Current State of Art in Security of Data Aggregator in Smart Grids

Naina Emmanuel[a]
nemmanuel1992@gmail.com

Adeel Anjum[a]
adeel.anjum@comats.edu.pk

Sadia Shafiq[a]
sadia.shafiq93@gmail.com

Mahamud Hussein Adam[a]
ramadaan555@gmail.com

[a]Comsats Institute of Information Technology, Park Road Chak Shahzad Islamabad

Abstract: Multiple sensor nodes known as detection stations make the sensor networks; each node is light and portable. Every sensor node contains power source, microcomputer, transducer and transceiver. Power source provides power to each node. Micro-computer is used for storing and processing the output coming from the sensors. The transducer is used to generate the signals and the transceiver is used to receive and transmit data to the central computer. Eavesdropping gets facilitated with wireless communication, and it has many useful applications in military, homeland, hostile and uncontrolled environments. So it is prone to the high level of security. The process in which information is gathered to form a summarized type for analysis is known as data aggregation, as it is used to reduce the energy consumption in wireless sensor networks. The security issues have become crucial in data aggregation, especially when gets deployed in hostile and remote environment. In wireless sensor networks many secure aggregations have been proposed. It still faces some resource constrained that's why new techniques are needed. In our survey we will discuss those approaches and their pros and cons.

Keywords: Data aggregation, Security and Wireless Sensor Network.

1. Introduction

A wireless sensor network (WSN) contains distributed devices that use the sensors for monitoring their assets. [27] It has sensor nodes, gateways and software. The data gained is sent for further processing and analysis to the base station. Its design depends on the application and it's being used in military, law enforcements, reports of accidents and environmental and physical monitoring. Sensors in WSN have recourse constrained in power sources, memory and capabilities of communication and computation. As the sensors has their sensing range so most often their sensing range gets overlapped with each other in dense deployment, which causes to produce some similar data of raw network data. [39]

Due to the production of redundant data large power is consumed relatively large bandwidth for data transmission, making it [40] inefficient in energy constraint WSN. This problem leads us to the Data aggregation technology. It is a process of compiling information coming from different sources using aggregation functions to produce results, and send that result to high aggregated node. After this step the redundancy in the transmitted data is removed, results in reduction of bandwidth and energy consumed and increased accuracy of data and life time of network.

Limitations in resources are not only the factor in reducing [34] the performance of the sensor networks but deployment nature has same affect. Communication instability is also one of the factors, as if two sensors having aggregator node, when they will start sending packets simultaneously then the conflict will occur near the aggregator node causing the failure. Even in more congestion environment these sent packets get dropped, since WSN is connectionless regarding packer based routing. Consequently if channel error rate does not get maintained then it might lose key packets very essential for the security of the nodes.

Because of these limitations, developing new protocols for wireless sensor networks is difficult and challenging and single adaption Solutions designed for the wired networks are not sufficient for WSN.

Studies made by Wagner in 2004 [4], and Krishnamachari in 2002 showed that transmitting data requires more energy than the computation of data; it accounts 70% of energy in computation and communication. This huge energy consumption can be reduced by removing redundant data, which resultantly will have less data for transmission. Aggregators are more exposed to attacks since they are not furnished with tamper-resistant hardware.

In-network, processing is done by the aggregator node or aggregator point. So the aggregated is protected by the attacks to maintain the authentication, confidentiality and integrity of the data in hostile environments. Here the high level of security and privacy of Data aggregator point comes.

The compromised sensor node in the network produces false readings, fake messages, stops authenticated messages, do not uses aggregate function properly. Thus generates the false aggregated results. [2] The attacker behaves in such a real way that, these false results produced by corrupted node is not understood by the base station. Hence for securing the data aggregation from eavesdroppers and intermediate accesses we need security. This promotes the approach of End-to-End encryption than Hop-to-Hop encryption. Many protocols have been introduces to this security.

DA protocols are based on network architectures or topology and are divided into tree-based and cluster-based data aggregation. [25] The design of DA protocols is the challenging task as they can reduce the accuracy, latency and security of network if not designed properly. Thus the architecture of data aggregation protocols plays the vital role. [26] Cluster-based DA reduces the latency by grouping the nodes in tree-based. This grouping is called clustering. The main cluster head uses cluster-based data aggregation while the intermediate parent nodes use tree-based data aggregation in the path towards base station. [3]

The already made survey on secure data aggregation by Sang et al. (2006), divided the schemes into Hop-by-hop and end-to-end aggregation, but his classification did not provide security analysis and performance of mentioned schemes. What we have done in this paper is as follow:

- Introduction to secure data aggregation and security issues in WSN data aggregation
- Secure data aggregation schemes has been discussed in details
- Possible attacks have been discussed along with their solutions
- Different protocols have been discussed in detail along with their pros and cons
- Secure data aggregation framework has been presented that compares the data aggregation schemes.

Roadmap: The paper has been organized as follow: In section 2, security issues, aggregation types, major attacks on data aggregation with their prevention and adversary types has been explained in detail. In section 3, Hop-by-hop and end-to-end protocols and access to secret data have been presented in detail. In section 4, existing scheme's classification has been discussed. In section 5, comparison of existing schemes has been made. In section 6, discussion has been made and in section 7 this paper has been concluded.

2. Security and privacy in data aggregation

doi: 10.20944/preprints201607.0077.v1

2.1 Requirements for the security

Having security of the data aggregation point in wireless networks is the most challenging task because of the resources constrained and the hostile environment. The security needs of data aggregation in wireless sensor networks are: data integrity, data availability, authentication, confidentiality, data accuracy [31]. The protocols discussed in our paper tried to achieve security of above mentioned features that have been explained in detail later.

For secure data aggregation WSN scheme must have following features: [4]

- Approximation of reading of sensors, though les nodes gets compromised
- Freshness and integrity of data must be considered in scheme along with the confidentiality
- Self-healing property of node for dynamic response against attacks
- Load balancing of aggregator by conducting dynamic rotation of aggregator [32]

2.1.1 Integrity of data

Data integrity makes sure that the data has not been changed by any attack or accidently and it is in its original form. If some data aggregation technique provides confidentiality but not integrity then I will not be enough because the adversary can change the data without having information about it. [33]

2.1.2 Confidentiality of data

Data confidentiality makes sure that the data has not been viewed or revealed to any person other than the intended one. It is divided into end-to-end and hop-to-hop basis.

2.1.3 Authentication of data

Data authenticity and entity authenticity are two types. Entity authentication ensures that the sender or receiver is the claimed person. If this feature gets enabled in data aggregation then intruder won't be able to interfere in WSNs. Data authentication guarantee the data received is the original one. In the security of DAP two categories matter.

2.1.4 Availability of data

Availability ensures that the WSN is alive and its data is accessible. When the node gets compromised, it is recommended to remove that from the network, because attacker can affect the data availability through compromised node.

2.1.5 Freshness of data

Data freshness is making sure that the data is not old and is recent one. This security feature is important to avoid replay attacks. Even the adversary can mislead the sensor about the current key by replaying the distributed shared key. [38]

2.1.6 Accuracy of data

doi: 10.20944/preprints201607.0077.v1

Every data aggregation technique works to provide the accuracy of aggregated data. There is a trade-off between size of aggregated data and data accuracy because higher accuracy requires more bits and power.

2.1.7 Non-repudiation of data

Non-repudiation makes sure that the data has been transferred by the claimed person. The data aggregator point when sends data it should not deny sending, it will make base station to understand any change in the results of aggregation. [4]

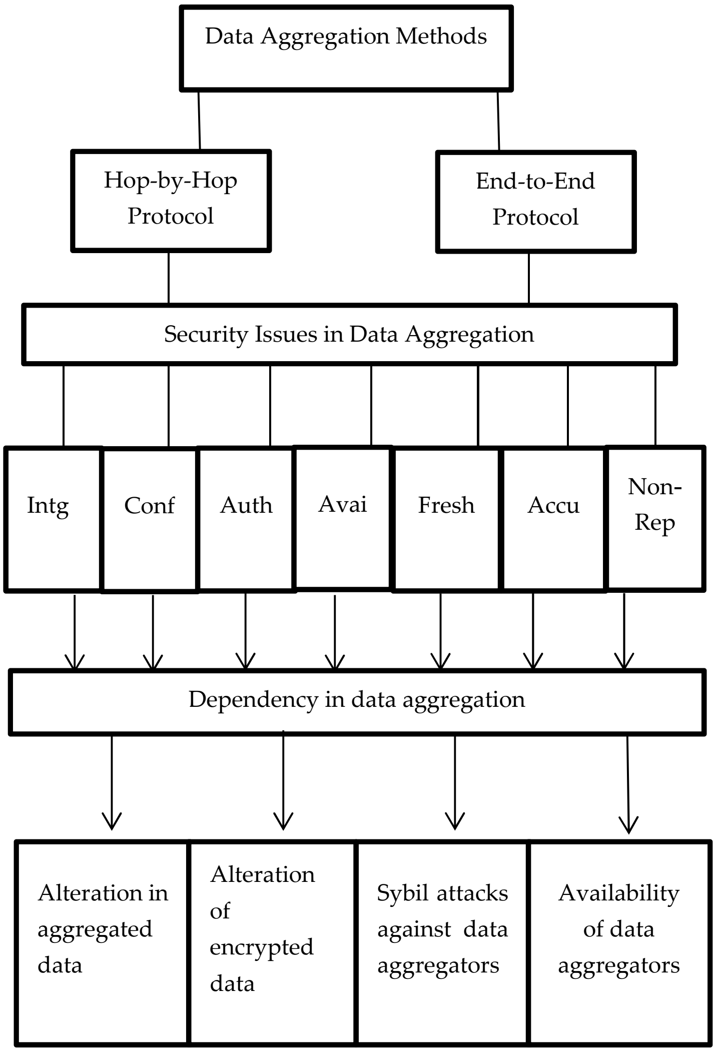
Data Aggregation Methods
Hop-by-Hop Protocol
End-to-End Protocol
Security Issues in Data Aggregation
Intg
Conf
Auth
Avai
Fresh
Accu
Non-Rep
Dependency in data aggregation
Alteration in aggregated data
Alteration of encrypted data
Sybil attacks against data aggregators
Availability of data aggregators

Figure1. Interaction between WSNs and DA process

2.2 Secure Data Aggregation types

doi: 10.20944/preprints201607.0077.v1

In wireless sensor networks data aggregation uses two methods: Hop-by-Hop data aggregation and End-to-End data aggregation. [1]

2.2.1 Hop-by-hop Data Aggregation

In hop-by-hop technique, sensing nodes encrypts and aggregator nodes decrypt the data and again encrypt the aggregation result. This encrypted data is travelled to the last sink node which decrypt the data. The Data Aggregation Point is vulnerable to any attacks because of data decryption.

2.2.2 End-to-End Data Aggregation

Data Aggregation Point aggregates the encrypted reading of sensors without decrypting. Intermediate nodes provide end-to-end privacy between the sink and sensor nodes. [5]

Table1. Comparison between data aggregation methods

Parameters	Hop-by-Hop	End-to-End
End to end privacy	No	Yes
Delay	Aggregation with delay	Aggregation without delay
Data integrity	Max. Data integrity	Min. Data integrity
Aggregation performed on	Plain sensor data	Encrypted sensor data
Computational cost	Low	High
Memory require	High	Low
Vulnerability	Passive attacks	Active attacks
Energy Consumption	High	Low
Data secrecy	Lesser security	High security
Computational power	High	Low

2.3 Major Attacks

There are two major attacks in digital world: Active attacks and the passive attacks. In passive attack the attacker does not change or insert the data but only monitor the transmission, while in active attack the adversary modify the data by interfering the connection. [7]

2.3.1 Sinkhole attack

The high capability node is a sink. So if the attacker gets the access to this higher node it can confuse or manipulate other nodes. In consequences he/she can get all the data.

The approaches like anomaly-based, rule-based, statistical, cryptographic and hybrid are used to deal with the sinkhole attacks. [19]

2.3.2 Sybil attack

In this type of attack the adversary within the network tries to present the more than one identity. After successfully launching the attack, the adversary can perform the following attacks:

- To generate multiple votes, it will create multiple identities to choose the aggregator. In this way it can elect the malicious node to become an aggregator. [24]
- Can generate difficult readings with multiple entries to affect the aggregated result.

- These multiple entries and identities can falsely validate the aggregated data, if n from m witnesses gets agreed on the aggregated results.

[20] For the prevention of Sybil attacks identity certificate mechanism is used. Sensor nodes are assigned unique information before deployment of nodes. Identity certificates gets bind against each node's identity. Using identity certificate node proves its possession of unique information.

2.3.3 Wormhole attack

This attack works on wormhole: a low latency link, which is between two parts of the network, the network messages get replayed over this link. A proactive routing protocol' i.e. DAWWSEN is used to prevent the wormhole attacks. It has hierarchal tree structure where root node is the base station and sensor nodes represent leaves. This protocol does not need geographical information of sensor nodes. [20]

2.3.4 HELLO flood attack

In Hello flood attack, adversary broadcasts HELLO packets to sender and receiver having large transmission power. The receiving nodes assume that the sender nodes are near to them. This attack causes the congestion in the whole network. [20] This attack can be prevented by noticing the bi-directional links, ensuring that nodes have accessibility to their parent only one hop away. A cryptographic technique deals with this attack.

2.3.5 Selective forwarding

In this type attack the nodes that have become malicious stop the certain messages' transmission (forwarding) by dropping them.

The defensive mechanism to the selective forwarding attack is the [21] beta and entropy trust mechanism. This protocol is based on two steps: detection of attacker and the re-routing awareness of the attacker.

2.3.6 Gathering passive information

If the attacker has the powerful resources, then with this power he/she can gather the data stream. These kinds of attacks can be prevented through strong encryption. [20] Passive gathering is prevented by using encryption.

2.3.7 Supervision attack

If one the nodes in the network gets compromised it can have secret information of all the network causing the network to be compromised. This attack is also known as node subversion.

2.3.8 Replay Attack

In this attack the adversary notes the traffic from the network, even if he/she does not understand it. Later on it will replay the saved traffic to misguide the aggregator. Like note the distributed shared key and after wards replay it to mislead the sensor node from the current one.

[22] Distributed Energy Efficient Clustering, Bloom filter and the Elliptic curve cryptography are the three main replay attack prevention techniques.

2.3.9 Stealthy attack

When the attacker injects the false data into the network traffic without making it disclosed then it is known as stealthy attack. This can badly affect the aggregation results. It also gets support from the Sybil attack by validating the results from multiple entries generated by the adversary [8, 22]. These types of attacks can

be prevented through the behavior-based detection i.e. local monitoring. It observes the neighboring node's behavior patterns and flagging the irregular patterns.
2.3.10 DoS attack
Denial of Service [20] attack makes the network to do not give response to its legitimate requests. This attack makes resources available to the compromised node, since it transmit extra packets and avoid legitimate user from tapping them. It causes flooding on the node.

2.4 ADVERSARY TYPE

2.4.1 Passive Adversary
The passive adversary eavesdrop the communication of the network, to get the sensitive information of sensed data. Attacker can monitor the aggregated results if the WSN does not have mechanism for ensuring confidentiality.

2.4.2 Active Adversary
Active adversary modifies the traffic in the network by injecting the packets, stopping or delaying the packets, compromising the nodes, destroying the nodes, manipulating and extracting the sensitive data. [9]

3: PROTOCOLS OF SECURE DATA AGGREGATION

3.1 Hop-by-Hop aggregation protocols
Hop-by-hop aggregation has the following protocols:

3.1.1 ESPDA
Pattern codes representing the characteristics of sensor data are the base of ESPDA. This protocol generates and transmits the pattern codes against the senor data instead of sending the whole sensor data. After the cluster head identifying the pattern code, it request for actual data from the node sending patterns. It reduces the data transmission. For security point of view the pattern codes' mapping gets refreshed after some interval. So this method is significant for energy, security and bandwidth efficiency. [10]

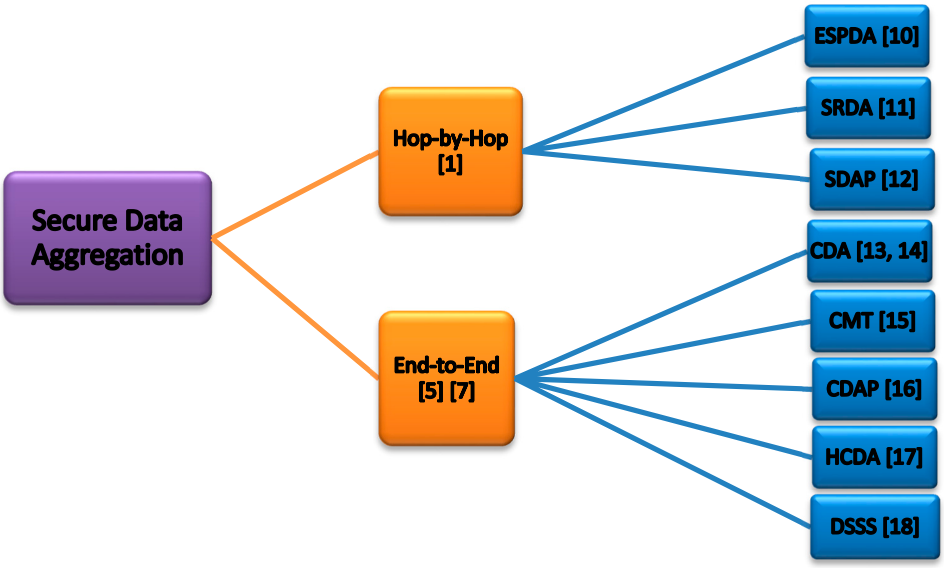

Figure2. Hierarchy of Secure DA Protocols

3.1.2 SRDA

This protocol sends the differential data by doing comparison between raw data to the reference data. It helps in reducing the size of data, by reducing no of bits. Consequently requires less energy consumption. For providing security SRDA has algorithm with security margin. Security is based on no of hops in the network from the base station. Firstly raw packets are transmitted to the cluster head reporting to higher head cluster. [11] The higher cluster head then generates reference entry for the node that has transmitted the raw sensed packets. Cluster head removes the reference entry when the session ends. This protocol can be applied in network at any level, because it is independent of clustering scheme. If the referenced value gets greater than the differential value then scheme's efficiency gets increased.

3.1.3 SDAP

Divide-and-conquer and commit-and-attest protocols [12] are the base of SDAP protocol. This protocol consists of three main steps. First step is to create the tress which child nodes to find their parent nodes and disseminate the query through tree. Second step is to dynamically partition nodes into different groups using probabilistic grouping technique that is dependent on group leader selection. Last step is the testing and verification step: suspicious groups are identified by the base station based on group aggregates then this suspected group verifies the trueness of the group aggregate. Verification process involves the verification of packet contents and aggregation message. This protocol has many advantages multiple aggregation functions' applicability, detection rate, confidentiality of data, source authentication and integrity, although it has a high energy consumption and transmission.

3.2 End-to-End aggregation protocols

The end-to-end protocols possess the based concealed aggregation which provides the confidentiality and privacy homomorphism application in network aggregation that allow cipher text data aggregation. [7] Privacy homomorphism is divided into two cryptographic methods: symmetric and asymmetric. In symmetric privacy homomorphism same key is shared between sensor and base station so base station has permission only to decrypt data coming from sensor node, providing end-to-end confidentiality. In the asymmetric privacy homomorphism nodes encrypt data using public key of base station and bas station can only decrypt it using its private key, maintain end-to-end confidentiality.

3.2.1 CDA

Concealed [13] data aggregation (CDA) protocol is based on the property proposed by the Domingo-ferrer [14], this symmetric additive privacy homomorphism property does not provide the confidentiality of individual sensor's data, since each node shares the same key with the base station. If one sensor node gets compromised then it will lead to decryption of each node. Each sensed data gets split in to'd' where d≥2 and encryption of this data is done by the same shared key. Encrypted sensed data is aggregated with other sensed data and then send to the sink, where data is decrypted using same shared key.

Replay attack, size grow, malicious aggregation and efficiency are some vulnerabilities to this technique and it does not address the non-response ID problem as well.

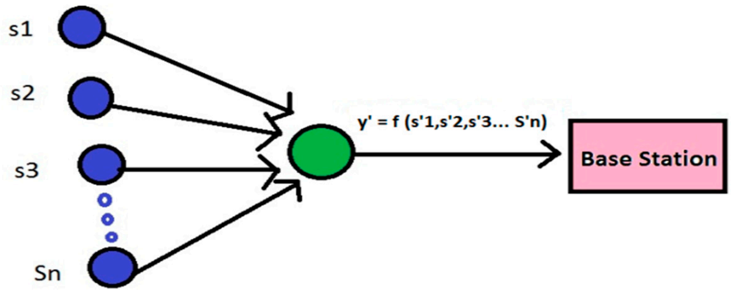

Figure3. CDA working

3.2.2 CMT-a key stream based PH

In this scheme each sensor node has different shared key with the base station. This technique resists replay attack. This is an extension of one-time pad with addition of modular than the Exclusive-OR of stream cipher. Encryption is done adding current key modulo with plain text and then aggregation is performed on encrypted values. Sink decrypt the data using that shared key, but it first requires that who contributed in aggregated results. It solves the ID problem by transmitting ID's of nodes, who have participated in encryption process, but it decreases WSN's life time and produce cost of additional communication of transmitting node's ID. CDA scheme having multiple shared keys provides end-to-end attacking between nodes, so it provides end-to-end confidentiality between nodes. This technique does not provide scalability since base station has to maintain the keys of aggregated packets. It doesn't provide integrity so it gets vulnerable to malicious aggregation. [15]

3.2.3 CDAP

Concealed [16] data aggregation using privacy homomorphism uses asymmetric privacy homomorphism: in which data is encrypted by public key of base station and decrypted by private key of base station by the base station. First public key of the base station is given to the AGGNODEs and then deployment of network is made. These AGGNODEs have special computational powers, memory and power source. Secondly AGGNODE shares shared key with its neighbors using any key distribution protocol. During data collection each node query sensor reading from its neighboring node, then this neighboring node encrypts data using RC5 algorithm and send to AGGNODE along with shared key. AGGNODE performs aggregation after decrypting the received data. The final aggregated results are then encrypted with base station's public key and forwarded to sink node. Because privacy homomorphism encryption [30] is being used, so data is concealed during sending data to sink from the nodes.

doi: 10.20944/preprints201607.0077.v1

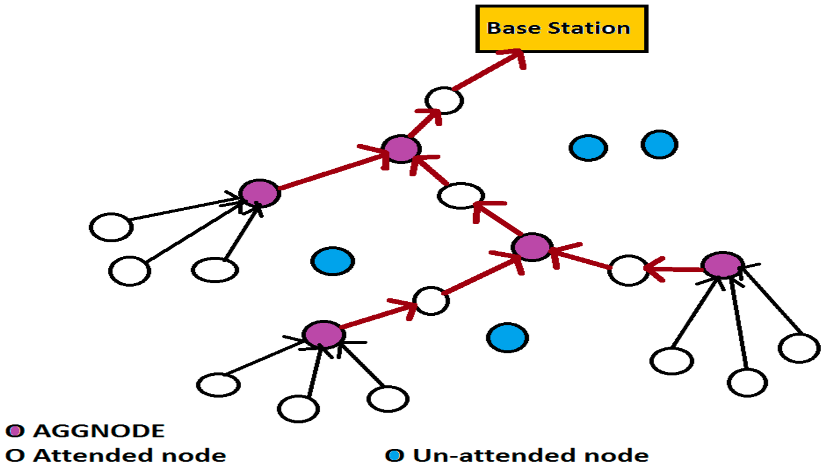

Figure4. CDAP working

3.2.4 HCDA

Hierarchical concealed data aggregation for WSN uses elliptic curve cryptography which saves it from node being compromised. [17] In this protocol uses different public keys to encrypt data. Its network scheme is based on groups. Sensor nodes are grouped before deployment of network and groups are deployed from specific location in such a way that every group covers network's part. Each group is assigned a public key and base station recognize the data of particular group from its public key that is being used to encrypt the data. In this way BS can easily identify the data from a particular region of the network.

3.2.5 Digital watermarking based on DSSS

In this protocol end-to-end authentication is gained using the approach of the [29] water marking. With water marking technique data can be validated from the node through sink. It removes the limitations in existing privacy homomorphism. Information related to authentication is modulated and superposed on sensed data and moved towards the sink. The node coming in the way of sink node aggregates the watermarked data. When data gets reached on sink, by validating the watermark on data it authenticates the received data. In this way it can check whether data has been changed by compromised node or not. [18] By visualizing the sensed data watermarking is performed, data which has been gathered from the whole network is converted into images, taking snapshots at particular time where node's reading is visualized as pixel's intensity and node as pixel. Direct spread spectrum watermarking is used for balancing energy consumption. When sink receives watermarked and aggregated data, it validates the watermark and hence authentication of sensor data. It provides a one way authenticity from the sensor node to the sink node. It also gives security in the process of in-networking on particular aggregation functions like sum, avg etc by doing cipher text aggregation.

doi: 10.20944/preprints201607.0077.v1

Table2. Comparison between DA protocols

Protocols	Authentication	Confidentiality	Integrity
ESPDA [10]	Yes	Yes	Yes
SRDA [11]	Yes	Yes	Yes
SDAP [12]	Yes	Yes	Yes
CDA [13,14]	No	Yes	No
CMT [15]	No	Yes	No
CDAP [16]	No	Yes	No
HCDA [17]	No	Yes	No
DSSS [18]	No	No	Yes

3.3 Accessibility of secret data

Secret data is the sensitive data in the nodes. While designing protocols, the designers for each scheme assume an adversary having different access levels to the secret information.

3.3.1 Total access

If the attacker has total access to the compromised node that he/she can manipulate all the sensitive data stored in nodes' memory and can harm or change aggregated results.

3.3.2 Partial access

When the adversary has partial access to the sensitive information stored in the sensor nodes' memory, he/she can get some of the data.

4: SECURE DATA AGGREGATION SCHEMES' CLASSIFICATION

In this part of the paper, we are classifying the secure data aggregation schemes into two models: single aggregator model and the multiple aggregator models, each model will be examined as having verification phase or no verification phase.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 25 July 2016 doi: 10.20944/preprints201607.0077.v1

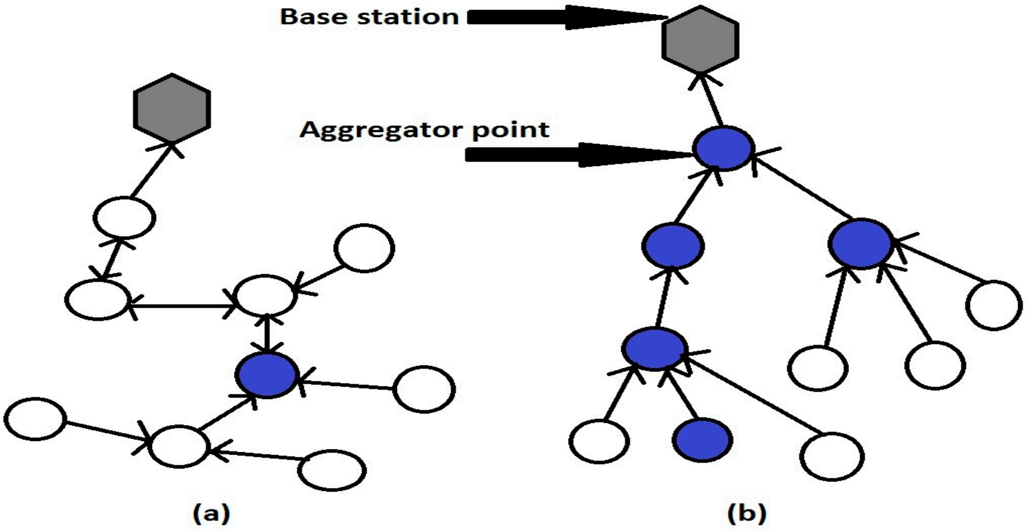

Figure5. (**a**) Single Aggregator Model; (**b**) Multi Aggregator Model

4.1 Single Aggregator Model

In this type of structure the aggregation take place only once between the base station and the sensor node. All the sensed data goes towards the single aggregator before going to the base station. [7] This single aggregator must have greater computational power and energy. This structure is best suitable when your requirement is small network or the query maker is not in the same network. This model is divided into two verification categories.

- Verification Phase: This phase provides information about the aggregator data being in its way to the query maker. This scheme enhances the ability to check between valid and invalid readings.
- No verification phase**:** This phase provide information which is not given by the verification phase. This scheme designer did not consider data integrity. In this phase adversary is honest and want to know about the sensitive information while he is not honest in verification phase for injecting false readings.

4.2 Multiple Aggregator Model

In multiple model data is aggregated many times before going to the destination. This scheme reduces the transmission bits and its sketch has been shown in figure 5 (b). This scheme fits when the requirement is large network. This model is again divided into two validation and no validation categories.

- Verification phase**:** Again it increases the ability of the query maker to check valid verses invalid aggregated readings. Multiple- aggregator verification phase is complex than the verification phase of single aggregator.
- No verification phase: This phase provide information which is not given by the verification phase. This scheme designer did not consider data integrity.

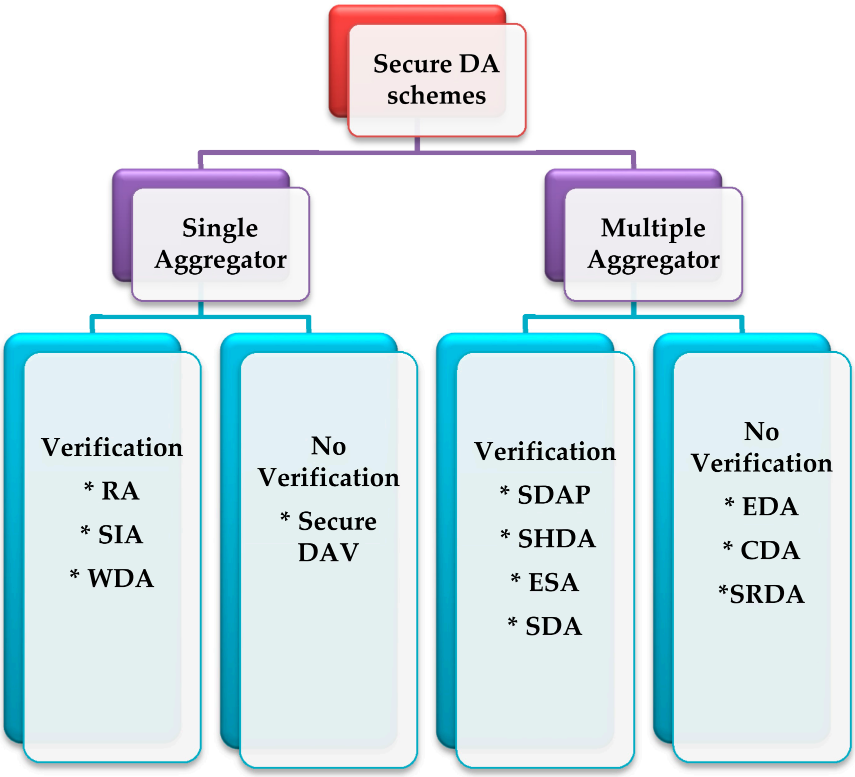

Figure6. Classifications of Secure DA schemes

5: COMPARISON BETWEEN SECURE DA SCHEMES

In this section comparison has been made between secure data aggregation schemes. Making comparisons between the schemes is the difficult task as the network architecture designer secures it from different angles.

Table3. Resistance against attacks in Secure DA Schemes

Scheme	DoS	Node Subversion	Sybil	Selective forwarding	Replay	Stealthy
CDA	No	No	Yes	Yes	Yes	Yes
SDA	No	No	Yes	No	Yes	No
SIA	No	No	Yes	No	Yes	Yes
SHDA	No	No	Yes	No	Yes	Yes
WDA	No	No	No	No	No	No
Secure DAV	No	No	Yes	No	No	No
SRDA	No	No	Yes	Yes	Yes	Yes
SDAP	No	Yes	Yes	No	Yes	No
ESA	No	No	Yes	No	Yes	No
EDA	No	Yes	Yes	Yes	Yes	Yes

doi: 10.20944/preprints201607.0077.v1

5.1 Existing Schemes

SDA [37] scheme was proposed by Hu $ Evans [4] in 2003, in which single node compromise scheme was studied. Resilience against the compromised node was achieved, delaying the aggregation at higher nodes. Damaged caused by the compromised node cannot be compensated, affecting node's data availability. **ESA** [4, 35] is the improved version of SDA given by Jadia $ Mathuria in 2004. In this protocol the designer uses one-hop keys pair for encrypting data between node and parent and two-hop keys pair for encrypting data between grandparent and node. Secure information aggregation [4] **SIA** framework was proposed by Przydatek in 2003 for WSN's. This framework is secure against the stealthy attack. It is consisted of three categories: home server, base station and sensor nodes, SIA takes each sensor as unique identifier. In 2002 Perrig used μTESLA for broadcasting authentic message.

Mathematical framework **RA** [4] was proposed by Wagner in 2004, for the evaluation of aggregation techniques. It provides better way for securing data aggregation in the wireless sensor networks. Warner suggested that trimming and truncation can be used to secure the aggregation primitives.

Table4. Comparison of Secure DA schemes

Scheme	Confidentiality	Integrity	Freshness	Availability	Authentication
CDA	No	Yes	Yes	Yes	Yes
SDA	Yes	No	No	Yes	No
SIA	No	No	No	Yes	No
SHDA	Yes	No	No	Yes	No
WDA	Yes	No	Yes	Yes	No
Secure DAV	No	No	Yes	Yes	No
SRDA	No	Yes	No	Yes	Yes
SDAP	No	No	No	Yes	No
ESA	No	No	No	Yes	No
EDA	No	Yes	Yes	Yes	Yes

Witness-based data aggregation, [4] **WDA** scheme was proposed by Du in 2003, this scheme validates the data being sent from node to base station. Witnesses (identities) approve the validation of the aggregated results, by computing MAC of the results. **Secure-DAV** [4] was suggested for improvement in SDA and ESA schemes to remove the data integrity issues. This scheme was given by Mahimkar $ Rappaport in 2004.

Yang in 2006 proposed hop-by-hop protocol known as **SDAP** in 2006, [4, 41, 26] this technique is known for tolerating more than one compromised node. It works on the principle of commit-and-attest. **SHDA** [4] gives data integrity, authentication ad confidentiality as SIA provides. This scheme was given by Chan in 2006, where parent node perform aggregation function when child node requests. It uses merkle hash tree to set inputs or computing aggregated results.

Sanli in 2004 developed **SRDA** [4] known as Secure Reference-Based Data Aggregation that transmits the difference between referenced and sensed data value instead of sending raw data. At higher cluster heads it uses higher security margin. Concealed data aggregation **CDA** was addressed by Westhoff in 2006 [4] [28] which uses the multiplicative and additive homomorphism privacy scheme. Another homomorphism privacy scheme **EDA** was proposed by Castellucia in 2005, [4, 36] this scheme aggregates the encrypted data. EDA does not use XOR operation used in stream cipher, since it has modular addition. Advantage of this scheme is that it maintains the confidentiality of the message even if the node gets compromised.

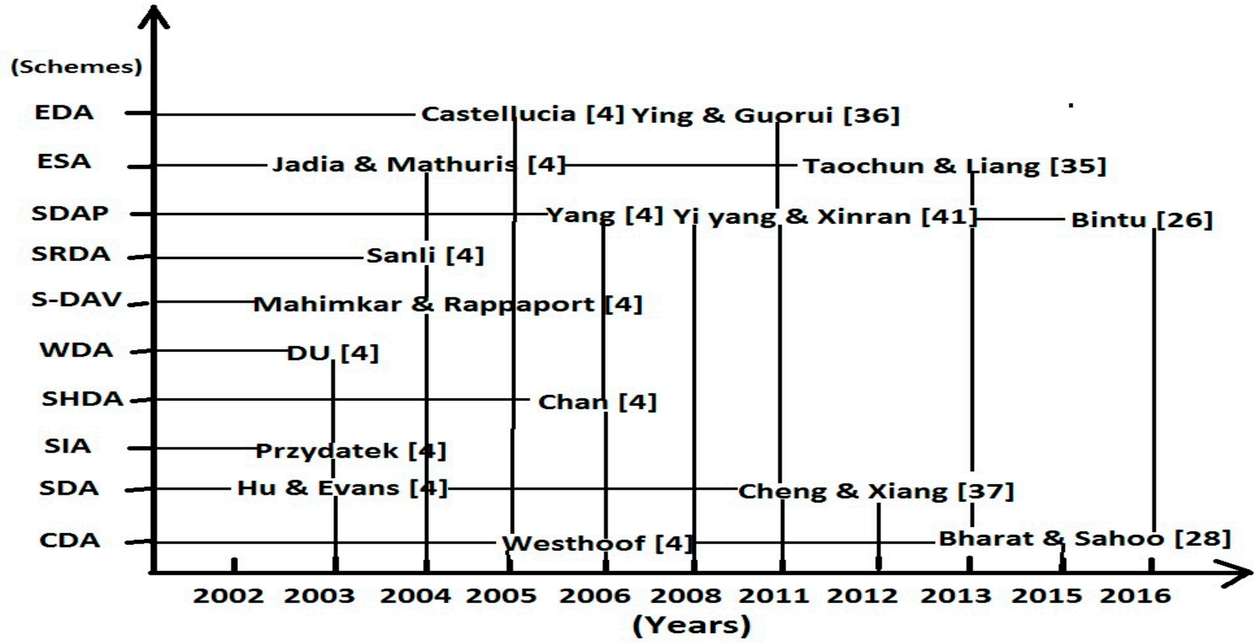

Figure7. Research timeline of Secure Data Aggregation Schemes

6: Discussion

In most of the protocols, confidentiality and authentication of the sensed data has been catered while freshness and integrity of the data has been dealt much. Though the freshness of the data is very much important, the adversary can eavesdrop the traffic in the wireless sensor network, note some traffic packets and can replay them in order to mislead the node. Any scheme or protocol must insure the freshness of the data and aggregated results.

Without the data freshness WSN's are vulnerable to replay attack, in which adversary even can replay distributed shared key to cause the confusion in the network. In this type of attacks schemes dealing with the confidentiality and integrity is not enough. In the same way data integrity should also be considered with confidentiality as confidentiality alone is not enough since the attacker can insert some packets or change the data without even knowing anything about the data. Attacker can insert or manipulate the results near the aggregator without detection.

7: Conclusion

In this paper, some issues in the secure data aggregation has been discussed, attacks on the WSN along with their detection and preventions have been given. Types of adversaries and access to secure data have been debated. Comparison between different secure data aggregation schemes has been made and their vulnerabilities against the attacks have been given. Reviewing all the protocols and schemes, it has been derived that confidentiality alone is not enough; integrity and the freshness of the data must also be considered while designing schemes of secure data aggregation.

References

1. Y.Sang and H.Shen. Secure Data Aggregation in Wireless Sensor Networks: A survey
2. Josna Jose, Joyce Jose and Fijo Jose. A survey on Secure Data Aggregation Protocols in Wireless Sensor Networks. International Journal of Computers Applications (0975- 8887) Volume 55- No.18, October 2012

3. Gunti Spandan, Archana Patel, C R Manjunath and Nagaraj GS. Data Aggregation Protocols in Wireless Sensor Networks. International Journal of Computational Enginering Research Volume 03 Issue 5
4. Hani Alzaid, Ernest Foo and Juan Gonzalez Nieto. Secure Data Aggregation in Wireless Sensor Network: a survey
5. Liehaung Zhu, Zhen Yang, Meng Li and Dan Liu. An Efficient Data Aggregation Protocol Concentrated on Data Integrity in Wireless Sensor Networks. International Journal of Distributed Sensor Networks Volume 2013 (2013), Article ID 256852, 9 pages
6. Ramesh Rajagopalan, Pramod K. Varshaney. Data Aggregation Techniques in Sensor Networks: A survey, 2006
7. Y.E.Aslan and E.Kayaaslan, Security in wireless sensor network, JOURNAL OF CS514 CLASS FILES, VOL.1, NO.1, JANUVARY 2008
8. A.Pandey and R.C Tripathi, A Survey on Wireless Sensor Networks Security, International Journal of Computer Applicationsc (0975-8887), Volume 3-No.2, June 2010
9. Mahimkar, A. & Rappaport, T. S. (2004), SecureDAV: A secure data aggregation and verification protocol for sensor networks, in 'Global Telecommunications Conference', Vol. 4, pp. 2175– 2179
10. H.Cam, S.Ozdemir, P.Nair, and D. Muthuavinashiappan, ESPDA: energy-efficient and secure pattern-based data aggregation for wireless sensor networks, IEEE Sensors– The Second IEEE Conference on Sensors, Oct. 22-24, 2003, Toronto, Canada.
11. H. Sanli, S. Ozdemir, and H. Cam, SRDA: Secure Reference-Based Data Aggregation Protocol for Wireless Sensor Networks, Proc. IEEE 60th Int'l Conf. Vehicular Technology (VTC 04-Fall), vol. 7, pp. 4650-4654, Sept. 2004.
12. Y. Yang, X. Wang, S. Zhu, and G. Cao, SDAP: A Secure Hop-by- Hop Data Aggregation Protocol for Sensor Networks, ACM Trans. Information and System Security (TISSEC), vol. 11, no. 4, pp. 1-43, 2008.
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. S.Peter and K.Piotrowski, On Concealed Data Aggregation for Wireless Sensor Networks.
15. C. Castelluccia, E. Mykletun, and G. Tsudik, Efficient Aggregation of Encrypted Data in Wireless Sensor Networks, Proc. Second Ann. Int'l Conf. Mobile and Ubiquitous Systems, pp. 109-117, July 2005.
16. S. Ozdemir, Concealed Data Aggregation in Heterogeneous Sensor Networks Using Privacy Homomorphism, Proc. IEEE Int'l Conf. Pervasive Services, pp. 165-168, July 2007.
17. S.Ozdemir and Y.Xiao, Hierarchical Concealed Data Aggregation for Wireless Sensor Networks.
18. W. Zhang, Y. Liu, S.K. Das, P. De, Secure data aggregation in wireless sensor networks: a watermark based authentication supportive approach, Elsevier Pervasive Mobile Comput. 4 (2008) 658–680.
19. Junaid Ahsenali, Usman Tariq, Arif Amin and Robert Rittenhouse. Dealing with Sinkhole Attacks in Wireless Sensor Networks. Advanced Science and Technology Letters Vol.29 (SecTech 2013), pp.7-12
20. Sampada A. Khorgade, Namrata D. Ghuse. Attacks and Preventions in Wireless Sensor Network. International Journal of Engineering Research and General Science Volume 3, Issue 2, Part 2, March-April, 2015
21. Youngho Cho and Gang Qu. Detection and Prevention of Selective Forwarding-Based Denial-of-Service Attacks in WSNs. International Journal of Distributed Sensor Networks Volume 2013 (2013)
22. Manju.V.C and Sasikumar.M. Mitigation of Replay Attack in Wireless Sensor Network Int. J. on Information Technology, Vol. 5, 2014.
23. Issa Khalil and Saurabh Bagchi. Stealthy Attacks in Wireless Ad Hoc Networks: Detection and Countermeasure.
24. Arabinda Nanda and Amiya Kumar Rath. Rough Set Approach for Malicious Node Detection And Secure Data Aggregation in WSN. International Journal of Applied Engineering Research ISSN 0973-4562 Volume 11, Number 8 (2016).
25. Rajasekaran and Dr V. Nagarajan. Improved Cluster Head Selection For Energy Efficient Data Aggregation In Sensor Networks. International Journal of Applied Engineering Research ISSN 0973-4562 Volume 11, Number 2 (2016).

26. Pooja Parmar and Bintu Kadhiwal. Secure Data Aggregation Protocol Using AES in Wireless Sensor Network. Emerging Research in Computing, Information, Communication and Applications, 2016.
27. Mauro Conti. Secure Data Aggregation. Secure Wireless Sensor Networks Volume 65 of the series Advances in Information Security pp 101-124, (2015).
28. *Bharat Bhushan and G. Sahoo*. Enhancement of Concealed Data Aggregation for Multiple Applications to Prevent Vulnerabilities in Wireless Sensor Networks. Networking and communication Engineering, Vol 7.
29. Djallel Eddine Boubiche,Azzedine , Samir Athmani and Homero Toral-Cruz. SDAW: secure data aggregation watermarking-based scheme in homogeneous WSNs. Telecommunication Systems June 2016, Volume 62.
30. Soufiene, Abdullah Ali and Abdelbasset . Confidentiality and Integrity for Data Aggregation in WSN Using Homomorphic Encryption. Wireless PersonalCommunications January 2015, Volume 80.
31. Sankardas Roy, Mauro Conti and Sushil Jajodia. Secure Data Aggregation in Wireless Sensor Networks. IEEE Transactions on Information Forensics and Security (Volume:7, Issue: 3), 2012.
32. Lei Zhang, Honggang Zhang and Mauro Cont. Preserving privacy against external and internal threats in WSN data aggregation. Telecommunication Systems April 2013, Volume 52, Issue 4.
33. Feng, T., Wang, C., Zhang, W., & Ruan, L. (2008). Confidentiality protection for distributed sensor data aggregation. In *INFOCOM'08*, April 2008 (pp. 56–60).
34. Hani Alzaid and Ernest Foo. Secure data aggregation in wireless sensor network: a survey. AISC '08 Proceedings of the sixth Australasian conference on Information security - Volume 81, 2008.
35. Taochun Wang,1Xiaolin Qin, and Liang Liu. An Energy-Efficient and Scalable Secure Data Aggregation for Wireless Sensor Networks. International Journal of Distributed SensorNetworks Volume 2013 (2013).
36. Guorui Li, and Ying Wang. An Efficient Data Aggregation Scheme Leveraging Time Series Prediction in Wireless Sensor Networks. International Journal of Machine Learning and Computing, Vol. 1, No. 4, October 2011.
37. Cheng Wang, Shaojie Tang, Xiang-Yang Li, Changjun Jiang. SelectCast: Scalable Data Aggregation Scheme in Wireless Sensor Networks. IEEE Transactions on Parallel and Distributed Systems (Volume:23 , Issue: 10), 03 January 2012.
38. Shehzad Ashraf Ch., Mian Muhammad Omair, Iftikhar Ali Khan and Tahir Afzal Malik. Ensuring reliability and freshness for Data Aggregation in Wireless Sensor Networks. International Journal of Machine Learning and Computing, Vol. 1, No. 3, August 2011.
39. Priyanka B. Gaikwad and Manisha R. Dhage. Survey on Secure Data Aggregation in Wireless Sensor Networks. Computing Communication Control and Automation (ICCUBEA), 2015.
40. Joyce Jose1 , M Princy2 and Josna Jose. EPSDA: Energy Efficient Privacy preserving Secure Data Aggregation for Wireless Sensor Networks. International Journal of Security and Its Applications Vol. 7, No. 4, July, 2013.
41. Yi Yang, Xinran Wang, Sencun Zhu and Guohong Cao. SDAP: A Secure Hop-by-Hop Data Aggregation Protocol for Sensor Networks. ACM Transactions on Information and System Security (TISSEC), Volume 11 Issue 4, July 2008, Article No. 18.