Secure Data Aggregation Schemes in WSN: A Survey

P.Manimala[#1], R.Senthamil Selvi[#2]

#1 P.G Student,Department of computer science,M.I.E.T Engineering College, Tiruchirappalli.
#2 Associate professor,Department of computer science,M.I.E.T Engineering college, Tiruchirappalli

Abstract- *A wireless sensor network consists of a large number of nodes and each nodes has a limited amount of energy, memory, processing and communication capabilities. It consumes much energy for transmission than any other process. In order to reduce the energy consumption we need to reduce the number of transmission and packet size. Data aggregation is the main techniques used to reduce the power consumption and to increase the lifetime of the intermediate network. Nodes should aggregate results from individual sensors instead of being sent directly to the sink. Here we study the different techniques used for aggregation. We also highlight the advantages and issues of each aggregation technique. In addition, we study some methods to secure the aggregated data by treating confidentiality, integrity and authentication issues.*

Key words*: Data aggregation, wireless sensor network, Cluster head, Aggregator*.

1. Introduction

A **wireless sensor network (WSN)** consists of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. WSNs can be classified on the basis of their mode of operation or functionality, and the type of target applications.To enhance the lifetime of the network reduce the unnecessary traffic and energy consumption of sensor nodes aggregation technique is used.Data aggregation is a technique which tries to alleviate the localized congestion problem. It attempts to collect various information from the sensors surrounding the event. It then transmits only the useful information to the end point thereby reducing congestion and its associated problems.

1.Secure Aggregation for Wireless Networks (SAWN)

This paper mainly focus on data integrity, with just a mention of symmetric key cryptography for encryption of data.This scheme is based on hop by hop encryption.It exploits two main ideas, delayed aggregation and delayed authentication for resilience against node compromise. The base station generates a key chain using a one way function F where $K_i = F(K_{i+1})$. where each sensor is preloaded with K_0 before deployment where $K_0 = F^n(K)$.During Data Aggregation phase each leaf node senses data along with its node id and a message authentication code $MAC(K_{Ai}, R_i)$. The parent just retransmits all the readings and the MACs it received from its children to its parent.The grandparent does the aggregation of the readings. This is known as delayed aggregation.

2. A Secure Hop-by-Hop Data Aggregation Protocol for Sensor Networks (SDAP)

The design of SDAP is based on the principles of divide-and-conquer and commit-and-attest. Partition of the nodes into multiple logical groups (subtrees) of similar sizes.

A group leader is elected in each group which receives data from all the group members.The group leader aggregates this data and sends it to the base station over multiple hops.This phase is termed the verification and attestation phase in SDAP. A request for attestation is then sent to the group leader.A probabilistic path is followed down the group and the request is forwarded to each node on the path. Nodes receiving the request send back their data and id to the base station for verification.

3.Secure Hierarchical In-Network Aggregation in Sensor Networks (SHDA)

Symmetric key encryption is used in the data aggregation phase and a distributed scheme is used for integrity verification which aids in reducing congestion near the base station.

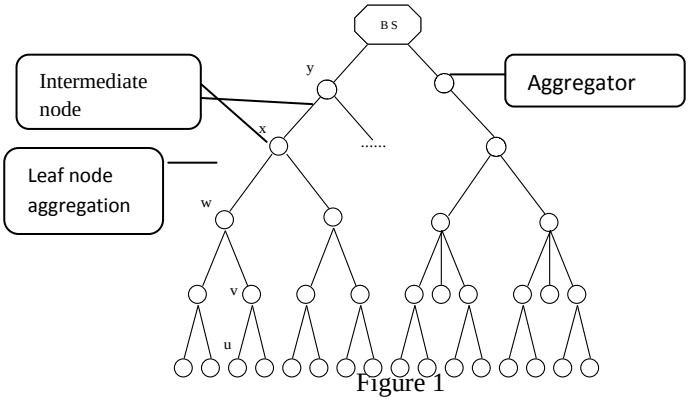

Figure 1

The scheme uses a hierarchical tree based structure as Fig 1 .After receiving the data the aggregator then aggregates the data and generates a hash for it.The commit process at every node, creates a hash tree in the network.The hashes are used to check the data for integrity using a distributed integrity verification technique. Upon receiving the final commitment value, the base station broadcast it into the network.

4.Hierarchical Aggregation in Sensor Networks (SHA)

It uses homomorphic encryption for data integrity purposes.The paper uses an Elliptic curve ElGamal (ECEG) variant for homomorphic encryption.The data generated by the leaf nodes is encrypted using this encryption algorithm and sent to the parent.The parent collects the encrypted data from all its children, performs a homomorphic aggregation and sends it to its own parent.Uses modified ECDSA to generate digital signatures.The signatures generated can be aggregated to form a single signature.The parent not only aggregates data, but also aggregates the signatures and the public keys of all its children.The network wide integer is used to generate a new public private key pair for each round of processing.Verification at the base station is done by using the aggregate public key on the aggregate signature.

5. Energy-efficient and Secure Patternbased Data Aggregation for wireless sensor networks(ESPDA)

ESPDA protocol [1] uses pattern codes, which represent the characteristics of the actual data to perform data aggregation. Instead of transmitting sensed data, sensor nodes first generate and transmit the pattern codes to cluster-heads. The mapping of pattern codes to intervals in sensor reading range is periodically refreshed for security. Then, cluster-heads determine the distinct pattern codes and request only one sensor node for each distinct pattern code to send the actual data to the base station. In addition to being energy and bandwidth efficient, this approach helps security because cluster-heads are not required to decrypt the actual sensed data for data aggregation.

6.Secure Information Aggregation in Sensor Networks

In this paper authors propose ”Aggregate-Commit-Prove” approach for secure data aggregation where the base stations check the correctness of the aggregated data by requesting sample small data pieces from sensors.

1) Aggregate

1)aggregator collect the data from sensors

2)compute aggregated result

2) Commit

1)commits to the data

2)Guarantee that result is computed using sensors’ data

3) Prove

1)Aggregator send the aggregate result and commitment to home server

2)home server -checks if commitment is good representation of the sensor data aggregation result is close to the committed data values.

7.SRDA: Secure Reference-Based Data Aggregation Protocol for Wireless Sensor Networks.

This paper mainly focus on data security. Secure Reference-BasedData Aggregation (SRDA) protocol that incorporates both data aggregation and security concepts together in cluster-based wireless sensor networks. SRDA exploits unique features of wireless sensor networks, continuous monitoring of the target area and dominant sensor to base station data flow, for its secure data aggregation technique. The basic idea behind SRDA is that nodes transmit the differential data rather than the raw sensed data.
The raw data sensed by sensor nodes are compared with a reference data and then only the difference data are transmitted.

8.Recoverable Concealed Data Aggregation for Data Integrity in W S N

In above two method ESPDA[5] and SRDA[7],the adversaries has the ability to capture cluster heads. It would cause the compromise of the whole cluster members. In RCDA, a base station can recover each sensing data generated by all sensors even if these data have been aggregated by cluster heads (aggregators). With these individual data, two functionalities are provided. It uses Encryption Scheme, based on the elliptic curve cryptosystem and Signature Scheme which aggregate signature which merges a set of distinct signatures into one aggregated signature.
Four procedures for homogeneous wsn

1)Setup

Base Station(BS) generates the key pairs.

2)Encrypt-Sign

Trigger while a sensor decides to send its sensing data to the cluster head(CH) .

3)Aggregate

Launched after the CH has gathered all ciphertext-signature pairs.

4) Verify

Receive the sum of ciphertext and signature from CH, BS can recover and verify each sensing data.

9.CDA: Concealed Data Aggregation for Reverse Multicast Traffic in Wireless Sensor Networks

In WSN the messages should be transferred in a confidential way. It is our aim that passive adversaries that eavesdrop communication between the sensors, aggregators, and the sink, cannot obtain the exchanged.A privacy homomorphism (PH) is an encryption transformation that allows direct computation on encrypted data .So each sensor nodes use PH scheme to encrypt the data and transmit to the aggregators where the data can be aggregated without decrypting the data. Finally the data transmitted to sink deciphers the data. The main weakness of asymmetric CDA schemes is that an AG can manipulate aggregated results without encryption capability. An AG is able to increase the value of aggregated result by aggregating the same cipher text of sensed reading repeatedly, or decrease the value by selective aggregation.

10.CDAMA:Concealed data aggregation for multiple applications in WSN network

Compromising a CH will allow adversaries to forge aggregated results [11] leads to as similar as compromising all its cluster members. To solve this problem, several studies, such as the ESPDA [5], SIA [6], and SRDA [7], have been proposed The proposed scheme, called CDAMA ,resolves above issues by using PH schemes, SNs of multiple applications encrypt their sensed readings and allow AGs to homomorphically aggregate their cipher texts without decryption. Therefore, compromising earns no advantage of forging aggregated results In CDAMA the base station exactly knows the number of messages aggregated to avoid insertion of falsify messages by obtaining the aggregated result M and its ζ count. If a malicious AG launches unauthorized aggregations, such as repeated or selective aggregation, ζ's value would be changed to a bigger or smaller value than the reference count.BS can detect based on the value ζ.

TABLE 1
COMPARISON BETWEEN DATA AGGREGATION SCHEMES

PAPER	ENCRY PTION	ARCHITE CTURE	KEY SHARING	SECURITY ATTRIBUTES	ADVANTAGES	DISADVANTAGES
SAWN	Hop-by-Hop	Tree based	Base station generates a key chain using a one way function F where $K_i = F(K_{i+1})$ and shares to sensor nodes	For confidentiality it is assumed that the sensor nodes are initialized with a symmetric secret key shared with the BS.The base station verifies the aggregate data using the MAC it receive	Provides lightweight security mechanisms to effectively detect node misbehavior (dropping, modifying or forging messages, transmitting false aggregate value).	The failure of any node cause failure of whole leaf nodes.
SDAP	Hop-by-Hop	Tree based	Every node shares a secret key with the base station and each pair of neighboring nodes share a pair wise key.	Probabilistic technique for integrity verification.	Base station identifies the suspicious groups based on the set of group aggregates.	Nodes receiving the request send back their data and id to the base station for verification which consumes much energy
EDA	End-to-end	Tree based	It is assumed that each sensor shares a distinct long term key K_i with the base station. This key is derived from a master secret, which is only known to the sink	For confidentiality protection, the encryption scheme which is additively homomorphic is used	Prevents a passive attacker(eavesdropper) from gaining any information about sensor data.	This scheme does not tackle the issue of data integrity
SHDA	Hop-by-Hop	Tree based	Each sensor is initialized with a unique identifier *s* and shares a secret key with the querier	Check the data for integrity using a distributed integrity verification technique	Novel method for distributing the verification of aggregation results onto the sensor nodes.	It need to know the set of responding nodes.

SHA	End-to-End	Tree based	Aggregation is using node's private key and encrypted using BS public key.The network wide integer used to generate a new public private key pair for each round of processing .	Authentication is done using aggregated signature. homomorphic encryption algorithm applied to the messages to achieve data confidentiality. ECDSA is used to achieve integrity.	Additively homomorphic encryption allows aggregation of encrypted values	It do not support multi layer hierarchical data aggregation
ESPDA	end to end	cluster based	Base station periodically broadcasts a session key .sensor node computes a node-specific-secret-key (NSSK) using the session key and the built in key for encrypting data	It sends the pattern seed periodically to all active sensor nodes to maintain the confidentiality of the pattern codes	ESPDA is the first protocol to consider data aggregation techniques without compromising security. More energy efficient technique.	It cannot support large sensor network
SIA	End –to-End	cluster based	Each sensor has a unique identifier and shares a separate secret cryptographic key with the home server and with the aggregator.	Base stations check the correctness of the aggregated data by requesting sample small data pieces from sensors.	Novel framework for secure information aggregation in large sensor networks.	The major drawback is this cannot be suited for very large networks.
SRDA	Hop-by-Hop	cluster based	collection of encryption keys is selected from a key pool to form a key set to be used	Aggregation specific security mechanism ensures message confidentiality by increasing security levels as aggregated data approach the base station.	Resilience against node capture and reduce the memory requirements of sensor nodes and unique property used which apply variable strength security in wireless sensor networks	Any conflict between aggregation and communication protocols might create loop holes in-network security such as violating data confidentiality.
RCDA	End-to-End	cluster based	BS generates the key pairs and shares with nodes.	Base station can verify the integrity and authenticity of all sensing data.	Reduces the corresponding delays during aggregations and BS securely recover all sensing data rather than aggregated results.	There occurs transmission overhead and signature scheme bring additional cost.
CDA	End-to-End	cluster based	Use topology-aware group keying by providing a key predistribution scheme suitable for transformations.	Confidentiality achieved by encrypting transmitted data	Increases security, while the additional efforts can be minimized .	No integrity and authentication of data
SDA	End-to-End	Cluster based	collection of encryption keys is selected from a key pool	cluster head uses this MAC for checking the integrity of the data.	Prevents false injection of data and filtering outliers	This scheme does not tackle the issue of data integrity
SDAV	Hop-by-Hop	Cluster based	CKE protocol is used to distribute secret shares to each sensor within a cluster.	Threshold signature provides authenticity of the data.	Base station never accepts faulty aggregate readings.	No integrity verification

CONCLUSION

Sensor Networks hold a lot of promise in applications where gathering sensing information in remote locations is required. The data aggregation is one of the main method used to reduce the power consumption in WSNs. Security is important issue in many applications and has been largely explored. Based on the security schemes CDAMA is more secure than any other CDA schemes .But there occurs a problem it cannot support when CDAMA(k>2)

which leads to fragments loss. Future more work is needed to provide secure and efficient aggregation over large area network.

REFERENCES

[1] L. Hu and D. Evans, "Secure Aggregation for Wireless Networks," Proc. Symp. Applications and the Internet Workshops, pp. 384-391,2003.

[2] A Secure Hop-by-Hop Data Aggregation Protocol for Sensor

Networks (SDAP)(Yi Yang, Xinran Wang, Sencun Zhu and Guohong Cao, "SDAP: a secure hop-by-hop data aggregation protocol for sensor networks". In MobiHoc '06: Proceedings of the seventh ACM international symposium on Mobile ad hoc networking and computing.).

[3] Secure Hierarchical In-Network Aggregation in Sensor Networks (SHDA) (Haowen Chan, Adrian Perrig and Dawn Song "A Secure Hierarchical In-network Aggrega-tion in Sensor Networks". In CCS 2006).

[4] Secure Hierarchical Aggregation in Sensor Networks (SHA) (Julia Albath and Sanjay Madria, "Secure Hierarchical Aggregation in Sensor Networks,". In Proceedings of IEEE Wireless Communications and Networking conference, 2009

[5] H.O. Sanli, "Energy-Efficient Secure Pattern Based Data Aggregation for Wireless Sensor Networks," Computer

Comm., vol. 29, no. 4, pp. 446-455, 2006.

[6] B. Przydatek, D. Song, and A. Perrig "SIA:Secure Information Aggregationin Sensor Networks", *Proc. of SenSys'03*, Nov 5-7, 2003, LosAngeles, CA

[7] H. Sanli, S. Ozdemir, and H. Cam, "SRDA: Secure Reference-based Data Aggregation Protocol for Wireless Sensor

Networks," Proc. IEEE 60th Vehicular Technology Conf. (VTC '04- Fall), vol. 7, 2004.

[8] RCDA: Recoverable Concealed Data Aggregation for Data Integrity in WirelessSensor Networks Chien-Ming Chen, Yue-Hsun Lin, Ya-Ching Lin, and Hung-Min Sun.

[9] J. Girao, D. Westhoff, M. Schneider, N. Ltd, and G. Heidelberg, "CDA: Concealed Data Aggregation for Reverse Multicast Traffic in Wireless Sensor

Networks," Proc. IEEE Int'l Conf. Comm. (ICC '05), vol. 5, 2005.

[10] CDAMA: Concealed Data Aggregation Scheme for Multiple Applications

In Wireless Sensor Networks Yue-Hsun Lin, Shih-Ying Chang, and Hung-Min Sun

[11] A. Perrig, J. Stankovic, and D. Wagner, "Security in Wireless Sensor Networks," Comm. ACM, vol. 47, no. 6, pp. 53-57, June 2004.

[12] D. Boneh, E. Goh, and K. Nissim, "Evaluating 2-DNF Formulas on Ciphertexts," Proc. Second Int'l Conf. Theory ofCryptography (TCC), vol. 3378, pp. 325-341, 2005.

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

[14] Energy-Driven Adaptive Clustering Hierarchy (EDACH) for Wireless Sensor Networks

Kyung Tae Kim and Hee Yong YounSchool of Information and Communications Engineering, Sungkyunkwan University, Suwon, Korea.