# Consistent and protected End-to-End Data Aggregation Using Secret distribution in WSNs

U.Jayasree[1], K.Reddamma[2]
[1.]Student, dept of mca kmm Insitute of Post Graduate Studies,Tirupati
[2].K.Venkataramana, dept of mca KMM Insitute of Post Graduate Studies,Tirupati

*Abstract-* **Data aggregation in WSNs (Wireless sensor Networks) can effectively reduce communication overheads and therefore the energy consumption of detector nodes. A WSN must be not solely energy economical, however conjointly secure. Varied attacks could build data aggregation unsecure. We investigate the reliable and secure end to-end data aggregation downside considering selective forwarding attacks and modification attacks in homogenous cluster-based WSNs, and propose two data aggregation approaches. Our approaches, namely, Sign-Share and Sham-Share, use secret sharing and signatures to permit aggregators to combination the data while not understanding the contents of messages and therefore the base station to verify the collective data and retrieve the raw data from the collective data.**

*Index Terms-* **data aggregation, wireless sensor Networks, sign-shared and sham-share.**

## I. INTRODUCTION

Data aggregation in WSNs (Wireless sensing element Networks) refers to the method of gathering and representing information in a very summary type. It will effectively scale back the info size, resulting in important energy reduction in transmittal and receiving data. Typically, a WSN is partitioned off into clusters with a cluster head in every cluster. Every cluster head gathers information from its members, aggregates the info, and sends the aggregate data to the bottom station. There square measure several security necessities for information aggregation, including information confidentiality, information integrity, information freshness, data convenience, authentication, and non-repudiation. The contents of the info in transit shouldn't be unconcealed to any party that's not licensed to own access. Data confidentiality is also achieved via 2 differing types of secure information aggregation schemes, namely, end-to-end theme and hop-by-hop theme. Associate end-to-end theme doesn't use cryptography once aggregating the info, and therefore is more energy economical. Many end-to-end information aggregation schemes are projected. In a very hop-by-hop theme, a sensing element node encrypts its information and sends the encrypted information to its individual. Every individual, when cryptography, applies an aggregation perform to mixture the info, then encrypts it before causation it to a different individual or the bottom station. Since secret writing and cryptography square measure computationally expensive, a hop-by-hop theme might consume a big amount of energy and permit the individual to grasp secret contents. In WSNs, numerous attacks might exist. Among them square measure selective forwarding attacks and modification attacks. In the selective forwarding attacks, a malicious sensing element node might deliberately drop some packets received from alternative sensing element nodes, leading to packet loss. Within the modification attacks, a malicious sensing element node might modify some packets received from alternative sensing element nodes and forward the wrong packets to the base station. In this paper, we have a tendency to investigate the reliable and secure end-to end data aggregation drawback beneath each selective forwarding attack and modification attacks in homogeneous cluster-based WSNs. we have a tendency to create the subsequent major contributions:

• We have a tendency to propose 2 secure information aggregation approaches for the end-to-end information aggregation in WSNs supported secret sharing and signatures. The projected approaches can defend against each selective forwarding attacks and modification attacks. To the simplest of our information, our approaches square measure the primary one considering each the selective forwarding attacks and also the modification attacks and providing secure end-to-end information aggregation in homogeneous cluster-based WSNs while not encrypting messages.

• We've compared each approach and 2 state-of-the art approaches, specifically PIP and RCDA-HOMO, using intensive simulations. The simulation results show that our approaches take less time in process the info and aggregating the info.

## II. PRAPOSED ALGORITHM

SIGN-SHARE:-In our Sign-Share approach, each sensor node splits its data into multiple shares and sends some of them to the aggregators of its cluster, allowing encoding each share with simpler codes For ease of description, we assume that the data sensed by each sensor each time is 32-bits long, and the 32-bit data is split into four 8-bit shares. Our Sign-Share approach consists of the following phases:

Setup Phase:

The following system parameters are generated and loaded into each sensor node at the design stage.

• A secret key-set K in a form of matrix shown as follows:

$$K = \begin{bmatrix} \lambda_0 & \mu_0 \\ \lambda_1 & \mu_1 \\ \lambda_2 & \mu_2 \\ \lambda_3 & \mu_3 \end{bmatrix} 0 \leq \lambda_k, \mu_k < P$$

The larger the P, the more secure the aggregations.

• A secret 32-bit pseudo random binary sequence generator P RBSp[I, n], where I is the seed and n is the clock.

• (puvi, prvi): this pair is generated according to the algorithm proposed by Boneh et al. [13]. However, the private key prvi is set to λ0.

– Puvi: the public key which is kept at the base station.

– Prvi: the private key which is loaded to each sensor node vi .

• A hash function H for all the sensor nodes.

Secret Sharing-Signature Phase:-

When a senor node vi senses the physical environment and prepares its data D to be sent to its aggregators, it does the following:

• Each sensor vi splits its data as follows:

1) Encode the data: D0 = D ⊕P RBSp [I, n], where ⊕ is the bitwise XOR.

2) Split the encoded data into 4 shares B0, B1, B2, and B3.

3) Encode each byte Bk using the key-set K as follows:

$$B'_k = ((B_k * \lambda_k) + \mu_k) \mod 256 \qquad (1)$$

• Sign each byte as follows:

$$h_i = H(B'_k) \qquad (2)$$

$$\sigma_i = pr_{v_i} * h_i \qquad (3)$$

• Send the data in a tuple (B0 k, σi) to each aggregator of its cluster such that the data after encoding is split equally between them

## III. AGGREGATION PHASE

When an aggregator node receives the tuple from every member of its cluster, it does the following:

Let $(B'_0, \sigma_0), (B'_1, \sigma_1), \cdots, (B'_{w-1}, \sigma_{w-1})$ be all the tuples received.

Aggregate the signatures as follows:

$$\hat{\sigma} = \sum_{i=1}^{w} \sigma_i$$

• Aggregate all the shares as follows:

– Concatenate the w bytes into a single value Q as follows:

$$Q = B'_0|B'_1|...|B'_{w-1} \qquad (5)$$

• Send the concatenated data in a tuple (Q, σˆ) to the base station.

Verification-Decoding Phase:-

When the base station receives the data from every aggregator AGi, it does the following:

• Let w be the number of shares received from AGi.

• Extract the Q bytes of each tuple received from AGi.

• Recover the 32-bit data of each node vi as follows:

1) Decode each byte using the key-set K of vi :

$$B_k = ((B'_k - \mu_k) * \lambda_k^{-1}) \mod 256 \quad (6)$$

2) Merge the decoded bytes into one 32-bit integer D0.

3) Decipher the data: D = D0 ⊕ P RBSp[I, n].

• Verify D by using Boneh et al. algorithm.

SHAM-SHARE:-

Our Sham-Share approach consists of the following phases:

Setup Phase: The base station generates the following key pair (puvi , prvi ) for each sensor node vi as in, where puvi is the public key kept in the base station, and prvi is the private key loaded to each sensor node vi along with H, the hash function for all the sensor nodes

Secret Sharing-Signature Phase: When a senor node vi senses the physical environment and prepares its data S to be sent to its aggregators, it performs the following tasks:

• The sensor node vi splits the data S into 4 shares as follows:

1) Generate two random numbers a0, a1.

2) Construct the following polynomial function:

$$f(x) = S + a_0 x + a_1 x^2 \quad (7)$$

3) Construct 4 shares with each share represented by a pair (x, f(x))(x = 1, 2, 3, 4). Shares start from (1, f(1)) because f(0) is the data S.

4) Let IDi be the ID of the sensor node vi . Encode each share of vi as follows:

$$Q_i = x + 10ID_i + 1000f(x) \quad (8)$$

• Sign each share as follows:

$$h_i = H(Q_i) \quad (9)$$

$$\sigma_i = pr_{v_i} * h_i \quad (10)$$

Send the tuples (Q1, σ1), (Q2, σ2) to one aggregator, and (Q3, σ3), (Q4, σ4) to the other aggregator

Aggregation Phase: After an aggregator AGi receives the tuple from every member of its cluster, it performs the following tasks:

• The aggregator gathers all the w tuples (Q0, σ0), (Q1, σ1), ..., (Qw−1, σw−1) from the members of its cluster.

• Aggregate the signatures as follows:

$$\hat{\sigma} = \sum_{i=1}^{w} \sigma_i \quad (11)$$

• Send the data in an array which contains the aggregated signature and the aggregated shares.

$$\begin{bmatrix} \hat{\sigma} \\ Q_0 \\ Q_1 \\ \dots \\ Q_{w-1} \end{bmatrix}$$

Reconstruction-Verification Phase: After the base station receives the data from all the aggregators, it performs the following tasks for each aggregator AGi:

• Let w be the number of shares received from AGi.

• Disaggregate Qi of each array received from AGi as follows:

$$\begin{bmatrix} f(x_0), ID_0, x_0 \\ f(x_1), ID_1, x_1 \\ \dots \\ f(x_{w-1}), ID_k, x_{w-1} \end{bmatrix} =$$

$$\begin{bmatrix} \lfloor Q_0/1000 \rfloor, \lfloor Q_0/10 \rfloor \mod 100, Q_0 \mod 10 \\ \lfloor Q_1/1000 \rfloor, \lfloor Q_1/10 \rfloor \mod 100, Q_1 \mod 10 \\ \dots \\ \lfloor Q_{w-1}/1000 \rfloor, \lfloor Q_{w-1}/10 \rfloor \mod 100, Q_{w-1} \mod 10 \end{bmatrix}$$

• Gather 3 shares of each sensor node vi , and reconstruct its data S as follows:

$$S = \sum_{j=0}^{2} f(x_j) \prod_{m=0, m \neq j}^{2} \frac{x_m}{x_m - x_j} \quad (12)$$

Verify S by using Boneh et al. algorithm.

## IV. CONCLUSION

We have planned 2 reliable and secure end-to-end information aggregation approaches that not exclusively conceal the detected data but in addition allow the bottom station to sight every the selective forwarding attacks and conjointly the modification attacks. The proposed ways perform higher performance than existing PIP and RCDA-HOMO in terms of the aggregation interval and conjointly the device interval, which they considerably perform beyond PIP in terms of the network time period, the network delay, and also the aggregation energy consumption.

REFERENCES


[1] D. Estrin, R. Govindan, J. Heidemann, and S. Kumar, "Next Century Challenges: Scalable Coordination in Sensor Networks," in Proceedings of the 5th ACM/IEEE International Conference on Mobile Computing and Networking. Seattle: IEEE Computer Society, 1999, pp. 263–270.

[2] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," IEEE Communications Magazine, vol. 40, no. 8, pp. 102–114, 2002.

[3] R. Rajagopalan and P. K. Varshney, "Data-aggregation techniques in sensor networks: a survey," IEEE Communications Surveys & Tutorials, vol. 8, no. 4, pp. 48–63, 2006.

[4] E. Fasolo, M. Rossi, J. Widmer, and M. Zorzi, "In-network aggregation techniques for wireless sensor networks: a survey," IEEE Wireless Communications, vol. 14, no. 2, pp. 70–87, 2007.

[5] P. Baronti, P. Pillai, V. W. C. Chook, S. Chessa, A. Gotta, and Y. F. Hu, "Wireless sensor networks: A survey on the state of the art and the 802.15.4 and ZigBee standards," Computer Communications, vol. 30, no. 7, pp. 1655–1695, 2007.

[6] B. H. Bloom, "Space/time trade-offs in hash coding with allowable errors," Communications of the ACM, vol. 13, no. 7, pp. 422–426, 1970.

[7] D. Westhoff, J. Girao, and M. Acharya, "Concealed Data Aggregation for Reverse Multicast Traffic in Sensor Networks: Encryption, Key Distribution, and Routing Adaptation," IEEE Transactions on Mobile Computing, vol. 5, no. 10, pp. 1417–1431, 2006.

[8] C. Castelluccia, A. C. F. Chan, E. Mykletun, and G. Tsudik, "Efficient and provably secure aggregation of encrypted data in wireless sensor networks," ACM Trans. Sen. Netw., vol. 5, no. 3, pp. 1–36, 2009.

[9] P. Steffen, W. Dirk, and C. Claude, "A Survey on the Encryption of Convergecast Traffic with In-Network Processing," IEEE Transactions on Dependable and Secure Computing, vol. 7, pp. 20–34, 2010.

[10] C. Fontaine and F. Galand, "A survey of homomorphic encryption for nonspecialists," EURASIP Journal on Information Security, vol. 2007, no. 1, pp. 1–10, 2007.

[11] C. Gentry, "Fully homomorphic encryption using ideal lattices," in Proceedings of the 41st annual ACM symposium on Theory of computing. Bethesda, MD, USA: ACM, 2009, pp. 169–178.

[12] M. van Dijk, C. Gentry, S. Halevi, and V. Vaikuntanathan, "Fully Homomorphic Encryption over the Integers," in EUROCRYPT'10, 2010.

[13] Z. Li and G. Gong, "Data Aggregation Integrity Based on Homomorphic Primitives in Sensor Networks," in Proceedings of 9th International Conference on Ad Hoc Networks and Wireless (ADHOC-NOW 2010). LNCS 6288, 2010, pp. 149–162.

[14] L. Hu and D. Evans, "Secure aggregation for wireless networks," in Proceedings of the 2003 Symposium on Applications and the Internet Workshops (SAINT'03 Workshops), 2003, pp. 384 – 391.

[15] P. Jadia and A. Mathuria, "Efficient Secure Aggregation in Sensor Networks," in High Performance Computing (HiPC 2004). LNCS 3296, 2004, pp. 40–49.

[16] Y. Yang, X. Wang, S. Zhu, and G. Cao, "A Secure Hop-by-Hop Data Aggregation Protocol for Sensor Networks," in Proceedings of the 7th ACM international symposium on Mobile ad hoc networking and computing (MobiHoc'06), 2006, pp. 356 – 367.

[17] B. Przydatek, D. Song, and A. Perrig, "SIA: Secure Information Aggregation in Sensor Networks," in Proceedings of the first international conference on Embedded networked sensor systems (SenSys'03), Los Angeles, California, USA, 2003, pp. 255 – 265.

[18] H. Chan, A. Perrig, and D. Song, "Secure hierarchical in-network aggregation in sensor networks," in Proceedings of the 13th ACM conference on Computer and communications

security. Alexandria, Virginia, USA: ACM, 2006, pp. 278–287.

[19] K. B. Frikken and J. A. Dougherty I. V., “An efficient integrity-preserving scheme for hierarchical sensor aggregation,” in Proceedings of the first ACM conference on Wireless network security (WiSec’08). Alexandria, VA, USA: ACM, 2008, pp. 68–76.

[20] H. Chan and A. Perrig, “Efficient security primitives derived from a secure aggregation algorithm,” in Proceedings of the 15th ACM conference on Computer and communications security (CCS’08). Alexandria, Virginia, USA: ACM, 2008.