamical freshness of keys. However, the establishment and maintenance of three different types of keys which are network key, group key and pair wise key increases the memory consumption as well as computational overhead of each ordinary sensor node. A hierarchical *KMS* that employs identity-based encryption (IBE), has been proposed in [17]. The proposed scheme converts a *WSN* in the form of distributed flat architecture into the hierarchical architecture before applying *KMS* which is based on Boneh-Franklin and Diffie-Hellman (DH) algorithms. A polynomial and multivariate mapping-based triple-key (PMMTK) distribution approach that generates a collective key (named as triple-key) in order to establish secure communication between the ordinary member nodes, *CH* and *BS* in the hierarchical *WSNs*, has been proposed in [18]. The proposed PMMTK approach can enhance the security of the *WSNs* without increasing memory consumption of the sensor nodes. A combined approach of pairwise and triple-key distribution mechanisms has been proposed in [19]. On the other hand, Inter-Cluster Multiple Key Distribution Scheme (ICMDS) that attempts to enhance the security of the *CH* in the multi-hop clustering environment, has been proposed in [20]. The proposed ICMDS needs to pre-deploy a master key into each sensor node and implements *CH*'s security in two phases by using both secret key as well as public key cryptographic technique.

Among the recently proposed works on the *KMS* for *WSNs*, a self-managing key scheme, which inserts the volatile master keys, i.e., master keys having very short life time, into a subset of all sensor nodes only in order to reduce their chances of obtaining by any attacker, has been proposed in [21]. The proposed scheme uses *symmetric cryptography* for generating the keys needed for establishing secure communication between the adjacent nodes. The researchers in [22] have proposed a light weight authentication protocol for hierarchical *WSNs*, in which the *CH* is assigned full responsibility of authenticating all the member nodes belonging to its cluster, in order to preserve the privacy of data within the *WSNs*. Since most of the polynomial-based *KMSs* proposed for *WSNs* are vulnerable to node capture attacks, a novel polynomial-based *KMS* integrated with *probabilistic security feature* has been proposed in [23] in order to reduce the security risks associated with the node capture attacks. Another light weight symmetric cryptography based *KMS* proposed by the researchers in [24], attempts to reduce the size of the *secret key*, which is shared among the nodes within the network, for the purpose of reducing the overall communication overhead incurred by the key distribution process. A key establishment scheme for hierarchical *WSNs*, which attempts to establish the pair-wise keys in order to support both intra-cluster communication as well as inter-cluster communication within the hierarchical *WSNs*, has been proposed in [25].

3. Proposed Key Management Scheme

This section presents our proposed key management scheme (*KMS*) in detail. At first, the clustering procedure along with *CH* selection mechanism adopted by our proposed scheme is given in Subsection 3.1. Then the proposed key generation and distribution technique is described in Subsection 3.2.

3.1. Clustering Procedure and Selection of Cluster Head

The network architecture of a typical hierarchical *WSN* is shown in fig. 1. A secret value (SV) is assigned and stored into the memory of each sensor node before its deployment into the target area. Initially, the network of sensor nodes is partitioned into a set of clusters in some random way. After formation of the clusters, each node is assigned a unique id by combining the cluster number and the local node id. The distances between each pair of nodes within the cluster are also computed. The node having shortest distance from the other nodes within a cluster, i.e., the centroid node of the cluster is selected as the *CH* in the first step. But, in successive steps, some centroid node having minimum residual energy is elected as the *CH* of the cluster.

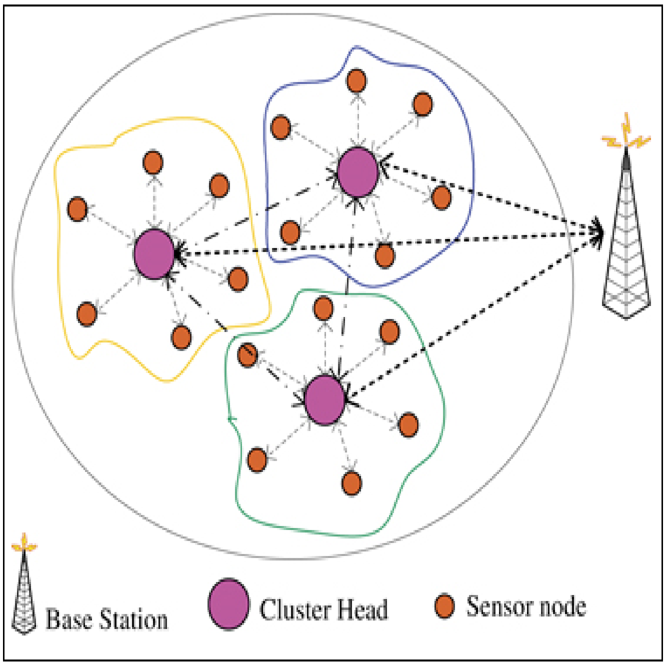

Figure 1. Network architecture of a typical hierarchical *WSN*

Table 1. List of notations used by proposed *KMS*

Id	Description
q	A large prime number
G	A cyclic additive group of order q
P	The generator of G
Z_q^*	$(1,2,\cdots,q-1)$
ID_{CH}	Node id of cluster head
T_{CH}	Timestamps contained in beacon packet sent by *CH*
SV_{CH}	Secret value assigned to *CH*, where $SV_{CH} \in Z_*^q$
SV_i	Secret value assigned to i^{th} sensor node, where $SV_i \in Z_*^q$
r_{BS}	A random number chosen by *BS*, where $r_{BS} \in Z_*^q$

3.2. Proposed Key Generation and Distribution Technique

The proposed *KMS* generates and distributes both kinds of keys, i.e., symmetric as well as asymmetric keys in

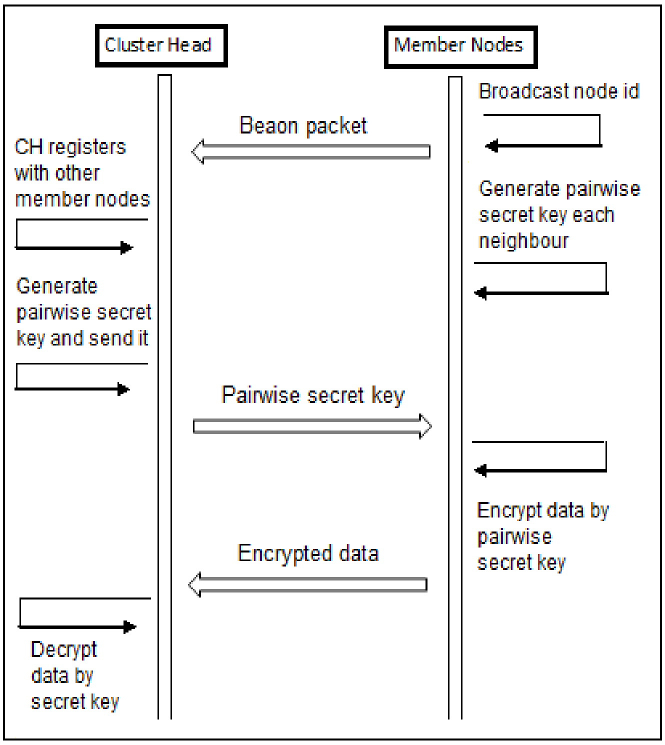
Cluster Head
Member Nodes
Broadcast node id
Beaon packet
CH registers with other member nodes
Generate pairwise secret key each neighbour
Generate pairwise secret key and send it
Pairwise secret key
Encrypt data by pairwise secret key
Encrypted data
Decrypt data by secret key

Figure 2. Sequence diagram of secure communication between the *CH* and its member nodes

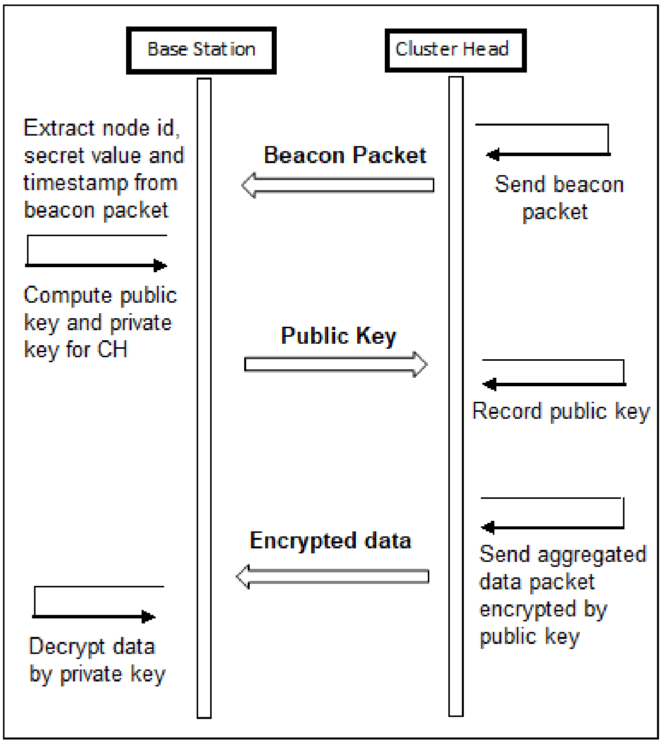
Base Station
Cluster Head
Extract node id, secret value and timestamp from beacon packet
Beacon Packet
Send beacon packet
Compute public key and private key for CH
Public Key
Record public key
Encrypted data
Send aggregated data packet encrypted by public key
Decrypt data by private key

Figure 3. Sequence diagram of secure communication along with the key exchange procedure between the *CH* and *BS*.

order to provide better security to the communication link between the *CH* and the *BS* without increasing the buffer requirement and computational overhead of the ordinary sensor nodes. Thus, the proposed key generation and distribution technique can be divided into two parts which are described in detail below. Various notations used by our proposed *KMS* are provided in table 1.

3.2.1 Keys Generation and Distribution within a Cluster

The communication between any two nodes within a cluster is encrypted using a separate secret key, that means, a pair-wise secret key (SK) for node i and node j within a cluster is generated by applying cryptographic hash function in the following way.

$$SK_{ij} = H_1(i,j)\,,\ H_1 : \{0,1\}^* XG \rightarrow Z_*^q, \qquad (1)$$

where i and j are the positive integers and refers to the local id values of i^{th} and j^{th} sensor node respectively. Thus, any data packet sent by an ordinary member node to the *CH* is encrypted by the pair-wise *SK* corresponding to them and the *CH* can decrypt it by using the same SK. The sequence diagram of secure communication between the *CH* and ordinary member nodes is shown in fig. 2.

3.2.2 Keys Generation and Distribution between the *CH* and the *BS*

After formation of the clusters as well as selection of the CHs, when *BS* receives the beacon packet from a new *CH*, the *BS* attempts to generate the pair of private and public key for that *CH* based on its node id (ID_{CH}), secret value (SV_{CH}) and the time stamp (T_{CH}) given in the beacon packet. The procedure of generating the pair of private and public key for the mobile node by the AAA server proposed in [26] has been adopted by the *KMS* proposed in this paper for key generation purposes. The *BS* executes the following set of equations in sequence in order to generate the key pair for the *CH*.

$$\begin{gathered} C_{CH} = SV_{CH} \cdot P \\ R_{BS} = r_{BS} + C_{CH} \cdot P \\ d_{BS} = (H_1(ID_{CH}, R_{BS}) \cdot T_{CH} - r_{BS})\ mod\ q \\ S_{CH} = (d_{BS} - SV_{CH})\ mod\ q \\ PK_{CH} = S_{CH} \cdot P \end{gathered} \qquad (2)$$

The *BS* uses the set (PK_{CH}, C_{CH}) as the private key and (S_{CH}, SV_{CH}) as the corresponding public key for the *CH*. Afterward, the generated public key is distributed to the *CH* while the corresponding private key is retained by the *BS* without revealing it to the others. Fig. 3 shows the sequence diagram of secure communication along with the key exchange procedure between the *CH* and the *BS*. After receiving several encrypted data packets from the member nodes, the *CH* at first, decrypts them using the pair-wise SKs established between the member nodes and it, then aggregates them and finally encrypts the aggregated data by using its public key before forwarding it to the *BS*. After reaching at *BS*, the aggregated data packet is decrypted using the private key of the corresponding *CH*.

4. Security Analysis

Our proposed *KMS* has sufficient potential for network resistance and resilience against node capture as well as it supports node revocation as explained below.

- **Network resistance:** If an adversary attacks the network by compromising several nodes including at least one *CH* and replicates them back into the network, our proposed *KMS* prevents the adversary to gain full control of the network since each *CH* is provided a separate pair of private and public key and also the key pair is renewed periodically by our proposed scheme.
- **Node revocation:** Since our proposed *KMS* generates the pair of private key and public key based on the current time stamp, it can easily revoke any compromised *CH* by creating a new key pair for it.
- **Resilience:** If the adversary captures an ordinary sensor node, it cannot obtain secret keys of the other nodes as well as that of the *CH* since a unique secret key for each pair of nodes is generated by our proposed scheme. On the other hand, by capturing a *CH*, adversary cannot obtain key information of other CHs as well as the *BS*.

5. Performance Evaluation

We have implemented our proposed *KMS* using $NS-3$ simulator [27] and evaluated its performance in terms of data freshness, average number of keys established, throughput and computational cost also. At first, various performance metrics have been defined in Subsection 5.1 and then the graphical results are provided in Subsection 5.2.

5.1. Performance Metrics

The following metrics have been considered to evaluate the performances of our proposed scheme.

i. **Data Freshness -** it is defined as ratio of the data packets received by a *CH* to the total number of packets sent by the ordinary member nodes during one communication cycle [18]. So, it is computed as follows.

$$Data\,freshness(\%) = \frac{P_{CH}}{P_N} \times 100,$$

where $P_{CH} \leftarrow$ number of packets received by a *CH* and $P_N \leftarrow$ total number of packets sent by ordinary member nodes.

ii. **Average number of keys establishment -** it is counted for each round. A single secret key is required between each pair of ordinary sensor nodes whereas a pair of public key and private key are used for communication between the *BS* and each *CH*.

iii. **Throughput -** it is defined as the total number of bits successfully sent through a communication network per time unit.

iv. **Computational cost -** The computational complexity incurred by our proposed scheme to generate various keys is as follows.

(a) *Key between any two ordinary nodes* - Our proposed scheme applies $q-bit$ hash function given in equation 1 to generate the secret key for any pair of ordinary nodes. So, the computational complexity incurred by generation of such key is $O(q)$.

(b) *Key between an ordinary node and CH* - Since the communication between a member node and the CH relies on a secret key generated by the $q-bit$ hash function given in equation 1, hence its computational complexity is $O(q)$.

(c) *Key between CH and BS* - The Generation of the pair of private key and public key to be used on the communication link between the CH and the BS relies on a polynomial of degree q as given in equation 2, So its computational complexity is $\Theta(q^2)$.

5.2. Graphical Results

Fig. 4 shows that the value of data freshness increases with longer duration of the simulation time. This happens because the data packets sent by the ordinary sensor nodes before the establishment of the pair wise secret keys between them and the *CH* are rejected by the *CH* as invalid packets.

Fig. 5 depicts that average number of keys established increases linearly with the increasing number of nodes within the network. So, the amount of buffer required to store the keys remain fixed for a static network.

The throughput (in bits/second) achieved by the network at different time interval during the simulation is shown by fig. 6. Fig. 6 depicts that the network

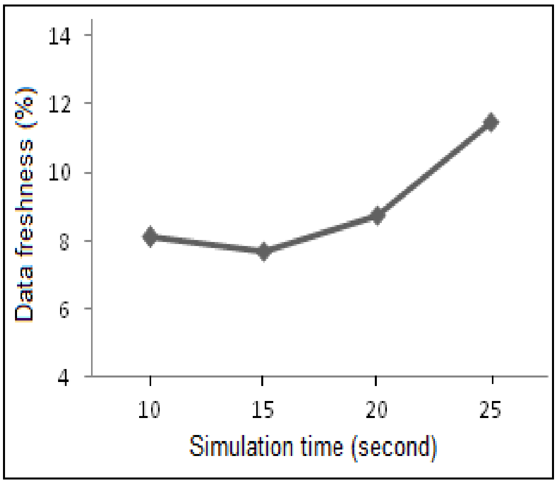

Figure 4. Data freshness vs simulation time

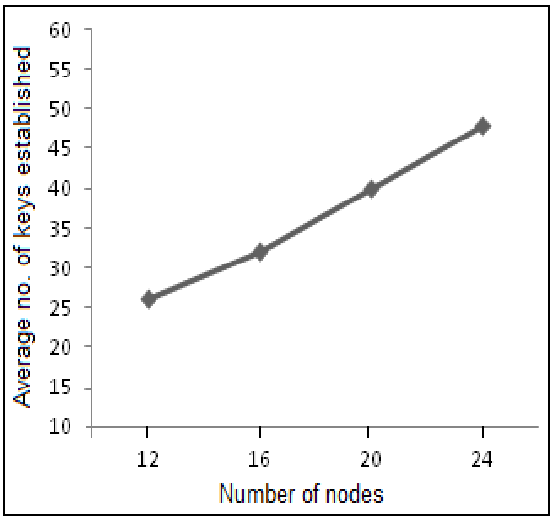

Figure 5. Average no. of keys established vs no. of nodes within network.

throughput achieved by our proposed scheme remains good at different time interval during the simulation period.

6. Conclusions

This paper proposes a robust and hybrid key management scheme for the large-scale hierarchical *WSNs* to provide better security to the cluster heads without increasing the computational overhead and memory consumption of the ordinary sensor nodes by combining both symmetric key as well as asymmetric key cryptographic techniques. The security analysis of our proposed *KMS* given in this paper leads to the conclusion that our proposed scheme has sufficient potential for network resistance and resilience against node capture and also supports node revocation.

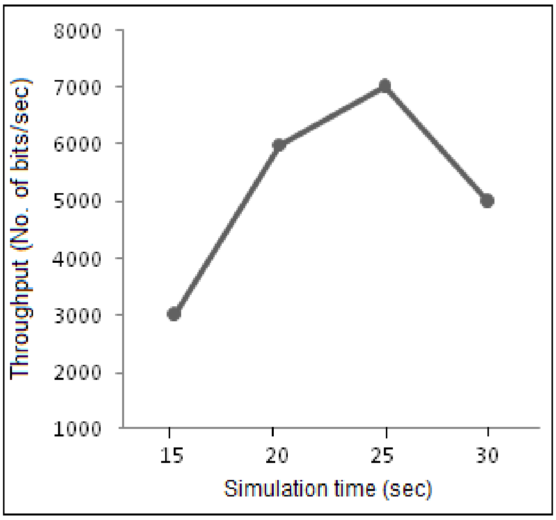

Figure 6. Throughput in bits/second vs simulation time.

Moreover, the performances of our proposed scheme are evaluated using *NS-3* in term of data freshness, average number of keys established and throughput as well as its performance is also analyzed in terms of computational cost to demonstrate its efficiency.

7. Copyright statement

The Copyright licensed to ICST.

Acknowledgement. The authors gratefully acknowledge the facilities and support provided by the Director and all other staff members of the School of Mobile Computing and Communication, Jadavpur University, a Center of Excellence set up under the ″University with potential for Excellence″ Scheme of the UGC.

References

[1] J. Zheng and A. Jamalipour, ″Wireless Sensor Networks: A Networking Perspective″, ISBN: 978-0-470-16763-2, Wiley.

[2] S. Bose and A. Kumar, ″Cryptography and Network Security″, ISBN: 9789332579125, Pearson Education India.

[3] J. C. Lee, V. C. M. Leung, K. H. Wong, J. Cao and H. C. B. Chan, ″Key management issues in wireless sensor networks: current proposals and future developments,″ IEEE Wireless Communications, vol. 14, no. 5, pp. 76-84, October 2007.

[4] A. Perrig, R. Szewczyk, J.D. Tygar, V. Wen, D. Culler,″SPINS: security protocols for sensor networks,″ Wireless Networks 8 (5) (2002), pp. 521-534.

[5] T. Park, K.G. Shin, ″LiSP: a lightweight security protocol for wireless sensor networks,″ ACM Transactions on Embedded Computing Systems (TECS) 3(3) (2004), pp. 634-660.

[6] J. Lee, D.R. Stinson, ″Deterministic Key Predistribution Schemes for Distributed Sensor Networks,″Proceedings of SAC 2004, Lecture Notes in Computer Science, Vol 3357. Springer, Berlin, Heidelberg.

[7] S. Zhu, S. Setia, S. Jajodia, ″LEAP+: efficient security mechanisms for large-scale distributed sensor networks,″ ACM Transactions on Sensor Networks 2(4), 2006, pp. 500-528.

[8] S. A. Camtepe and B. Yener, "Combinatorial Design of Key Distribution Mechanisms for Wireless Sensor Networks," in IEEE/ACM Transactions on Networking, Vol. 15, No. 2, April 2007, pp. 346-358.

[9] A. A. Abbasi and M. Younis ″A survey on clustering algorithms for wireless sensor networks, ″Computer Communications, Volume 30, Issues 14–15, 15 October 2007, pp. 2826-2841.

[10] A.C. Ferreira et al., ″On the Security of Cluster-Based Communication Protocols for Wireless Sensor Networks,″ In: Lorenz P., Dini P. (eds) Networking - ICN 2005. ICN 2005. Lecture Notes in Computer Science, vol 3420. Springer, Berlin, Heidelberg.

[11] W.R. Heinzelman, A. Chandrakasan, H. Balakrishnan, ″Energy-efficient communication protocol for wireless microsensor networks,″ IEEE Hawaii Int. Conf. on System Sciences, 2000, pp. 4-7.

[12] R. Azarderakhsh, A. Reyhani-Masoleh and Z. Abid, "A Key Management Scheme for Cluster Based Wireless Sensor Networks," 2008 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, Shanghai, pp. 222-227.

[13] Jia Hu, Enjian Bai and Yang Yang, ″A novel key management scheme for hierarchical wireless sensor networks,″ 2010 IEEE 12th International Conference on Communication Technology, Nanjing, 2010, pp. 526-529.

[14] H. Lu, J. Li and M. Guizani, ″Secure and Efficient Data Transmission for Cluster-Based Wireless Sensor Networks,″ IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 3, pp. 750-761, March 2014.

[15] A.S.M.S. Hosen, Gideon, G. Cho ″A Robust Key Management Scheme Based on Node Hierarchy for Wireless Sensor Networks,″ In B. Murgante et al. (eds) Computational Science and Its Applications – ICCSA 2014, Lecture Notes in Computer Science, vol 8580. Springer, Cham, pp 315-329.

[16] X. Zhang and J. Wang, ″An efficient key management scheme in hierarchical wireless sensor networks,″ 2015 International Conference on Computing, Communication and Security (ICCCS), Pamplemousses, 2015, pp. 1-7.

[17] S. Hu, ″A hierarchical key management scheme for wireless sensor networks based on identity-based encryption,″ 2015 IEEE International Conference on Computer and Communications (ICCC), Chengdu, 2015, pp. 384-389.

[18] A. R. Selva and E. Baburaj, ″Polynomial and multivariate mapping-based triple-key approach for secure key distribution in wireless sensor networks,″ Computers and Electrical Engineering 59 (2017), pp. 274-290.

[19] S Ruj, A Nayak, I. Stojmenovic, ″Pairwise and triple key distribution in wireless sensor networks with applications,″ IEEE Trans Comput 2013, Vol. 62, No. 11, pp. 2224-2237.

[20] A. Mehmood, M. M. Umar, H. Song, ″ICMDS: Secure inter-cluster multiple-key distribution scheme for wireless sensor networks,″ Ad Hoc Networks 55 (2017), pp. 97-106.

[21] A. Laouid et al, ″A self-managing volatile key scheme for wireless sensor networks,″ Journal of Ambient Intelligence and Humanized Computing, 10(9), 2019, Springer, pp.3349-3364.

[22] D. Liu et al., ″Lightweight and practical node clustering authentication protocol for hierarchical wireless sensor networks,″ International Journal of Sensor Networks, 27(2), 2018, pp.95-102.

[23] A. Albakri, L. Harn and S. Song, ″Hierarchical key management scheme with probabilistic security in a wireless sensor network (WSN),″ Security and communication networks, Vol. 2019, DOI: https://doi.org/10.1155/2019/3950129.

[24] K. Hamsha and G. S. Nagaraja, ″Threshold cryptography based light weight key management technique for hierarchical WSNs,″ International Conference on Ubiquitous Communications and Network Computing, Feb., 2019, pp. 188-197, Springer, Cham.

[25] S. Prema, and T. C. Pramod, ″Key establishment scheme for intra and inter cluster communication in WSN,″ 2018 IEEE Second International Conference on Computing Methodologies and Communication (ICCMC), February, 2018, pp. 942-944.

[26] S. Biswas, P. Sadhukhan, S. Neogy,″An Asymmetric Key Based Efficient Authentication Mechanism for Proxy Mobile IPv6 Networks,″S.M. Thampi et al. (Eds): Security in Computing and Communications (SSCC) 2017, CCIS 746, ISBN: 978-981-10-6897-3, pp. 65-78, 2017, Springer, Singapore.

[27] https://www.nsnam.org/releases/ns-3-26/.