Journal of Engineering Research and Reports

Volume 25, Issue 12, Page 162-170, 2023; Article no.JERR.110565
ISSN: 2582-2926

Secret Key Management in Wireless Sensor Network Based on Probabilistic Technique

Aniebiet Effiong Bassey [a*], Enyenihi Henry Johnson [a] and Gabriel Etim Umoh [a]

[a] *Department of Electrical and Electronic Engineering, Akwa Ibom State University, Ikot Akpanden, Mkpat Enin L.G.A, Akwa Ibom State, Nigeria.*

Authors' contributions

This work was carried out in collaboration among all authors. All authors read and approved the final manuscript.

Article Information

DOI: 10.9734/JERR/2023/v25i121049

Open Peer Review History:
This journal follows the Advanced Open Peer Review policy. Identity of the Reviewers, Editor(s) and additional Reviewers, peer review comments, different versions of the manuscript, comments of the editors, etc are available here:
https://www.sdiarticle5.com/review-history/110565

Original Research Article

Received: 14/10/2023
Accepted: 20/12/2023
Published: 26/12/2023

ABSTRACT

Data confidentiality implies that data access is limited to authorized entities only, thus measured data and transmitted data by wireless sensors require optimum security and privacy. Various techniques have been employed to implement effective security mechanisms for a wireless sensor network. However, the arsenal of these potential solutions is useless, considering the constrained nature of the Wireless Sensor Network (WSN) resources in terms of memory, processing and computational capacity. While considering an effective solution for this situation, care must be taken not to trade the desired solution for other factors. This paper considers the implementation of a probabilistic approach for key management in WSN. In the implementation, all kinds of communication within the wireless sensor nodes are presented by forwarding encrypted keys for mutual authentication. A successful authentication opens a communication channel for the communicating nodes. The encrypted keys are computed by generating a polynomial which constitutes the hashed ID concatenated with the master key and Message Authentication Code

---

Corresponding author: Email: aniebietbassey980@yahoo.com;

(MAC) address of the node. The results presented from the simulation of this model are benchmarked with the Dynamically Generated Polynomial (DGP). The proposed model was simulated using MATLAB tools and the comparison of the results obtained shows that the proposed model outperforms the DGP model by 87%, based on the key metrics which are energy consumption, storage and communication overhead.

Keywords: Wireless sensor network; energy consumption; cluster head; sensor node; base station.

1. INTRODUCTION

Technological advancement, in the last two decades, has boldly pronounced the relevance of Wireless Sensor Networks (WSN) in many applications [1-4]. In real-world circumstances, WSNs are mostly deployed in harsh, isolated, and/or autonomous areas which are generally not human-friendly. Few specific areas of application of WSN include military [5], hospital [6], home [2], and industries [7]. If WSN is applied in the military, such information as intrusion, speed, position, acceleration [8], and radar [9] could be some interesting quantities to monitor the opponent. In hospital applications, Internet of Things (IoT) could offer monitoring of quantities such as blood pressure, body temperature, and heartbeat. In homes and industries, quantities such as temperature of the surroundings, gas leakage, humidity of the surrounding illumination, and intrusion could be measured with WSN.

Despite the promising advantage of WSN, the area of security has kept researchers active in their quest to find a solution to such a lingering problem. In the application instances presented above, all the data collected by the sensors are confidential and should not be revealed to unauthorized persons in an ideal situation. For instance, an enemy who has access to the military tracking information could use the information to fortify their defense.

Usually, data is transmitted within the sensor network which includes the sensor nodes, the cluster heads, and the base station [10]. Before Data transmission, information is encrypted along with the sender’s and receiver’s identity. This unique identity is what the members within the cluster or network use for identification. If an attacker could clone the key of any member node, then such an attacker could mimic the member node to perform malicious activities within the network. Surprisingly, many efforts contributed by various researchers found in [11-15] have not been able to provide a balanced solution to the impending problem. In some cases, the solution to security problems becomes a tradeoff to other factors such as computational overhead, shortened network lifespan, and communication overhead.

It is important to consider the fact that WSN is made up of resource-constrained devices, hence overloading it with heavy algorithms will eventually lead to more problems than what the proposed algorithm seeks to solve. Hence, this paper proposes a probabilistic solution to secret key management for effective security. This technique ensures that a good balance is maintained between securities, energy consumption, computational overhead, and communication overhead.

2. METHODOLOGY

This paper focuses on session key establishment and mutual authentication between communicating nodes. During key establishment, all nodes within the network take part in the authentication process, hence this scheme is a Multi-Party Keying Scheme (MPKS). The system model is presented in Fig. 1. In this paper, it is assumed that cluster heads are high-powered nodes while other sensor nodes are resource-constrained.

During cluster key setup, a cluster head (CH) receives encrypted IDs of all the member nodes within the network. Each of the received encrypted IDs is decrypted with the master key KM stored in the cluster head. This master key is pre-loaded to all the network members before installation. Once the IDs are unmasked, a hash of these IDs is computed and stored in memory as illustrated in Fig. 1. After computing the hash of all the IDs, the cluster head calculates the polynomial by randomly selecting some hashed IDs from the hash pool. To have a secure identity and subsequent authentication of members of the network, the polynomial is concatenated with Message Authentication Code (MAC) using the pre-distributed master key. This encrypted symbol is then transmitted to all the member nodes within the network.

The constituents of the polynomial preloaded to every related node include; master key, hash function, encryption and decryption functions along with a distinctive ID by the sink. In this paper, elliptical cryptographic curve (ECC) algorithm is used to develop the secure mechanism. The application of ECC ensures that no input can be obtained by its corresponding output. The CH transmits this request after securing it to sink that verifies the request and responds to the CH granting or declining this request. The response that goes to the CH contains the encrypted text which is as integral of the ID of the individual nodes, and $MAC(ID_{Li})$. The encryption text is represented as: $E_{KM}(ID_{LI}\,||\,MAC(ID_{LI}))$, where KM denotes the master key. At this point, the CH has to compute the polynomial P_δ using the model presented in Eqn. (1) and (2).

$$P_\delta = \left(x - \delta_a(ID_{La})\right)XOR\left(x - \delta_{a+1}(ID_{La+1})\right)\ldots XOR\left(x - \delta_{a+\gamma}(ID_{La+\gamma})\right) \tag{1}$$

$$P_\delta = \left(x - \delta_a(ID_{La})\right)XOR\left(x - \delta_b(ID_b)\right)\ldots XOR\left(x - \delta_c(ID_c)\right) \tag{2}$$

Where, x is a pre-defined positive integer, and the hash δ is calculated for all nodes unique identifier within the network (i.e., ID_{L_a} to $ID_{L_{a+\gamma}}$, where γ denotes the number of clusters). To mitigate the computational overhead, this model applies the XOR operator on the conglomerate of randomly selected hashes from the hash pool. The number of hashed IDs to be selected for the XOR operation depends on the randomnization index R_i and in this research, $R_i = 3$. It should be noted that the hash for all the sensor node unique identifiers is generated at the initialization stage as shown in Algorithm 1. Array of all the node unique identifiers is defined as N_{IDs}, and the array that contains all the corresponding hash IDs for N_{IDs} is defined as: $A_{h(ID)}$.

Algorithm 1. Polynomial Generator

```
Begin
Define and initialize $N_{IDs}$
Define and initialize $A_{h(ID)}$
Define and initialize $P_\delta$
for i=1 to $sizeof(N_{IDs}) - 1$
    $A_{h(ID)}[i] = hash(N_{IDs}[i])$
end for
Set $R_i$ as Array
$P_\delta = x - A_{h(ID)}[R_i[0]]$
for i=1 to $sizeof(R_i) - 1$
    $P_\delta = P_\delta XOR\left(x - A_{h(ID)}[R_i[i]]\right)$
end for
End
```

2.1 New Node Integration

In certain circumstances, there might be need to add new nodes to the sensor network. In such case, the base station is in charge and is responsible to authenticate and initiate the establishment phase. During the establishment phase, base station (BS) broadcasts the new sensor to the cluster head after the sensor node is pre-loaded with a hash function $\delta(\cdot)$, and master key KM. The base station encrypted broadcast contains $nounce_B$, $N_{ID_{Li}}$ (list of L-sensor IDs) and message authentication code (MAC) address ($MAC_{ADRS_{ID_{Li}}}$) to all cluster heads. Cluster head responds by sending encrypted text containing ID_{CH} and $nounce_B$; it also publishes the encrypted version of the list of member nodes, the session key and MAC. This facilitates the authenticity of the concatenation process. The node integration algorithm is presented in Algorithm 2.

Algorithm 2. New Node Integration

```
1:  $BS \rightarrow CH: E_{K_{CB}}\left[\left(nounce_B, MAC_{ADRS_{ID_{Li}}}, N_{ID_{Li}}, T_1\right)\right], ||[h(CH_{ID})]$
2:  $CH \rightarrow BS: E_{K_{CB}}[(ID_{CH}, nounce_B, T_2)]\,||[h(BS_{ID}), h(ID_{CH})]$
3:  $CH \rightarrow L_i: E_{K_{CH_j}}\left(K, MAC_{L_i}\,||List_{L_i}\,||T_3\right)$
4:  $CH$: Verify using secrete credentials
5:  $L_i \rightarrow CH: E_{K_M}\left(ID_{Li}\,||\,MAC_{ADRS_{ID_{Li}}}\right)$
6:  $CH$: Regenerate polynomial $P$, upon adding a new node
7:  $CH \rightarrow L_i: E_{K_M}(P_h, nounce_{CH})$
8:  $L_i \rightarrow CH: E_{K_{CL}}(nounce_{CH}, ID_{Li})$
```

The setup phase is implemented in line 1 – 4 while the joining phase is implemented in line 5 – line 8.

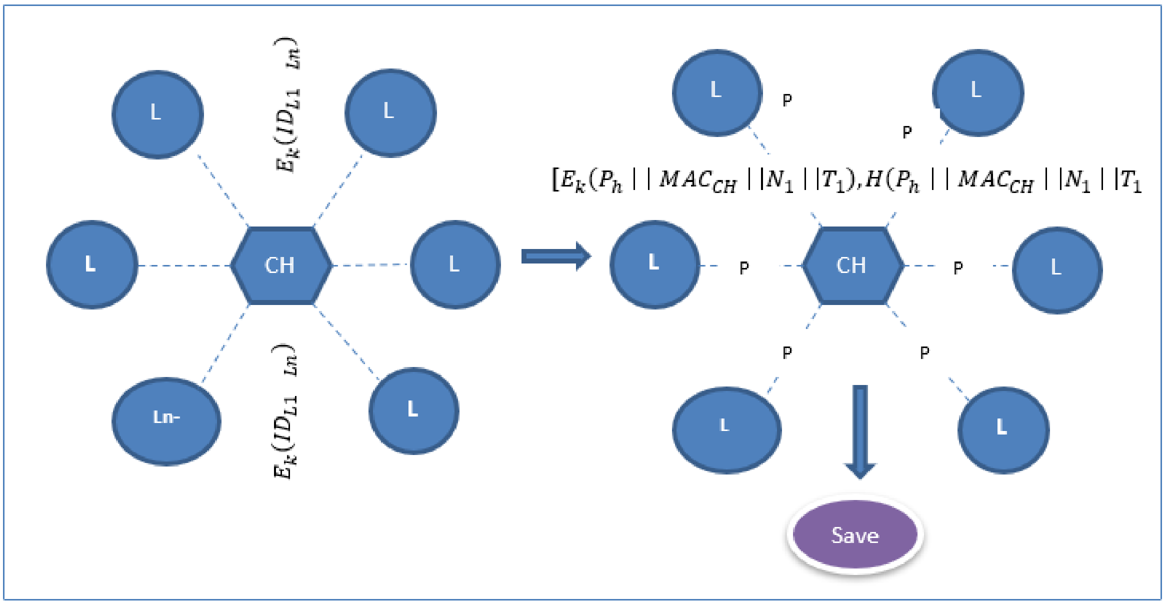

Fig. 1. System model

3. RESULTS AND DISCUSSION

3.1 Evaluation of Polynomial Based Key Distribution Scheme with Probabilistic Security

The proposed scheme is simulated using MATLAB Software. High-capacity sensors marked as (H-sensors) are configured differently with 10,000 Joules of energy, and message reception and sending has a cost of $0.049\,J$, and $0.5809\,J$ respectively. The transmission radius for both the low resourced sensors and high resourced sensors are set at $50\,m$ and $300\,m$, respectively. Five clusters having distinct sizes ranging from 10 to 100 in a region of $1300 \times 1300\,m$ are used for measurement. The performance metrics to be considered in the results evaluation are: Time latency, communication overhead, storage overhead, and energy consumption. The results of the proposed model presented in this paper will be compared to those presented in [13].

3.2 Performance Evaluation of Time Latency

During communication within the sensor node, the time required to transmit packet from a cluster head to a member node is defined as latency. A significant reduction in latency for the proposed model with respect to the DGP model is observed as shown in Table 1 and Fig. 2. The result in the proposed model was obtainable by allowing the model to compute the anchor protocol for session key and final time, hence minimizing the time lag on cluster head. It was also ensured in the proposed model that the cluster heads and the sensor nodes within the cluster took part in generating session key. This concept eliminates the delay incurred by generating the session key for each cluster nodes. Again, Table 2 and Fig. 3 show the energy requirement for communication among the nodes.

From the results presented in Fig. 2, time latency increases as the number of clusters increase on both schemes. However, it is observed that the rate of increase on the proposed model is slower compared to the DGP model, hence makes the proposed model a better option especially when many nodes are involved.

In terms of energy consumption, Fig. 3 shows that the proposed model maintains lower and almost constant energy consumption for a greater number of nodes added. On the other hand, the DGP energy consumption curve shows that there is a drastic increase in energy consumption for number of additional nodes more than two.

Table 1. Time latency performance

Number of nodes within network	latency $(seconds)$	
	Proposed model (MPKS)	DGP model
10	38.4	86.1
20	52.3	150.4
30	97.5	230.6
40	105.2	305.2
50	139.7	399.7
60	170.8	472.1
70	193.1	530.7
80	204.7	624.2
90	241.4	699.8
100	286.2	784.3

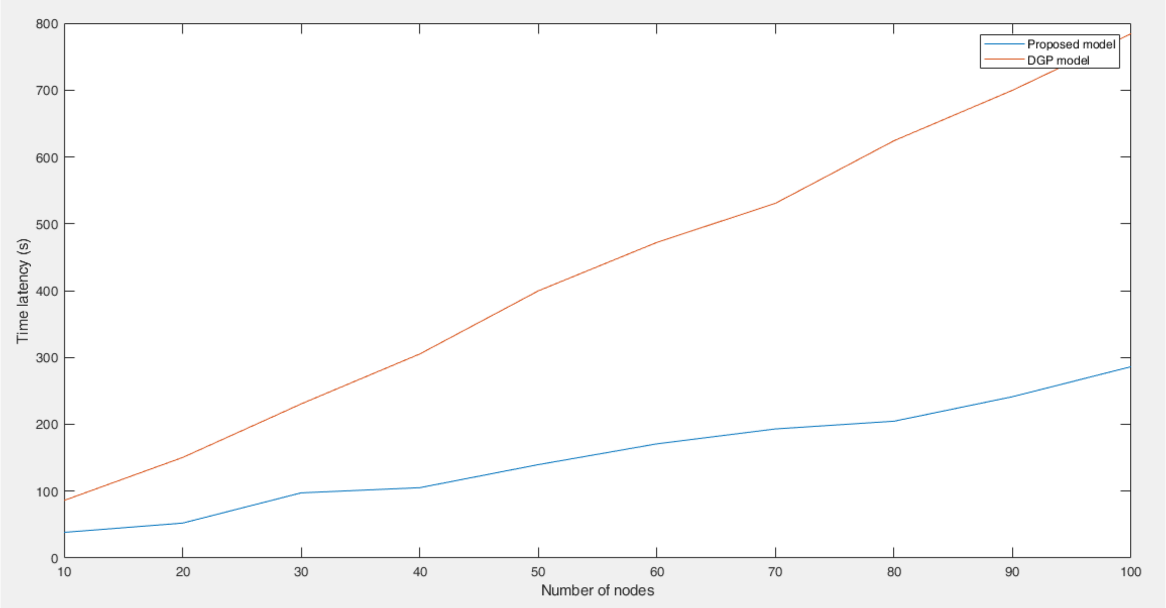

Fig. 2. Time latency performance

Table 2. Energy requirement for communication among the nodes

Number of additional nodes	Energy consumption $(\mu J/byte)$	
	Proposed model (MPKS)	DGP model
1	0.125	0.156
2	0.137	0.221
3	0.146	0.502
4	0.153	0.611
5	0.161	0.798
6	0.174	0.984
7	0.182	1.362
8	0.194	1.537
9	0.208	1.712
10	0.212	1.935

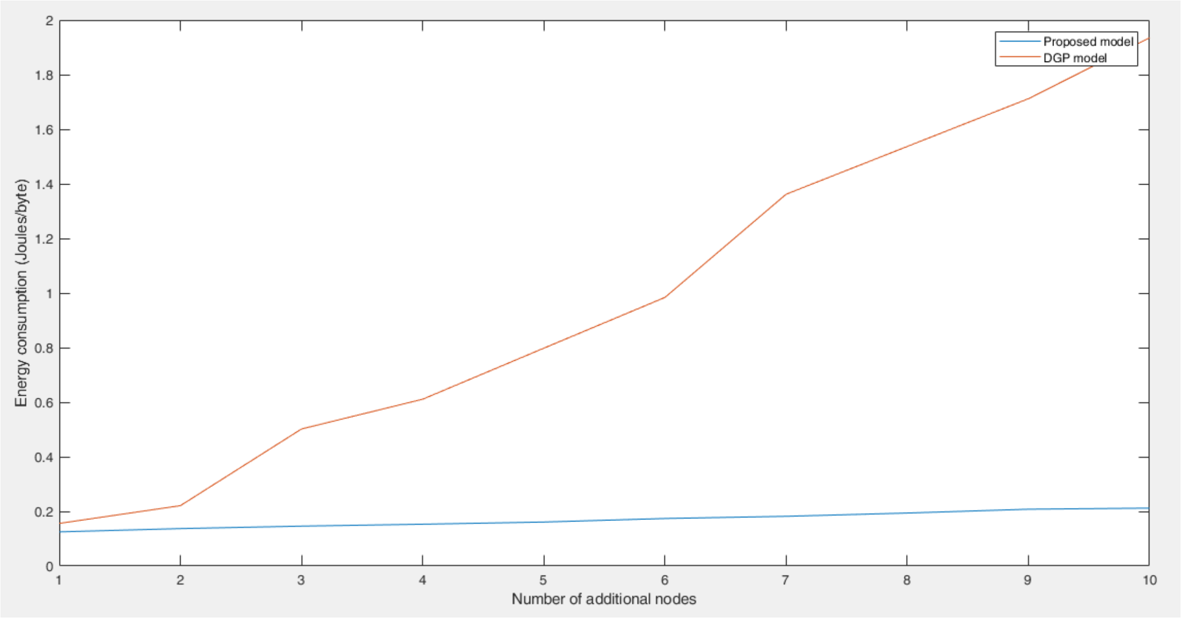

Fig. 3. Energy requirement for communication among the nodes

3.3 Performance Evaluation of Communication Overhead

The expense of communication in wireless sensor network is defined as the ratio of transmitted packet to received packet. In this evaluation, the energy consumption cost for transmitting a byte T_c is measured as $56.3\mu J/byte$, and the energy consumption cost for receiving a byte R_c is measured as $22.7\mu J/byte$. Hence, the wholesome energy consumption cost for effective communication between two points is defined as: $m \times (T_c + R_c)$, where m denotes the message count. If the communication cost is too high, the energy consumed will be high, hence, the lifespan of the network will be reduced since network lifespan and energy consumed in the network are inversely proportional. In the proposed designed presented in this research, a lightweight mechanism is introduced for client authentication of the wireless sensor network in the IoT scenario, which relies on some hash function and XOR computations. Specifically, the novelty introduced in this research is based on the sensor-hub initial-contact technique, coupled with the security features; the cluster heads and the sensor hub are required to carry the weight.

During node migration, the proposed model refreshes its associated keys to fasten security, but then, the underlying cost of this effect has no significant impact on the communication cost. To evaluate the cost of communication, the entire parameters of the cluster head required to save in node memory while performing signup and authentication are computed. The size of each variable is also computed. The performance analysis on the communication cost in terms of data exchange size at registration phase, node addition phase and node migration phase is presented in Table 3 and Fig. 4.

Fig. 4 shows that communication cost is intensive during node migration, followed by node addition and then node registration. The intensive requirement for node migration is due to the fact that three parties are involved which include: the base station, and two cluster heads (the sender and the receiver), whereas, in node addition, only the base station and one cluster head is involved. In any case, the result presented in Fig. 4 shows that the communication cost for the proposed model is significantly lower compared to the DGP model.

3.4 Performance Evaluation on Storage Overhead

Adequate memory capacity is required to store the key and security components of the network. The integral sum of nodes in WSN scheme considered in this research can be computed as: $nT = nH + nL$, given that nH is the number of high-powered nodes, and nL is the total number of low powered nodes. The DGP model uses a factor $F = ID \times nL$ for the polynomial computation. This will have to store $\left(ID_B \times (\eta - 1)\right) + \left(h(ID_B) \times (\eta - 1)\right)$ size of bytes. Note that ID_B denotes ID size in bytes, η denotes the size of cluster, $h(ID_B)$ denotes the hash value size in bytes. With the concept deployed in DGP method, η number of clusters will require a multiple of η factors for polynomial computation. This analysis considers a $2\ bytes$ ID_B and $h(ID_B) = 160\ bits$ for adequately ciphered hash function. In this research, a constant multiplication factor $F = 3$ was selected for all cluster size, which is approximately 607% less compared to DGP model at $\eta = 30$, for instance. Recall that in our method as presented in Algorithm 1, only three random IDs are required, this selected to generate polynomial. When the $16\ bits\ IDs$ are ciphered and XORed, it becomes impossible for an attacker to break the security. The memory storage comparison is presented in Table 4 and Fig. 5.

Table 3. Performance analysis on communication cost based on data size transfer

	Communication cost (bits)	
	Proposed scheme	**DGP scheme**
Registration	98	450
Node addition	250	1058
Node migration	480	1960

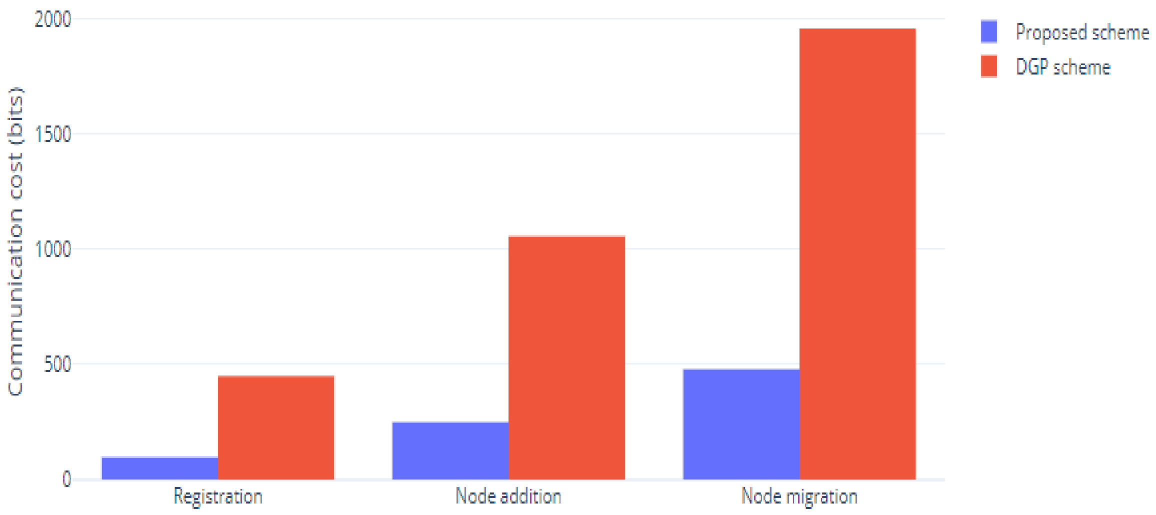

Fig. 4. Performance analysis on communication cost based on data size transfer

Table 4. Storage overhead comparison

Cluster size	Storage (bytes)	
	Proposed Scheme	**DGP scheme**
10	3	86
20	3	157
30	3	610
40	3	782
50	3	1056
60	3	1025
70	3	1571
80	3	1724
90	3	1937
100	3	2212

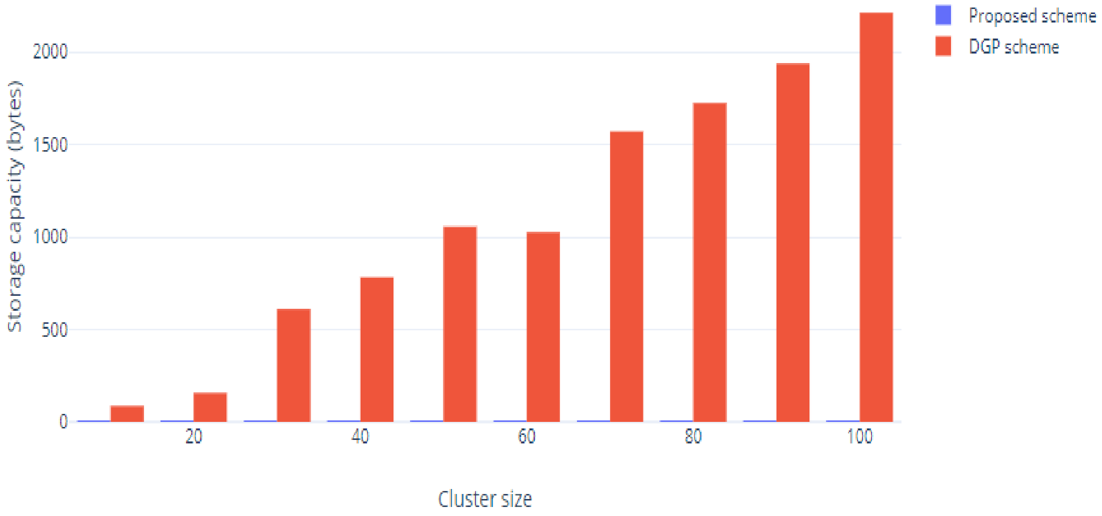

Fig. 5. Storage overhead comparison

Fig. 5 has clearly shown that for any cluster size, the storage requirement for the propose model is 3 bytes (note that the proposed model requires only three IDs to generate polynomial) whereas, the DGP model requires $\left(ID_B \times (\eta - 1)\right) + \left(h(ID_B) \times (\eta - 1)\right)$ bytes of storage space. This implies that for a very large cluster size, the DGP model will require a significantly large amount of storage space to store the polynomials generated.

4. CONCLUSION

Other techniques used by various researchers on a related subject to this research relied on serial multiplication to compute polynomial. These approach as seen in the results is resource intensive. The polynomial computational procedure is repeated each time a new node is engaged or disengaged from the network in the case of DGP. This repetitive expensive operation has a significant undesired impact on the communication overhead, and storage overhead as seen in the results for DGP model presented in Fig.s 3, 4 and 5.

The novelty introduced by the proposed model to mitigate this pertinent issue is based on using XOR of arbitrarily selected values to generate polynomial. The multiplicative method deployed by the existing schemes has computational complexity of $O(n^2)$, while that of the proposed scheme is $O(n)$. This complexity has significant impact on time latency as shown in Fig. 2

Evidently, from the results presented it can be observed that energy consumption drops in the proposed model and consequently, a longer life span of the network is guaranteed. Secure authentication is achieved from the proposed model by distributing the cluster controller tasks among the cluster members.

The result presented in Fig. 5 shows that a fixed number of hash values (3) is required to compute the polynomial, this is contrary to what is obtainable in DGP model where the hash value is directly proportional to the cluster size, hence, the bigger the cluster size, the larger the value. By comparison, the proposed model outperforms the DGP model by 87%.

COMPETING INTERESTS

Authors have declared that no competing interests exist.

REFERENCES

1. Charles Q, Jones P, Young L. Impact of wireless sensor network in 21st century" in Proceedings of the 2018 IEEE Symposium. 2018;7–13.
2. Sharibu D, Levite K. Effects of modern technology in home automation, Journal of Network and Computer Applications. 2020;4:3–7.
3. Damson J, Joe M. Application of ZigBee based WSN in smart agriculture in Proceedings of the IEEE International

Conference on Computer and Communications. 2019;9-15.

4. Oloyede O, Lopez N, Ozuomba S, Asuquo P, Essien E, Agbu A. Upper-air meteorological dataset for Uyo, using radiosonde, Data in Brief. 2023;46: 108904. Available:https://doi.org/10.1016/j.dib.2023.108904
5. Titus L, Sivasobramanian P. Design and implementation of LoRa based sensor network for military applications" in Proceedings of the 2021 IECC symposium on framework for networking and communications systems. 2021;12-21.
6. Meon B, Fastish V. Design and evaluation of security protocols in wireless sensor networks in Proceedings of the 2020 IEEE International Conference on Advances in Computer Applications, ICACA. 2020;19–24.
7. Lopez N, Agbu A, Oloyede A, Essien E, Eze A, Mhambe C. Software tool to store IoT device data onto a blockchain, Software Impacts. 2023;16. Available:https://doi.org/10.1016/j.simpa.2023.100511
8. Duriˇsi´c M, Tafa Z, Dimi´c G, Milutinovi´c V. A survey of military applications of wireless sensor networks in Proceedings of the 2020 Mediterranean Conference on Embedded Computing (MECO '20). 2020;196–199.
9. Azzabi T, Farhat H, Sahli N. A survey on wireless sensor networks security issues and military specificities in Proceedings of the 2019 International Conference on Advanced Systems and Electric Technologies, IC ASET 2019;66–72.
10. Harn L, Hsu C, Ruan O, Zhang M. Novel design of secure end-to-end routing protocol in wireless sensor networks. IEEE Sensors Journal. 2016;16(6):1779–1785.
11. Eschenauer L, Gligor V. A key-management scheme for distributed sensor networks in Proceedings of the 9th ACM Conference on Computer and Communications Security, New York, NY, USA. 2019;41-47.
12. Kumar N, Nene M. Deterministic approach to cryptographic key management in Proceedings of the 2019 International Conference on Inventive Systems and Control, ICISC. 2019;1–6.
13. Dinker A, Sharma V. Trivariate polynomial based key management scheme (TPB-KMS) in hierarchical wireless sensor networks, using EE-SAR algorithm, Advances in Intelligent Systems and Computing. 2018;696:283–290.
14. Usoh M, Asuquo P, Ozuomba S, Stephen B, Inyang U. A hybrid machine learning model for detecting cybersecurity threats in IoT applications, Int. j. inf. tecnol. 2023;15:3359–3370. Available:https://doi.org/10.1007/s41870-023-01367-8
15. Padal Jr C, May L, Salado M, Sobejana P. SPAMAST smart garbage bin monitoring system using wireless sensor network, Journal of Engineering Research and Reports. 2019;6(3):1-16. Available:https://doi.org/10.9734/jerr/2019/v6i316953

Peer-review history:
The peer review history for this paper can be accessed here:
https://www.sdiarticle5.com/review-history/110565