A Novel Secure Data Aggregation Scheme Based on Semi-Homomorphic Encryption in WSNs

Samir Ifzarne, Imad Hafidi, and Nadia Idrissi
National School of Applied Science: ENSA Khouribga, Khouribga 25000, Morocco
Email: {sifzarne; imad.hafidi; nadia.idrissi}@gmail.com

Abstract —Privacy protection in Wireless Sensor Networks (WSN) constitutes a big challenge for the adoption of WSNs in data sensitive applications like health monitoring or tracking and surveillance of borders. Privacy protection require additional controls and communications overloads, which impact the overall network lifetime. Research community has proposed several scenarios to minimize the impact of data protection generally based on secure aggregation and encryption to meet the practical requirements of energy constraints imposed by WSN. However, efficiency of privacy protection must be assessed before deployment. The privacy protection mechanisms are evaluated based on their hackability and network performance using four main metrics: Control Packet Overhead, delay, Throughput, Packet delivery ratio. The purpose of this paper is to propose a secure aggregation scheme based on homomorphic encryption. The new scheme will be will be compared to another scheme based on network metric and attack detection accuracy to have full view on the scheme performance for both network and security metrics. The proposed scheme named "Cluster-based Semi-Homomophic Encryption Aggregated Data" (CSHEAD) offer better performance as it reduces the controls overhead with higher detection accuracy. The conducted simulations confirm the expected results.

Index Terms—Wireless Sensor Network (WSN), data aggregation, homomorphic encryption

I. Introduction

In recent years, Wireless Sensor Network has witnessed an accelerated deployment increase reaching market value USD 46.76 billion in 2019. WSN offer the monitoring capability of the physical world in different environments thanks to the tiny sensors embedded with connectivity.

Healthcare is an example of WSN applications where the follow-up of remote health care patients becomes feasible. Thanks to the increase of bandwidth available in the WSN and the increase of its lifetime mainly because of energy decrease [1]**,** [2]. There are many applications of wireless sensor networks: in transportation like monitoring traffic density and road conditions in a large metropolis; in robotics, such as advanced robotic sensing, multiple robot coordination, robot planning and navigation, in engineering, monitoring buildings structures like bridges and maintenance planning. Using wireless sensors network helps build adaptive emergency response to be conscious of environment conditions, such as electromagnetic field monitoring, forest fire detection.

WSN is attracting research attention and industrials interest to improve the technology reliability and reduce its cost. Challenges like network lifetime, energy consumption and data privacy protection [3] continue to be the focus of many studies.

Sensor Nodes energy is based on a battery which remain for all the node lifetime. The major power drain for the sensor node occurs from wireless communication. Thus saving energy is mainly relying on reducing wireless communications. Effort to optimize routing protocols contribute partially to this goal as it's reduce the number of hopes and total number of communications required to deliver data to the sink. However the data volume is not reduced by the route choice from sensing node to the sink.

Compressed Sensing is providing capabilities to compress raw sensor reading data. It compress the signal at the nodes level by taking only fewer signal samples far less than what is required by the Nyquist–Shannon sampling theorem. The sink can use decompression methods, through optimization, to reconstruct the original sparse signal. Compressed sensing is used in imaging applications like video surveillance and medical imaging where the volume of data is huge and signal is sparse in some domain.

Data aggregation techniques [4] are used when the reading raw data from sensors are redundant or correlated. For example in precise agriculture, it's important to follow up temperature, humidity and luminosity. All these data tend to be redundant over time and will not change over few minutes or even one hour. Also there is a spatial or temporal correlation as sensor which are close to each other or in similar locations will be reporting almost same value.

WSN has some intrinsic limitations that could be reviewed as follows: limited node power and processing capabilities, low physical security due to harsh deployment environment, unreliable radio transmission medium, and multi hop communication scheme. The research community in Internet of Things (IoT) and WSN is carrying active work mainly in the fields of power source lifetime optimization, security, system capacity

Manuscript received January 17, 2021; revised March 27, 2021.
Corresponding author email: sifzarne@gmail.com
doi:10.12720/jcm.16.8.323-330

and routing. Because of the importance of power saving and data privacy protection, a lot of Secure Data Aggregation scheme have been proposed in the last few years in order to overcome energy constraints and guarantee the data protection required by WSN applications such as Medical, Transportation, Military and Security. Privacy preserving in data aggregation seems to offer a good security and data protection while reducing its volume.

This paper present a new algorithm based on the homomorphic encryption and data aggregation in a tree or cluster based network topology. Data decryption is done only at the Sink level and thus allowing to reduce energy consumption related to the decryption operations. Aggregation is processed at cluster heads on encrypted values coming from children nodes. The communication overhead is then reduced as only small amount of data transmission is operated by each node especially non leaf nodes which need to route the data through the network. The proposed scheme is developed to provide attack detection capability and keep managing communication overhead which will be measured for Packet Overhead, Packet delivery ratio, delay and throughput.

This paper is organized as follows: in section 2 related works are reviewed and briefly presenting a Cluster-based Secure Data Aggregation (CSDA) scheme whereas Section 3 is about the contribution of this research. Section 4 presents the proposed methodology, simulation result and shows the analysis of the proposed system. Conclusion of the research with a summary is done in Section 5.

II. Related Work

In recent years, many researches have been putting considerable effort to secure data aggregation.

Aggregation structure in the network defines the role of nodes where some will relay data and others will be managing the information aggregation. Hierarchy structure such as tree or cluster based pre-organize the nodes into children nodes and parent's nodes (Tree structure) or Common node and Cluster Head (Cluster structure). The data flow from children or common node to parents or Cluster heads until reaching the sink.

Xiaohan *et al.* [5] developed a Privacy Data Aggregation Scheme for Wireless Sensor Networks. The model manage key distribution and uses privacy homomorphism to support encryption. Also authors have designed a mechanism to perform hop-by-hop verification based on an algorithm which generate Media Access Control (MAC) in rotation manner.

Qiang *et al.* [6] proposed a Trust-based Dynamic Slicing Mechanism for Wireless Sensor Networks. Authors introduces a trust value to be allocated to each node in the network. The trust value in a time interval is used to make sure only trusted nodes could be elected as Cluster Heads. This mechanism protect from selecting non trusted nodes as Cluster Heads but once a node becomes CH, it will remain CH even if it's trust value drop.

Rajathi *et al.* [7] proposed a Secure Privacy-Preserving Data Aggregation Scheme (SPPDAS) Based on Bilinear ElGamal Cryptosystem for Remote Health Monitoring Systems and private data security. This scheme uses encryption and signature for secure data aggregation. The computational load required by the cryptosystem and the communication overhead are main weaknesses of the system model.

Authors in [8] presented a secure model for data aggregation which improvise both the communication overhead and the computational overhead. This model is Elliptic Curve-Based for cryptography and achieve privacy preservation based on a Secure Multidimensional Aggregation for Smart Grid Communications.

To improve security models and their parameters, Boudia, *et al.* [9] worked on privacy protection and compared several models. The authors proposed a new scheme with fault tolerance capability. The proposed scheme target a combination of high reliability as well as low communication overhead alongside computational security as it's the main purpose. Subsequently, another efficient mechanism named Distributed Laplace Perturbation Algorithm (DLPA) scheme is presented; DLPA define the low quantity of noise redundancy. Be that as it may, both the security schemes and the protection method are just on the constrained resources.

Active external Attack detection and protection is proposed in [10] Lightweight Privacy Preserving for data Aggregation LPDA enables to filter the false injected data by external attackers. LPDA is suitable for certain devices as part of IoT which supports fault tolerance and efficient aggregation. This scheme is lightweight as it has low Communication Overhead as well as computation costs.

Internal attacks were the focus for an efficient method [11] named Privacy-Preserving Data Aggregation (PPDA). This Scheme for Smart Grid protect Against Internal Adversaries and is capable of thwarting internal attacks for the given smart grid environment. PPDA also combine both objectives: privacy preserving and low communication cost.

III. Contribution of this Research

Secure Data Aggregation has been achieved via the usage of semi-homomorphic cryptosystem. This research contributions are:

Propose an aggregation scheme with attack detection capability.

Communication overhead maintained in a reasonable level.

Better performance results compared to a recent and efficient CSDA scheme.

IV. Proposed Methodology

In this section, CSHEAD is presented as the new scheme for secure data aggregation based on semi-homomorphic encryption. The proposed mechanism is compared to a recent and efficient Cluster-based Secure Data Aggregation (CSDA) scheme. CSDA [12] is an energy efficient secure data aggregation scheme based on cluster privacy preserving. The scheme is classified into three steps. The first step is cluster formation and second step involves data aggregation in one cluster using slice assemble technology. The third step is the data aggregation between clusters. In the first two steps of CSDA, the cluster head node is used to data aggregation, while other member nodes are responsible for keeping watch on head node's operations.

The goal of the CSHEAD is to secure data aggregation and provide active attack detection capability. The communication overhead is also taken into consideration as a key factor for practical usage of the scheme.

Aggregation function is one of the most important questions to answer while designing the aggregation scheme in order to define how sensor node aggregate raw data into a digest. Functions such as MIN, MAX, SUM, COUNT, AVERAGE and MEDIAN or Standard Deviation are used as function aggregation. Raw sensors reading data have temporal or spatial correlations. Aggregation function use these correlations to reduce the volume of useful data like Average function for temperature aggregation in same room which should be similar between sensors. Sum function would be a better choice for monitoring the total number of vehicles.

Symmetric Key Cryptography is less expensive in term of resources and hence was preferred over Asymmetric Key Cryptography. In general, Classic Cryptosystems requires high computational resources, hence Secure Data Aggregation was about providing security without encryption.

A. CSDA Aggregation Scheme

CSDA is based on the data slicing mechanism combined with encryption to protect the data. Slice assembly technology means each node divides its data into pieces and send each piece to the other cluster members. Let's assume the cluster has $\boldsymbol{C_i}$ members. Each node will divide its data into M_i pieces and send the $M_i - 1$ to the cluster members.

Each sensor node establish a secure link with its neighbors which share the same encryption key (ki).

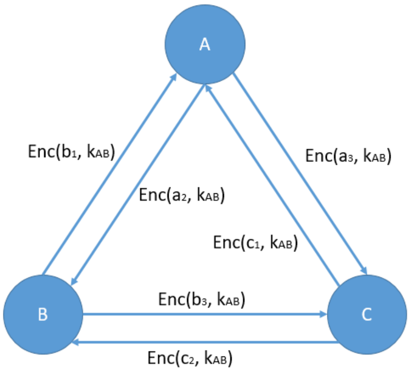

Fig. 1. Data exchanging: Encrypt and deliver part of values

The example below shows three neighbor nodes A, B, and C dividing their private data a, b, and c into three slices separately: a1, a2, a3, b1, b2, b3 and c1, c2, c3. They deliver encrypted values to each other and keep the 3rd piece for themselves. (Fig. 1)

A receive b1 and c1 and have a1 which was not shared. A will calculate the value of a1 + b1 + c1. Same do node B to calculate the value of a2 + b2 + c2, and a3 + b3 + c3 is to be calculated by node C.

Fig. 2 shows the nodes broadcasting the three values, and the three nodes add up three values to infer the value of a + b + c.

In CSDA scheme, hop-by-hop encrypted data aggregation is used, each non-Leaf node is decrypting the received data. This scenario present a high risk for data confidentiality if an attacker compromises a node. The attacker can then get access to the encryption key and become able to perform the decryption process.

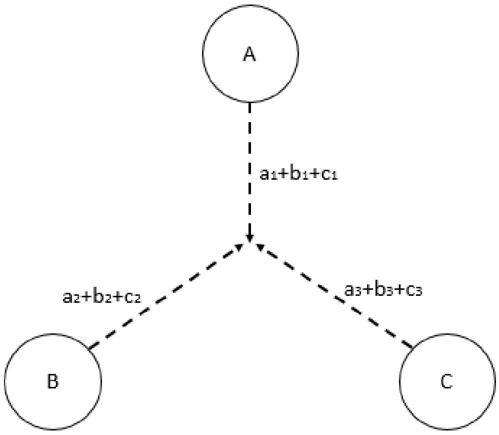

Fig. 2. Broadcast the result of aggregation

B. Homomorphic Encryption

Homomorphic encryption [13] allow arithmetic operations on ciphertexts without losing capability to recover transformed data. Semi-homomorphic cryptosystems are asymmetric homomorphic [14] encryption algorithm with public and private keys.

Let's denote E the encryption function and m_i the message or private data of node i.

In Fig. 3, the aggregation of encrypted data transform the multiplication of 2 encrypted messages m_1 and m_2 into and addition.

$$E(m_1).E(m_2) = E(m_1 + m_2) \tag{1}$$

Sensor node S1 encrypted it's information m1 and send encrypted message E(m1) to the parent node S3. Sensor node S2 encrypt it's reading m2 and encrypt it before sending E(m2) to S3.

Aggregation applied at parent node S3 is performed by multiplying the received encrypted messages from S1 and S2. Sensor S3 encrypt its own reading m3 and multiply E(m3) with received encrypted messages E(m1) and E(m2) before forwarding the result $E(m_1).E(m_2).E(m_3)$ to the Sink.

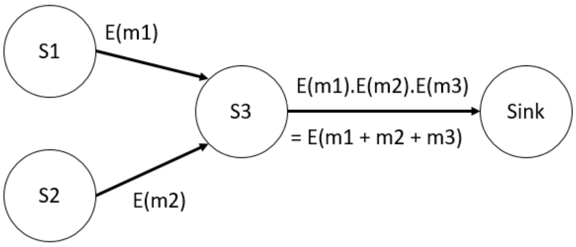

Fig. 3. Semi-homomorphic encryption transform multiplication of encrypted data into an encrypted message of the additive result from initial messages.

Given a scalar t, then:

$$E(t.m) = E(\sum_{i=1}^{t} m) = \prod_{i=1}^{t} E(m) = E^{t}\,(m)\ (2)$$

And $E(\sum_i t_i.m_i) = \prod_i E(t_i.m_i) = \prod_i E^{t_i}(m_i)$ (3)

At the sink level and by applying (1), the received message is same as $E(m_1 + m_2 + m_3)$ and hence after decryption sink will get the sum value $m_1 + m_2 + m_3$.

The sensed data collected by the cluster members is encrypted using public key based on semi-homomorphic encryption.

End-to-end encrypted data aggregation uses homomorphic encryption to apply certain aggregation functions such as addition or multiplication on the encrypted data.

No decryption is required during the data routing from sensor node until delivery to the sink. Therefore, this scenario reduces the decryption workload in the network. In addition, in case of sensor node physically compromised, the data confidentiality during transmission is not affected, as the decryption key is not available on the network. The nodes have the public key for encryption but the decryption key is known by the sink only. In this paper, Benaloh and Paillier cryptosystem have been used for sensor reading confidentiality protection.

C. Network Model

The network is modeled as a set S = {S1 … SN} of randomly distributed sensor nodes. Each node is battery powered. Sink has no energy constraint and has enough resources to process higher computational load compared to the nodes.

Let x_i(t) (i ∈ [1, N]) denote the sensor Si reading of the round t. A random value M_i is associated for each node x_i which is known by the node and the sink.

The network is structured as a tree. Leaf nodes are responsible for collecting data and forwarding it to their parents or cluster head. Non leaf node have the additional task of data aggregation and forwarding the results to the next hop.

Once a sensor S$_i$ gets it's reading at the t th-round, S$_i$ multiplies its reading x_i(t) by its coefficient M_i and send the result $M_i x_i$(t).

The sum is used as the aggregation function.

The readings encoding are distributed across the whole network nodes by performing some multiplications and summations. Thus, the computation cost of encoding is very low. (Fig. 4)

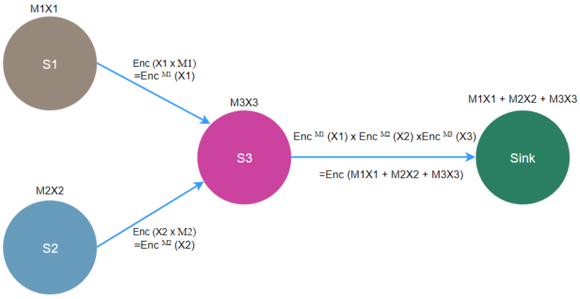

Fig. 4. Schematic diagram of data aggregation

D. Attack Model

Critical applications requires high protection of private data. Security in Wireless Sensor Network is big concern as it's important but very challenging because of the nature of the network where nodes have low resources and limited energy. Also wireless communication means more exposure toward eavesdroppers.

A hacker may launch different types of passive and active attacks. The attacker can be an untrusted eavesdroppers intercepting or listening to packets or even capture a node and hence disclose the security mechanism adopted across the network.

In the CSHEAD scheme by using an asymmetric cryptosystem, even if a node is compromised, the attacker won't get access to private data from other nodes. Then the challenge would be the overload which has been managed to keep it in CSHEAD scheme less than the CSDA. Packets controls are also less in CSHEAD scheme as every node send only one communication to the cluster nodes instead of CSDA scheme, each node send a piece of its information in phase 1 to cluster members and then send the calculated sum.

This paper is also interested into data injection attacks. An active attacker may inject additional data during aggregation phase. The attacker can also send a duplicated encrypted data already transmitted by another node. The scope of the new scheme protection is limited to avoid an attacker either duplicate, change the content or add a new data during aggregation phase. Even in case the attacker is a compromised node, it won't be able to report non valid data for the other trusted nodes.

E. Proposed scheme: Cluster-based Data Aggregation for WSN using Semi-Homomorphic Encryption (CHEAD)

In this scheme, the neighbors monitoring mechanism for attack detection has been introduced. As the initial status, a trusted node is known as such by its neighbors in the network. If a node have been identified as an attacker by multiple neighbors, then the detected attacker is reported across the network to the sink so it should get isolated from the network.

CSHEAD attack detection model is designed to send data only once to all nodes within same cluster including the cluster head or parent node and all nodes keep monitoring the activity of their neighbors.

The secure aggregation and attack detection works as the following phases:

Phase 1:

Every node start communicating to identify its neighbors. The Network architecture setup is completed in this phase. Formation of the Cluster: this is where the network structure is completed and the routing path is defined from nodes to the sink. Nodes desiring to become cluster heads send a Hello message to all neighbors which can accept to join the cluster. Each node will either respond to one of the requests to join a cluster or be the one sending the request to become the Cluster Head. At the end of this phase, the network will be splitted into clusters. This process will be repeated to enable every node to become a cluster head and thus better manage the network energy and life. This phase is similar to what happen in CSDA scheme as an initiation phase.

Phase 2: The sink generate public and private keys.

The Sink has enough energy and is the responsible of generating the keys as decryption will happen in the Sink. Also the Sink is the most protected component of the network with no energy constraints. Then, distribution of public key from the sink to the nodes. The distribution will use the Cluster heads for routing the keys from sink to nodes.

Phase 3: Data aggregation in one cluster at round t. At this phase, all sensor nodes send their readings to their Cluster Head and to all nodes in the same cluster. At each round t, all nodes from same cluster receive encrypted data $Enc(M_i x_i(\text{t}))$ that is being sent to the Cluster Head. CH share its own encrypted data with its cluster members. Encrypted Data is now shared at cluster level and every node has received encrypted data from all nodes including Cluster Head.

Phase 4: Cluster Head multiply the received encrypted data from cluster members with its own encrypted reading. Same operation is done by the cluster members and they should all get same encrypted value $\prod_i Enc(M_i.x_i)$. Every node has received encrypted data from all other nodes within same cluster which it will multiply it with its own encrypted reading. The result should be the same value for all nodes. This value will the one sent by Cluster Head to the Sink.

Phase 5: Cluster Head forward the aggregated encrypted data to the Sink. During this phase, cluster members keep monitoring the Cluster Head (CH) activity and they compare the data sent by the CH to the Sink with their calculated data. If any difference is noticed then CH is reported as the attacker. The attacker is then isolated from the network. As the Cluster Head is the responsible of routing the data, then it has a critical role in forwarding correct data. If CH is compromised it may change the data and send other values to the Sink hence it’s important to monitor what data is being sent by CH to the Sink.

Nodes are comparing their calculated values with the one sent by the CH. In case of a different value, they will report it to the Sink. Then the sink can detect the compromised node or Cluster Head and isolate it from the network and start phase 1 without the attacker.

Phase 6: The sink receive aggregated data from all cluster heads and calculate the $\prod_i Enc(M_i.x_i) = Enc(\sum_i M_i.x_i)$.

As the sink has the decryption key, it will get original aggregated value $\sum_i M_i.x_i$ where M_i is only known by each node S_i, so even a compromised node won’t be able to reproduce easily encrypted data for another node even if they have same reading x_i and same public encryption key.

The sink is using the aggregated value $\sum_i M_i.x_i$ for the whole network as a reference. If big change is detected over an acceptable threshold, then it can ask for getting raw data and detect if there is a compromised node.

This phase allow to detect a node sending non expected data as its own reading. If the attacker is detected, the Sink will communicate the message to the network to isolate the attacker.

F. Simulation and Results Analysis

The performance of CSHEAD scheme is evaluated using NS2. Cluster Head Selection and Data Forwarding is managed using LEACH (Low Energy Adaptive Clustering Hierarchy) protocol.

Low Energy Adaptive Clustering Hierarchy (LEACH) [15] is a hierarchical cluster based routing protocol which uses random rotation of the nodes required to be the cluster-heads to evenly disperse energy among all the sensor nodes. LEACH works in two phases: Setup phase & Steady phase. The setup phase is used to organize the clusters and the steady-state phase that deals with the actual data transfers to the sink node. Each node decides to become Cluster head (CH) based on its residual energy & certain probability. The threshold for CH selection is decided using the equation, which as follows.

$$\text{T(n)} = \text{P}/\ \{1\text{-P(r mod (1/P))}\} \qquad (4)$$

where, P represents the CH probability and r represents the random number. The term ‘(r mod (1/P))’ ensures that every node becomes a cluster-head once within 1/P rounds. When the node selects a random number less than a threshold T(n), it acts as a cluster-head for the current round. After the cluster head selection, the advertisement of nodes joining the particular cluster head, and then data transmission from node to sink node take place. However, it spends more energy for data forwarding.

On receiving the encrypted data, the cluster head performs end to end aggregation technique to avoid the high transmission delay and energy consumption. Due to the use of semi-homomorphic encryption based on Paillier cryptosystem [16], the aggregation technique is directly applied on the encrypted data. It can be seen that there are no more great amounts of complex computations, and only some simple linear operations are processed at the cluster head.

The performance of CSHEAD is evaluated using Network Simulator NS2. Network density is set by varying the node number within same area. The performance metrics are measured for both CSDA and CSHEAD. (Fig. 5)

Parameter	Values
Simulator	NS2
Number of Nodes	50, 60, 70, 80
Area	100m X 100m
Transmission Range	50 m
Interface Type	Phy/Wirelessphy
Queue Type	Droptail/Priority Queue
Antenna Type	Omni Antenna
Routing protocol	LEACH
Propagation Type	Two ray ground
Application Layer Protocol	CBR
Transport Layer Protocol	UDP
MAC layer protocol	802.15.4
Simulation Time	2000s

Fig. 5. Simulation parameters

The metrics are Packet delivery Ratio, Throughput, overhead, communication delay and attack detection.

For each metric, CSDA is compared to CSHEAD. Results shows that CSHEAD has better performance. (Fig. 6a)

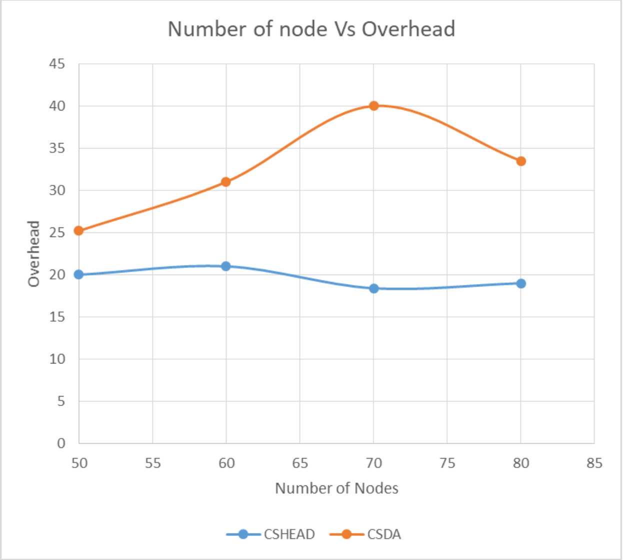

Fig. 6a. Number of nodes Vs overhead

Overhead: Total number of control messages used for providing the security in WSNs.

CSDA sends more control packets than CSHEAD, due to that CSDA have high overhead value than CSHEAD. (Fig. 6b)

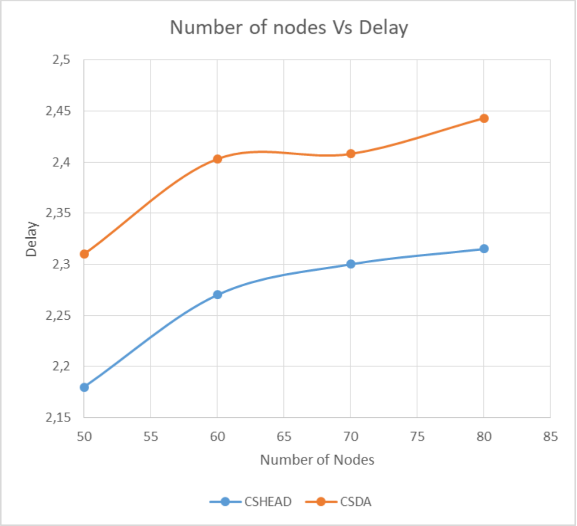

Fig. 6b. Number of nodes Vs delay

Delay: Total time taken by a packet to reach the sink in the network.

CSHEAD have reduced delay than CSDA. (Fig. 6c)

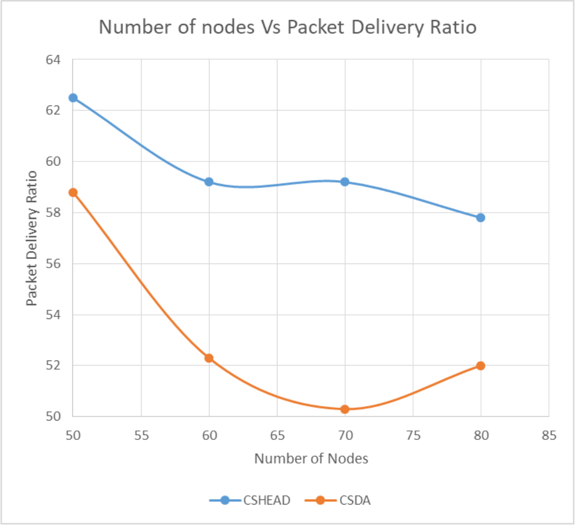

Fig. 6c. Number of nodes Vs packet delivery ratio

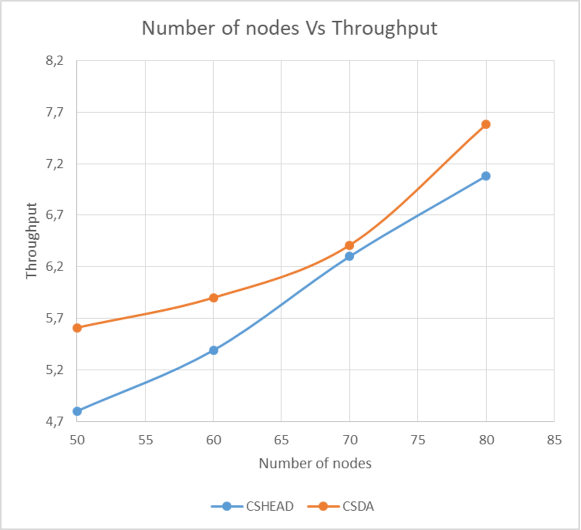

Fig. 6d. Number of nodes Vs throughput

Packet Delivery Ratio: It is the fraction of packets sent by the application that are received by the receivers.

Compared to CSDA, CSHEAD have more packet delivery ratio than CSDA. (Fig. 6d)

Throughput: Total number of delivered bits to the base station.

CSHEAD is reducing the number of delivered bits to the base station compared to CSDA. (Fig. 6e)

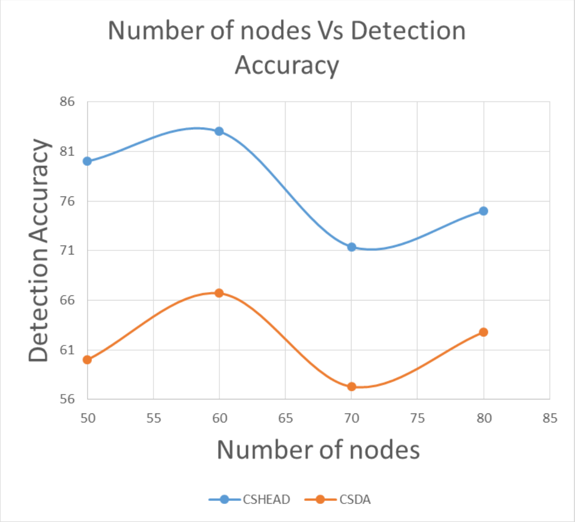

Fig. 6e. Number of nodes Vs detection accuracy

Detection Accuracy: The ratio of total number of detected active attacks and total number of active attacks in the network.

CSHEAD detect more attackers than CSDA, hence CSHEAD have more detection accuracy than CSDA.

V. Conclusion

This paper introduce a new scheme for Secure Data Aggregation in Wireless Sensor Networks. The proposed scheme is using semi-Homomorphic cryptosystem for data encryption. This Cryptosystem allows arithmetic operations on encrypted data at the Cluster Heads without need to decrypt. The data confidentiality remain protected during all its route from the sensor node to the Sink. Sum function has been used for aggregation as it's the case in many applications in practice. CSHEAD scheme has been compared to the existing CSDA scheme. CSHEAD scheme reduce the number of communications in the network and has attack detection capability. Evaluation of both schemes is conducted under different network densities and measure the key metrics such as throughput, end-to-end delay, packet delivery ratio and routing overhead. CSHEAD improves all Network metrics and hence increases the network lifetime and overall performance. Also, Active Attack Detection is more accurate in CSHEAD scheme compared to CSDA.

Information integrity was out of scope of this research and will be a perspective of a future work.

Conflict of Interest

The authors declare no conflict of interest.

Author Contributions

All authors discussed the work structure and aligned on the research scope. S. Ifzarne conducted the research and wrote the paper; I. Hafidi analyzed the data and provided guidance until getting to the last version; all authors had approved the final version.

References

[1] P. H. Vilela, J. J. P. C. Rodrigues, R. da R. Righi, S. Kozlov, and V. F. Rodrigues, "Looking at fog computing for e-health through the lens of deployment challenges and applications," *Sensors*, vol. 20, no. 9, p. 2553, Apr. 2020.

[2] J. F. A. Rida, "Development of a remote health care wireless sensor network based on wireless spread spectrum communication networks," *Materials Today: Proceedings*, Mar. 2021.

[3] L. Fan, L. Liu, H. Gao, Z. Ma, and Y. Wu, "Secure K-Nearest neighbor queries in two-tiered mobile wireless sensor networks," *Digital Communications and Networks*, p. S2352864820302674, Oct. 2020.

[4] M. Kaur and A. Munjal, "Data aggregation algorithms for wireless sensor network: A review," *Ad Hoc Networks*, vol. 100, p. 102083, Apr. 2020.

[5] X. Qi, X. Liu, J. Yu, and Q. Zhang, "A privacy data aggregation scheme for wireless sensor networks," *Procedia Computer Science*, vol. 174, pp. 578–583, Jan. 2020.

[6] Q. Zhang, X. Liu, J. Yu, and X. Qi, "A trust-based dynamic slicing mechanism for wireless sensor networks," *Procedia Computer Science*, vol. 174, pp. 572–577, 2020.

[7] A. Ara, M. Al-Rodhaan, Y. Tian, and A. Al-Dhelaan, "A secure privacy-preserving data aggregation scheme based on bilinear elgamal cryptosystem for remote health monitoring systems," *IEEE Access*, vol. 5, pp. 12601–12617, 2017.

[8] O. R. M. Boudia, S. M. Senouci, and M. Feham, "Elliptic curve-based secure multidimensional aggregation for smart grid communications," *IEEE Sensors Journal*, vol. 17, no. 23, pp. 7750–7757, Dec. 2017.

[9] S. Goryczka and L. Xiong, "A comprehensive comparison of multiparty secure additions with differential privacy," *IEEE Transactions on Dependable and Secure Computing*, vol. 14, no. 5, pp. 463–477, Sep. 2017.

[10] R. Lu, K. Heung, A. H. Lashkari, and A. A. Ghorbani, "A lightweight privacy-preserving data aggregation scheme for fog computing-enhanced IoT," *IEEE Access*, vol. 5, pp. 3302–3312, 2017.

[11] D. He, N. Kumar, S. Zeadally, A. Vinel, and L. T. Yang, "Efficient and privacy-preserving data aggregation scheme for smart grid against internal adversaries," *IEEE Transactions on Smart Grid*, vol. 8, no. 5, pp. 2411–2419, Sep. 2017.

[12] W. Fang, X. Wen, J. Xu, and J. Zhu, “CSDA: A novel cluster-based secure data aggregation scheme for WSNs,” *Cluster Comput*, vol. 22, no. 3, pp. 5233–5244, May 2019.

[13] B. Alaya, L. Laouamer, and N. Msilini, “Homomorphic encryption systems statement: Trends and challenges,” *Computer Science Review*, vol. 36, p. 100235, May 2020.

[14] W. Ren, *et al.*, “Privacy-preserving using homomorphic encryption in mobile IoT systems,” *Computer Communications*, vol. 165, pp. 105–111, Jan. 2021.

[15] I. Daanoune, B. Abdennaceur, and A. Ballouk, “A comprehensive survey on LEACH-based clustering routing protocols in wireless sensor networks,” *Ad Hoc Networks*, vol. 114, p. 102409, Apr. 2021.

[16] V. R. Falmari and M. Brindha, “Privacy preserving cloud based secure digital locker using paillier based difference function and chaos based cryptosystem,” *Journal of Information Security and Applications*, vol. 53, p. 102513, Aug. 2020.

Samir Ifzarne was born in Sale city, Morocco, in 1977. He received the Engineering degree from the Mohamadia School of Engineers (EMI), Rabat, in 2001. He is currently pursuing the Ph.D. degree with the Department of Mathematics and Computer Engineering, ENSA Khouribga. His research interests include WSN, compressed sensing, and homomorphic encryption.

Imad Hafidi is currently professor at the National School of Applicable Science (ENSA), Khouribga. He is head of the Department of Mathematics and Computer Engineering, ENSA Khouribga. His research interests include WSN, Data Mining, Big Data, Equilibria, Clustering algorithms.

Nadia Idrissi is currently professor at the National School of Applicable Science (ENSA), Khouribga. Here research interests include Numerical simulations, Chemical kinetics, Alloy Electrodeposistion, Mathematical analysis