Energy-Efficient Privacy Homomorphic Encryption Scheme for Multi-Sensor Data in WSNs

Suraj Verma
Faculty of Engineering & Informatics
University of Bradford
Bradford, United Kingdom
s.verma4@bradford.ac.uk

Prashant Pillai
Faculty of Engineering & Informatics
University of Bradford
Bradford, United Kingdom
p.pillai@bradford.ac.uk

Yim Fun Hu
Faculty of Engineering & Informatics
University of Bradford
Bradford, United Kingdom
y.f.hu@bradford.ac.uk

***Abstract*—The recent advancements in wireless sensor hardware ensures sensing multiple sensor data such as temperature, pressure, humidity, etc. using a single hardware unit, thus defining it as multi-sensor data communication in wireless sensor networks (WSNs). The in-processing technique of data aggregation is crucial in energy-efficient WSNs; however, with the requirement of end-to-end data confidentiality it may prove to be a challenge. End-to-end data confidentiality along with data aggregation is possible with the implementation of a special type of encryption scheme called privacy homomorphic (PH) encryption schemes. This paper proposes an optimized PH encryption scheme for WSN integrated networks handling multi-sensor data. The proposed scheme ensures light-weight payloads, significant energy and bandwidth consumption along with lower latencies. The performance analysis of the proposed scheme is presented in this paper with respect to the existing scheme. The working principle of the multi-sensor data framework is also presented in this paper along with the appropriate packet structures and process. It can be concluded that the scheme proves to decrease the payload size by 56.86% and spend an average energy of 8-18 mJ at the aggregator node for sensor nodes varying from 10-50 thereby ensuring scalability of the WSN unlike the existing scheme.**

Keywords—wireless sensor networks; homomorphic encryption scheme; data aggregation; energy-efficient WSNs; end-to-end data confidentiality; contiki-OS

I. INTRODUCTION

Wireless Sensor Networks (WSNs) have gained immense popularity in several applications due to their low-cost and low-power nature [1]. With the advent of the 6LoWPAN standard WSNs have light-weight IP capabilities such as transmission and reception of IPv6 data and the integration of the WSN with IP-based backbone networks such as the Internet [2], satellite [3], and Internet of Things [4]. Sensor nodes (SNs) today are capable of sensing multiple sensor data such as temperature, pressure, humidity, etc. all using the same sensor unit, therefore enabling a large number of different types of sensor data that can be sensed. However, with the recent advances in WSN technology in terms of IP network integration and multi-sensor data there still remains the eminent problem of ensuring end-to-end data confidentiality along with the implementation of in-processing techniques such as data aggregation [5] and multi-sensor data [6] in resources-constrained WSNs integrated with the Internet. Traditionally when data aggregation is implemented in WSNs the SNs transmit encrypted data to their aggregator nodes which decrypts the data, performs the data aggregation function over the plaintext sensor data and then re-encrypts the aggregated plaintext data prior to transmission towards the next node. This gives rise to hop-by-hop security which consumes more energy for every decryption/encryption and also induces a delay for the additional processing, all of which prove expensive for WSNs in terms of resources. Apart from the added security feature of end-to-end data confidentiality, end-to-end security mechanisms remove the need for additional utilization of resources thereby proving to be more efficient compared to hop-by-hop security [7]. However, implementing data aggregation with end-to-end data confidentiality mechanisms is challenging since the data aggregation function at the aggregator nodes would require access to the plaintext sensor data in order to aggregate the sensor data [8]. Research in this aspect has led to the design and development of a special category of encryption schemes called Privacy Homomorphic (PH) encryption schemes [9] that ensure end-to-end data confidentiality along with the implementation of data aggregation. PH schemes also ensure that the knowledge of encryption keys at intermediate nodes are not required since there are no intermediate decryptions of the ciphertext and the overall energy consumption of the network components and the induced latency can be reduced since there is no need for intermediate decryptions/encryptions. PH schemes can be broadly classified into asymmetric [10] and symmetric PH schemes. This paper mainly focuses on the symmetric PH schemes due to their low computational expense which proves to be suitable for resource-constrained networks and their computational delay which is several orders of magnitude lower as compared to asymmetric PH schemes. There has been a significant amount of research conducted in PH schemes for WSNs presented in [11] and out of the schemes proposed in [10] the Castelluccia-Mykletun-Tsudik (CMT) [12] scheme is chosen due to its low computational costs and simplicity which proves efficient for resource-constraint WSNs. However, despite the low computational costs and simplicity, the CMT scheme has the ID-issue which increases the overhead when the number of responding sensor nodes increase. This is mainly because the 16-bit node addresses of individual sensor nodes which participate in the data aggregation process are appended to the aggregated ciphertext during each transmission towards the end-user. Also, there is no support for multi-sensor data in the CMT scheme.

This paper proposes an optimized version of the original CMT scheme in order to counter the ID-issue faced by the CMT scheme and ensure that the proposed scheme is more energy and bandwidth efficient for multi-sensor data and large scale WSNs. The proposed scheme is a slot-based CMT scheme (SCMT) which transmits bit-field information pertaining to the security keys used during encryption in order to determine and use the corresponding security keys for decryption such that the correct aggregated plaintext data is retrieved from the aggregated ciphertext data. This paper explains the principle working of the SCMT scheme and presents Contiki-OS [13] based simulation results of the energy consumed during the initialization and data transmission phase of the SCMT scheme for multi-sensor data and overall payload length in comparison to the existing CMT scheme. The remainder of this paper is as follows: Section 2 introduces the CMT algorithm and methods proposed by other authors to reduce the bandwidth consumption. Section 3 presents the working principle of the SCMT scheme along with the initialization and data transmission phase. Section 4 presents the simulation results of the payload length and the energy consumptions of the CMT and SCMT schemes. Section 5 presents the future work and concludes the paper.

II. Related Work

A privacy homomorphic encryption scheme is an encryption transformation which allows direct computation over ciphertext data. Let Q denote a modulus ring and + denotes the addition operations on the ring; if K is the key space and a, b $\in$ Q & k, k_1, k_2 $\in$ K then a + b = $Dec_{k1,2}$ ($Enc_{k1}(a)$ + $Enc_{k2}(b)$) is termed as additively homomorphic with a single secret key k and a + b = $Dec_{k1,2}(Enc_{k1}(a)$ + $Enc_{k2}(b))$ as additively homomorphic with k_1 and k_2 as the multiple secret keys [10]. The authors of [12] present an additively homomorphic stream cipher scheme known here as the Castelluccia Mykletun Tsudik (CMT) privacy homomorphic scheme, that allows data aggregation and end-to-end data confidentiality. The main advantage of this scheme is that it uses modular arithmetic with very small moduli making this highly suitable for resource-constrained WSNs and achieving a significant bandwidth gain. However, a drawback of the proposed scheme is that the identities of non-responding sensor nodes or responding nodes need to be sent along with the aggregated ciphertext data to the Sink node which significantly increases the overhead costs thereby increasing the energy consumption. The working principle of the CMT scheme is as shown as follows:

CMT Algorithm

Parameters: Select a large integer M such that M = $2^{[\log 2\ (t\ *\ n)]}$ where t = max_sensor_value and n is the number of sensor nodes

Encryption: If the message is m $\in$ [0, M-1] and a random keystream is k $\in$ [0, M-1] then the ciphertext is given as c = (m + k) mod M

Decryption: Dec (c, k, M) = (c – K) mod M

Aggregation: Let the ciphertexts be $c_1 = (m_1 + k_1)$ mod M & $c_2 = (m_2 + k_2)$ mod M then the aggregation data is given by $c_1 + c_2 = (m_1 + m_2) + (k_1 + k_2)$ mod M

In order for the receiver to compute the aggregated plaintext data ($m_1 + m_2$) from the aggregated ciphertext data, the receiver should be able to determine the keysum value ($k_1 + k_2$) for a successful decryption which are obtained from the node IDs (16-bit or 64-bit IPv6 addresses). This proves to be expensive in terms of bandwidth consumption and induced packet overhead since as the number of responding sensor nodes increases the induced packet overhead which contains the IDs also increases thereby causing fragmentation of the packet and transmission of several packets. This inclusion of the sensor node IDs in the payload is termed as the ID-issue which is mainly addressed in this paper.

The author of [14] introduced a symmetric probabilistic PH scheme, Domingo-Ferrer (DF), wherein addition, subtraction, multiplication and division can be performed on ciphertext data. The proposed homomorphism scheme was the first one to allow full arithmetic operations while being secure against the known-ciphertext attacks which requires that the ciphertext splitting is always used when encrypting with a splitting factor d >= 2 and the ciphertext space is much larger than the plaintext space. The DF algorithm uses a single symmetric key in every sensor node to encrypt the sensor data wherein the aggregator performs aggregation over the ciphertext and the end node decrypts the result using the same secret key. Thus, there is no need of appending the node IDs along with the ciphertext. However, this reduces the level of security despite the implementation of probabilistic encryption since the physical compromise of a single sensor node can disclose the secret key in use and induce several security attacks on the whole network. It is seen in [15] that value of *d* ranging from 2 to 4 proves to be beneficial for WSNs wherein the power consumption of the transmitting sensor nodes increases linearly with packet size.

The authors of [16] evaluate three homomorphic algorithms suitable for WSNs and propose two approaches to mitigate the weaknesses of the algorithms in terms of the potential attacks and low security level. The first approach is the successful combination of two algorithms (DF and CMT) which increases the security and the minimization of additional efforts by the careful selection of parameters such as the splitting factor. The second approach tackles specific weaknesses by considering homomorphic message authentication codes and also describes in detail the ID-issue of the CMT scheme. The authors of [16] integrate the CMT algorithm with the Concealed Data Aggregation (CDA) algorithm which is the DF scheme in order to create a cascading encryption. The inner encryption function is CMT which suffers from the ID-issue and its malleable nature. However, the malleability can be countered by the implementation of an outer encryption transformation such as the DF, where the knowledge of the secret key is needed to modify the content of a single data packet. The advantage of this combination is that the aggregation requires exactly the same computational effort as the standalone DF. From the results presented in [16] it was seen that the hybrid scheme of DF and CMT proves to be 5 times more efficient in terms of bandwidth gain. However, this hybrid scheme is not scalable to large number of sensor nodes as the further increase of responding nodes increases the bandwidth utilization.

III. Slot-Based CMT Scheme

The Slot-based Castelluccia Mykletun Tsudik (SCMT) privacy homomorphic encryption scheme for multi-sensor data is designed as an optimized version of the CMT scheme wherein the ID issue highlighted in [12] is being addressed. The scheme mainly creates a variable length bit slot at the Cluster Head (CH) nodes. The status of each bit in the slot determines if a particular Sensor Node (SN) participated in the data aggregation process of ciphertext sensor data. The information contained in the slots are used by the Remote Monitoring Station (RMS) to decrypt the aggregated ciphertext data in to its respective aggregated plaintext sensor data for each sensor data type. The network architecture considered for this paper is as shown in Fig. 1. It mainly consists of the WSN which has several wireless sensor nodes (SNs), deployed within the sensing region in a star topology cluster-based node layout scheme [17].

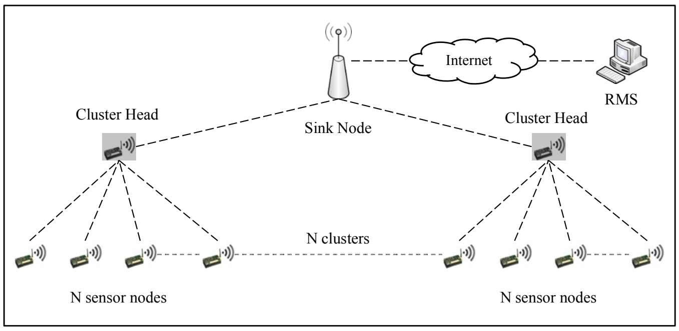
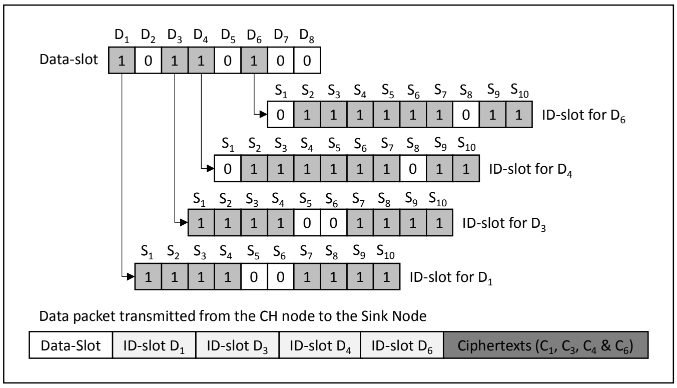


Figure 1: General network architecture employed for the SCMT scheme

The individual SNs within each cluster encrypts the sensor data using the SCMT encryption scheme and transmits the encrypted sensor data to their respective CH nodes which in turn proceeds to aggregate the ciphertext sensor data received from several SNs within the WSN cluster. Upon completion of the data aggregation process the ID-slot and the Data-slot, which are variable bit slots depending on the number of SNs and the different types of sensor data types, are updated and appended to the aggregated ciphertext data and transmitted to the Sink node. The Sink node acts as a bridge between the 6LoWPAN and the Internet and upon reception of the aggregated ciphertext and the respective slots the data packet from the Sink node is transmitted over the Internet as a full IPv6 packet to the RMS. When the RMS receives the full IPv6 packet it obtains the payload which contains the respective slots and the aggregated ciphertext sensor data. The SCMT decryption process is then employed wherein the information in the slots are used for the correct decryption of the aggregated ciphertext data in to the respective aggregated plaintext data. Each SN can be assumed as a single unit that consists of several on-board sensors capable of sensing different types of sensor data such as temperature, pressure, humidity, etc. and thus forms what is termed as a multi-sensor unit which transmits multi-sensor data (temperature, pressure, humidity, etc.). For instance, if there are 8 different types of sensor data that can be transmitted by multi-sensor units (SNs) within each WSN cluster then the size of the Data-slot will be *m*, where *m* is 8 bits in length, and the size of the ID-slot will be *n*, where *n* is the total number of SNs within each cluster. Suppose there are only 4 types out of the 8 types of sensor data information transmitted by 8 out of the 10 SNs within each WSN cluster then the Data-slots and ID slots will be updated accordingly as shown in Fig. 2.



D1 D2 D3 D4 D5 D6 D7 D8
Data-slot 1 0 1 1 0 1 0 0
S1 S2 S3 S4 S5 S6 S7 S8 S9 S10
0 1 1 1 1 1 1 0 1 1 ID-slot for D6
S1 S2 S3 S4 S5 S6 S7 S8 S9 S10
0 1 1 1 1 1 1 0 1 1 ID-slot for D4
S1 S2 S3 S4 S5 S6 S7 S8 S9 S10
1 1 1 1 0 0 1 1 1 1 ID-slot for D3
S1 S2 S3 S4 S5 S6 S7 S8 S9 S10
1 1 1 1 0 0 1 1 1 1 ID-slot for D1
Data packet transmitted from the CH node to the Sink Node
Data-Slot
ID-slot D1
ID-slot D3
ID-slot D4
ID-slot D6
Ciphertexts (C1, C3, C4 & C6)

Figure 2: Updating of the Data-slot and the ID-slot by the SCMT scheme

It is seen from Fig. 2 that the sensor data types {D_1, D_3, D_4 and D_6} are transmitted from 8 out of 10 SNs. For the data types {D_1 and D_3} the SNs that do not transmit the corresponding data types are {S_5 and S_6} and for the data types {D_4 and D_6} the SNs that do not transmit data the corresponding data types are {S_1 and S_8}. The Data-slot and the ID-slot is set to 1 and zero respectively, as shown in Fig. 2 where '1' in the Data-slot signifies the transmission of a particular sensor data type and in the ID-slot it signifies that the CH node received encrypted sensor data from a particular SN. A '0' in the Data-slot signifies no transmission of a particular sensor data type and in the ID-slot it signifies that the CH node did not receive encrypted data from a particular SN. Once the slots are updated the final data packet to be transmitted from the CH node is generated as shown in Fig. 2. The size of this packet is significantly smaller than the CMT scheme since the IDs (16-bit or 64-bit addresses) are not appended in the data packet since they are replaced by light-weight bit slots. However, in order for the SCMT scheme to work efficiently and accurately there needs to be an initialization phase which is responsible for setting up the structure of the slots at the CH node and the RMS. Thus, the SCMT scheme mainly consists of 2 phases; the initialization phase and the data transmission phase.

A. Initialization Phase

The initialization phase is triggered upon network setup and is considered as a one-time process unless it is invoked due to changes within the WSN such as node failure, security breach, mobility, etc. All the messages exchanged during the initialization phase is as shown in Fig. 3 along with their general packet structures. For each data packet transmission there is a 16-bit sequence number (SEQN) and a 16-bit checksum (CRC) appended in order to ensure data freshness and data integrity at the receiving nodes respectively. During the reception process the type of control message (M_{type}) received is determined, the packet is checked for freshness and the packet is checked for any errors induced due to noisy channel conditions. The 8-bit control flags field in each message depicts the processes which are set/unset and are as follows:

- *ENC* – No encryption (0); Encryption (1)
- *MOB* – No node mobility (0); Node mobility (1)
- *D_TYPE* – homogeneous data (0); heterogeneous data (1)
- *DISS_TYPE* - Random (00); Periodic (01); Event-driven (10); On-demand (11)
- *ID* – No ID-slot (0); ID-slot (1)
- *D_ID* – No Data-slot (0); Data-slot (1)
- *OF* – No payload overflow (0); Payload overflow (1)

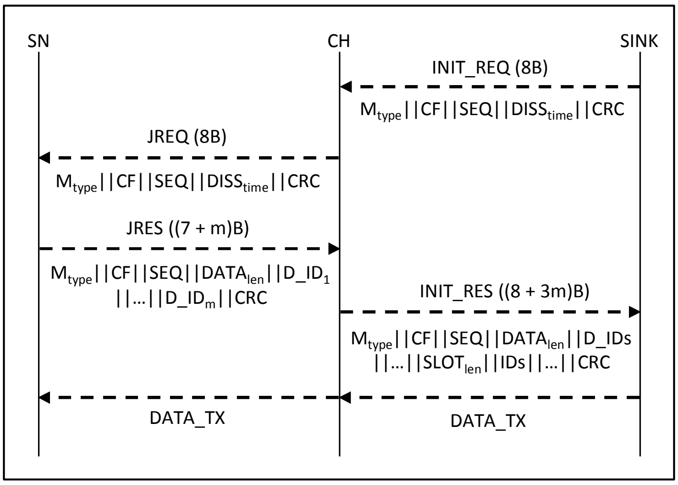
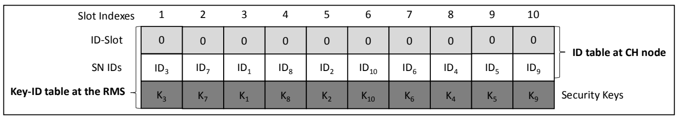

SN
CH
SINK
INIT_REQ (8B)
M_{type}||CF||SEQ||$DISS_{time}$||CRC
JREQ (8B)
M_{type}||CF||SEQ||$DISS_{time}$||CRC
JRES ((7 + m)B)
M_{type}||CF||SEQ||$DATA_{len}$||D_ID_1 ||…||D_ID_m||CRC
INIT_RES ((8 + 3m)B)
M_{type}||CF||SEQ||$DATA_{len}$||D_IDs ||…||$SLOT_{len}$||IDs||…||CRC
DATA_TX
DATA_TX

Figure 3: Message exchange during initialization phase of the SCMT scheme

The RMS node broadcasts an initialization request message (INIT_REQ) via the Sink node which is received by all neighboring CH nodes. This message signifies the start of the initialization process and consists mainly of the desired sensor data dissemination period ($DISS_{time}$) which is 16-bits in length (0 – 65535s). When the CH node receives this message the data freshness and integrity checks are performed and upon successful verification a join request message (JREQ) is broadcasted to all SNs within the respective WSN cluster which mainly consists of the $DISS_{time}$ data field. When this broadcast message is received by the SNs it checks for data freshness and integrity and upon successful verification the SNs transmit a unicast join response message (JRES) to the CH node which mainly consists of an a 8-bit data type length field that holds the value of *m* along with the *m* different data types IDs (8-bit each). The data type ID is used to identify the type of sensor data that is received (temperature, pressure, etc.) and it is transmitted only during the initialization phase. When the CH node receives the JRES messages from the individual SNs within the WSN cluster the CH node checks for data freshness and data integrity of each message before updating the Data-slot and the ID-slot. Upon the successful verification of each JRES message within a time period (T_{setup}), which is the time period the CH node will wait for the JRES messages from the SNs, the structure for the ID-slot and Data-slot is generated. The slot lengths along with the SN IDs and the data type IDs are transmitted as an initialization response message (INIT_RES) to the RMS via the Sink node. When the RMS receives the INIT_RES message it proceeds to build the key-ID table for each sensor data type as shown in Fig. 4. It is seen from Fig. 4 that at the CH node the ID table contains only the node addresses (ID_1, ID_2 … ID_n) along with the bit slot. At the RMS the key-ID table contains the same ID-table along with the respective security keys of the individual SNs. Once the tables are setup, the RMS node broadcasts a data transmission message (DATA_TX) which is then received by the CH node and broadcasted to the SNs thereby indicating that the initialization phase was successfully complete.



Slot Indexes	1	2	3	4	5	6	7	8	9	10
ID-Slot	0	0	0	0	0	0	0	0	0	0
SN IDs	ID_3	ID_7	ID_1	ID_8	ID_2	ID_{10}	ID_6	ID_4	ID_5	ID_9
	K_3	K_7	K_1	K_8	K_2	K_{10}	K_6	K_4	K_5	K_9

Figure 4: Basic structure of the slots built during the initialization phase of the SCMT scheme at the CH node and the RMS

B. Data Transmission Phase

Upon reception of the DATA_TX broadcast message the SNs proceed to collect sensor data and transmit the encrypted data using the SCMT encryption scheme. If m_j is the plaintext sensor data collected by SN *j* and M is a large integer then the ciphertext sensor data can be given as $c_j = (m_j + k_j) mod\ M$ where k_j is the unique secret key to sensor node *j*. The encrypted data packet is then transmitted to the CH node which receives several such similar data packets from SNs within its cluster. Upon reception of each message the CH node verifies data freshness and data integrity of each message before updating the Data-slot and the ID-slot set up during the initialization phase. Once the verification is successful and the slots have been updated successfully for each type of sensor data received, the CH node performs the data aggregation process using the ciphertext values of the respective sensor data types and appends the aggregated ciphertext values of each sensor data type to the data packet to be transmitted to the Sink node. Upon reception of the aggregated ciphertext data of different data types the Sink node encapsulates the entire payload filed, which includes the slots and the respective aggregated data, into the payload field of a full IPv6 packet and transmits it to the RMS via the Internet. The entire data transmission process is as shown in Fig. 5 where the packet structure for each packet transmitted at every node is depicted.

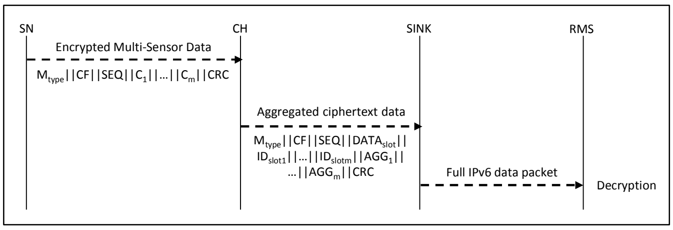

SN
CH
SINK
RMS
Encrypted Multi-Sensor Data
M_{type}||CF||SEQ||C_1||…||C_m||CRC
Aggregated ciphertext data
M_{type}||CF||SEQ||$DATA_{slot}$|| ID_{slot1}||…||ID_{slotm}||AGG_1|| …||AGG_m||CRC
Full IPv6 data packet
Decryption

Figure 5: Message exchange during data transmission phase of the SCMT scheme

IV. Simulation Results

The open source operating system Contiki [13] designed for the Internet of Things (IoT) enables a wireless sensor node to connect to the Internet. The java-based simulator Cooja [18] designed for the Contiki OS allows the rapid deployment of a simulation test-bed of a WSN with Internet connectivity that supports the WSN standard of 6LoWPAN. Hence the simulator Cooja was used in the Contiki OS environment to gather simulation results presented in this paper which focuses on the energy consumption of the radio and CPU usage of each process of the SN and the CH node when the SCMT scheme for multi-sensor data is employed. The simulation is divided into two phases; the initialization phase analysis and the data transmission analysis. Prior to analyzing the average energy consumption this paper also highlights the payload size of the SCMT scheme for varying number of SNs within the WSN cluster thereby signifying the percentage decease in payload size of the SCMT scheme over the CMT scheme. In order to determine the percentage decrease in payload sizes of the SCMT scheme over the CMT scheme a varying number of SNs within a WSN cluster ranging from 10 to 50 is considered in this paper. Also the analysis is performed over varying responding percentages (0.1, 0.25 and 0.5) which can be defined as the percentage of SNs within the cluster that transmit data over the total number of SNs within the cluster. For a given range of M (0 to $4.2*10^9$) the ciphertext size is 32 bits or 4 bytes in length ($\log_2$ (M)) and for every byte increase of the ciphertext data the range of M is multiplied by 256. Thus, with the ciphertext data length at 4B the payload sizes of the CMT and the SCMT scheme for varying number of SNs and responding percentages is as shown in Fig. 6.

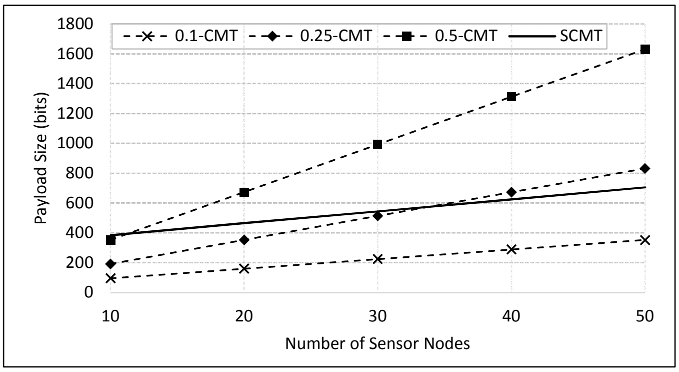


Figure 6: Comparison of payload sizes between the CMT and SCMT scheme

It is important to note that the CMT scheme does not support multi-sensor data transmission and it is safe to assume that if there were 8 different types of sensor data then the CMT scheme would transmit the 8 different data types as individual packets, thereby increasing the computation and transmission costs by 8 times. However, for the comparison of the SCMT scheme with the CMT scheme Fig. 6 considers single sensor data transmission for the CMT scheme and multi-sensor data (8 different data types) transmission for the SCMT scheme. Despite supporting multi-sensor data the SCMT scheme proves to be 56.86% lighter in terms of payload size compared to the CMT scheme which supports single sensor data transmission for 50 SNs and 8 different sensor data types.

Due to the resource constrain nature of the WSNs it is imperative to have a clear understanding of the energy budget when a new framework is introduced. The processes that consume energy when the SCMT scheme for multi-sensor data is employed are as follows; radio listen which is a process that listens to any incoming traffic and radio transmit which is a process that transmits data packets which can be collectively classified as the radio energy consumption along with the energy consumed due to the processing of data (encryption, decryption, slotting, etc.) can be classified as the CPU energy consumption. The energest power tool provided by the Contiki OS is used to calculate the total radio and CPU energy consumptions during the initialization phase and the data transmission phase. For the analysis in this paper, the radio and CPU energy consumption at the CH node is particularly important as majority of the proposed scheme is operational at the CH node. The SNs only add a small overhead (1-3 Bytes) which does not affect the energy consumed by the SNs significantly in comparison to the CMT scheme. The average radio and CPU energy consumption of the SN during the initialization phase is 620 µJ and 75 µJ respectively. The radio and CPU energy consumption at the CH node during the initialization is as shown in Fig. 7 for SNs ranging from 10 to 50 SNs within the WSN cluster.

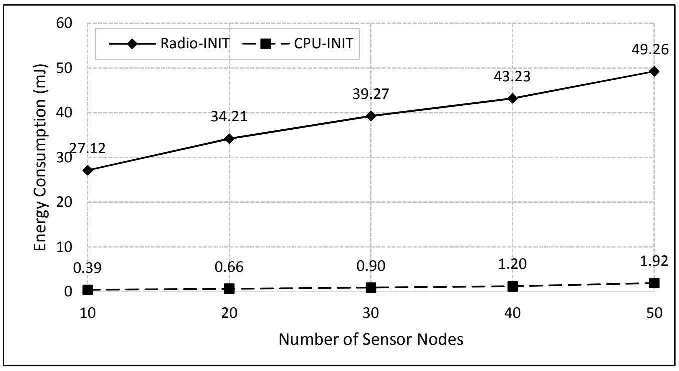


Figure 7: Energy consumption of the CH node during the initialization phase of the SCMT scheme

It is seen that with the increase in the number of SNs the radio energy consumption increases due to the increased packet size of the INIT_RES message which contains the 16-bit IPv6 address of individual SNs within the cluster. The CPU usage also increases since larger slots need to be formulated at the CH node with the increase in the number of SNs. The radio and CPU energy consumption at the CH node during the data transmission phase of the CMT and SCMT scheme for 8 different types of sensor is as shown in Fig. 8 for SNs ranging from 10 to 50 SNs within the WSN cluster.

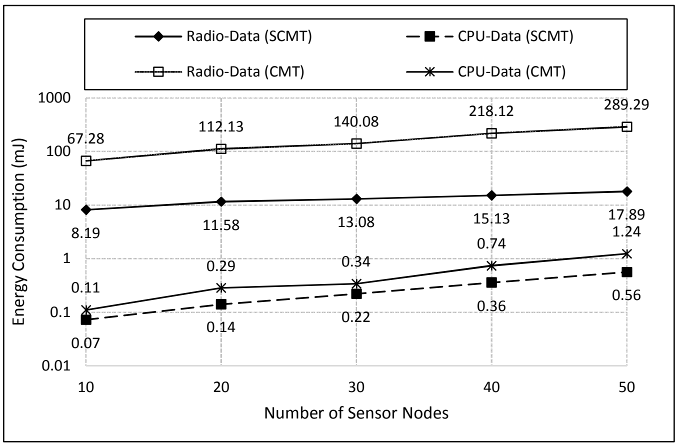


Figure 8: Energy consumption of the CH node during the data transmission phase of the CMT and SCMT scheme

The energy consumption analysis varies for increasing number of sensor data types (m) and increasing number of SNs (n). From the above analysis it can be concluded that the energy consumption is moderate when 8 different sensor data types are considered for a maximum of 50 SNs for the SCMT scheme. However, there is a significant increase in the energy consumption when the CMT scheme was employed for the same scenario where the 8 independent transmissions were made in order simulate the effect of the multi-sensor data (8 different sensor data types). For a maximum of 50 SNs within a single WSN cluster there is a 93.82% energy consumption when the SCMT scheme is used for multi-sensor data. Therefore, this proves that the additional ID overheads in the CMT scheme and the lack of multi-sensor data support in the CMT scheme makes the SCMT scheme a highly energy and bandwidth efficient scheme for privacy homomorphic encryption schemes in WSNs for multi-sensor data.

V. Conclusion

The main ID-issue of the CMT scheme [12] is being addressed in this paper with the implementation of a bit field slotting mechanism. The only drawback of the proposed scheme is that the initialization phase must be successfully completed prior to the data transmission phase. Since the initialization phase is a one-time process it may be periodically triggered over long intervals of time or in the case of large number of node failures. However, it is worth considering the effects of mobility of SNs and the CH node as it will invoke the initialization phase for every node entry or exit. In terms of the payload sizes the SCMT scheme proves to be significantly lighter than the CMT scheme since the IDs of SNs are not appended to the aggregated ciphertext data. There is a 56.86% decrease in the payload size compared to the CMT scheme which proves to twice as efficient compared to the CMT scheme in terms of energy consumption since the energy consumed mainly depends on the packet size of the data being transmitted. In terms of the energy consumption of the CH node during the initialization phase, for every increase in the number of SNs by 10 the energy consumed by the radio for reception and transmission is increased by 16.85% of the energy consumed for 10 SNs. Similarly for the data transmission phase the energy consumed by the radio is increased by 23.68% of the energy consumed for 10 SNs. With the advancement in WSNs which enable SNs to measure multiple sensor data it is important to understand the energy consumption of the multi-sensor data transmission when homomorphic encryption is implemented along with data aggregation. Also, with respect to the data transmission phase of the SCMT scheme compared to the CMT scheme it is evident that the SCMT scheme is highly efficient for large-scalable WSNs that support multi-sensor data with an average energy efficiency between 87% - 93% for SNs varying from 10 to 50 within the WSN cluster. This paper proposes a light-weight homomorphic encryption scheme for multi-sensor data transmission within large scale WSN integrated networks. Work in progress with respect to this paper is to incorporate node mobility and evaluate the effects of storing and mapping the ID-slot tables in the most efficient way at the aggregator nodes when SNs join and leave a WSN cluster, thereby, creating a dynamic environment for the SCMT scheme with varying channels conditions and bit error rates which may significantly affect the ID-slots generated.

References

[1] I.F. Akyildiz, W. Su, Y. Sankrasubramaniam and E. Cayirci, “Wireless Sensor Networks: A Survey,” Computer Networks, vol. 38, no. 4, pp. 393-422, 2002.

[2] W. Colitti, K. Steenhaut and N. De Caro, “Integrating Wireless Sensor Networks with the Web,” Presented at IP+SN, 2011.

[3] N. Celandroni, E. Ferro, A. Gotta, G. Oligeri, C. Roseti, M. Luglio, L. Bisio, M. Cello, F. Davoli, A. D. Panagopoulos, M. Poulakis, S. Vassaki, T. De Cola, M. A. Marchitti, Y. F. Hu, P. Pillai, S. Verma, K. Xu, G. Acar, “A Survey of Architectures and Scenarios in Satellite-based Wireless Sensor Networks: System Design Aspects”, International Journal of Satellite Communications and Networking, vol. 31, no. 1, pp. 1-38, 2013.

[4] L. Mainetti, L. Patrono and A. Vilei, “Evolution of wireless sensor networks towards the internet of things: A survey,” Presented at 19th International Conference on Software, Telecommunications and Computer Networks (SoftCOM), 2011.

[5] S. Ozdemir and Y. Xiao, “Secure data aggregation in wireless sensor networks: A comprehensive overview,” Computer Network, vol. 53, no. 12, pp.2022 -2037, 2009.

[6] B. Khaleghi, A. Khamis , F. O. Karray and S. N. Razavi, “Multisensor data fusion: A review of the state-of-the-art,” Information Fusion, vol. 14, no. 1, pp.28-44, 2013.

[7] S. Verma, P. Pillai and Y. F. Hu, “Performance Analysis of Data Aggregation and Security in WSN-Satellite Integrated Networks,” IEEE 24th Annual International Symposium on Personal, Indoor, and Mobile Radio Communication (PIMRC), 2013, pp. 3312-3316.

[8] C. Fontaine and F. Galand, “A Survey of Homomorphic Encryption for Nonspecialists,” EURASIP Journal on Information Security, vol. 1, pp. 41-50, 2009.

[9] S. Peter, D. Westhoff, and C. Castelluccia, “A Survey on the Encryption of Convergecast Traffic with In-Network Processing,” IEEE Trans. on Dependable and Secure Computing, vol. 7, no. 1, pp. 20-34, 2010.

[10] A. Viejo, Q. Wu and J. D. Ferrer, “Asymmetric homomorphisms for secure aggregation in heterogeneous scenarios,” Information Fusion, vol. 13, no. 4, pp. 285-295, 2012.

[11] S. Peter, D. Westhoff, and C. Castelluccia, “A Survey on the Encryption of Convergecast Traffic with In-Network Processing,” IEEE Trans. on Dependable and Secure Computing, vol. 7, no. 1, pp. 20-34, 2010.

[12] C. Castelluccia, E. Mykletun, G. Tsudik. “Efficient Aggregation of encrypted data in Wireless Sensor Networks,” Proceedings of the Second Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services, 2005, pp.109-117.

[13] A. Dunkels, and V. Thiemo, “Contiki-A Lightweight and Flexible Operating System for Tiny Networked Sensors,” 37th Annual IEEE Conference on Local Computer Networks. IEEE Computer Society, 2004.

[14] J. D. Ferrer, “A Provably Secure Additive and Multiplicative Privacy Homomorphism,” Proc. Fifth Information Security Conf. (ISC’02), 2002, pp. 471-483.

[15] J. Girao, D. Westhoff, M. Schneider, “CDA: Concealed Data Aggregation for Reverse Multicast Traffic in Wireless Sensor Networks,” Proc. IEEE Int’l Conf. Comm. (ICC’05), 2005.

[16] S. Peter, P. Langendorfer, K. Piotrowski, “On Concealed Data Aggregation for Wireless Sensor Networks,” Proc. Fourth IEEE Consumer Comm. and Networking Conf. (CCNC), 2007.

[17] S. Verma, P. Pillai and Y. F. Hu, “Performance Evaluation of Alternative Network Architectures for Sensor-Satellite Integrated Networks,” The 8th International Workshop on the Performance Analysis and Enhancement of Wireless Networks (PAEWN'13), 2013, pp. 120-125.

[18] F. Österlind, A. Dunkels, J. Eriksson, N. Finne, and T. Voigt, "Cross-level sensor network simulation with cooja," in Proceedings of the First IEEE International Workshop on Practical Issues in Building Sensor Network Applications (SenseApp 2006), Tampa, Florida, USA, Nov. 2006.