Secure Data Aggregation Protocols in Wireless Sensor Networks

Anish Soni[#1], Dr. Rajneesh Randhawa[*2]
[#]Punjabi University, Patiala (Punjab), India
[1]soni_anish@yahoo.com
[*]Department of Computer Science & Applications, Punjabi University, Patiala (Punjab), India
[2]drrajneeshrandhawa@gmail.com

Abstract: **Data communication between nodes in Wireless Sensor Networks consumes a large percentage of their total energy. Data Aggregation is one of the major techniques to preserve energy level in such type of networks because it eliminates the transfer of redundant data. But. Because of deployment in remote areas, the sensor nodes are easy target for the intruders to make attacks and gather the sensitive information. Different security goals has to be achieved by a good protocol but unfortunately none is perfect because of some tradeoffs in different security goals and energy consumption. Many secure data aggregation protocols have been proposed in wireless sensor networks which achieve one or the other goals viz Data Availability, Confidentiality, Integrity, Freshness , Authentication, Accuracy. In this paper, many existing secure data aggregation protocols have been analyzed deeply and compared in terms of the security goals they achieve. To the best of our knowledge, no such large number of protocols are compared before.**

Keywords: Data Aggregation, Security, Secure Data Aggregation Protocol, WSN.

I. INTRODUCTION

Wireless Sensor Network [1] is made up of number of sensor nodes having small size and low cost. These nodes are capable of sensing the surrounding environment and sharing the information collected through wireless links. Data gathered by a node from the monitored field is forwarded to the base station via multiple hops. Four basic components of a sensor node are sensing unit, transceiver unit , processing unit and power unit. Other than these, sensor nodes may also have application dependent additional components. WSNs have many applications such as in military field surveillance, environment monitoring, health care, accident reports, law enforcement, and also in home applications.

WSNs have many issues that affect their design and performance, few of them are related to their deployment, localization, synchronization, energy consumption and security. Out of these, energy consumption always remains the main issue because ones node is dead, other issues have no meaning. That is why extensive research has been done by different researchers to reduce the energy consumption of nodes after they have been deployed. Due to dense deployment of sensor nodes in WSN, nodes residing in the nearby area sense and transmit similar data which is useless in terms of energy and bandwidth usage. One of the solutions to this problem is data aggregation. Data aggregation [2] is a process in which data sensed by the nodes is aggregated using min, max, sum or average functions and transferred to the higher level aggregation node. Thus, decreasing the number of transmissions in the network, eventually reducing the bandwidth usage, eliminating unnecessary energy consumption and hence increasing the overall network lifetime.

Whereas aggregation reduces consumption of energy, in a hostile environment, there are also chances of different attacks on this aggregated data. There must be some provisions for protection of the nodes from different attacks such as selective forwarding attack , sybil attack, sinkhole attack, wormhole attack, node subversion etc. A compromised sensor node generates false reading and false aggregation result. Base station(Sink) is not capable of detecting the presence of compromised node because attacker present themselves in a manner that base station easily accept their incorrect results also. Therefore it becomes necessary to employed security with data aggregation so as to achieve data confidentiality, data integrity, data freshness, data availability and source authentication. There are two types of secure data aggregation protocols [3] depending upon the topology they used for aggregation. First topology used is tree in which the sensor nodes lies in the path from leaf to sink node makes data aggregation. The main issue in this type of protocols is to construct an energy-efficient data aggregation tree. Second type of data aggregation protocols are based on cluster formation where in each cluster, a head is chosen for aggregation and transmission of sensed data to the base station. Various secure data aggregation protocols have been introduced by different authors which achieve different security goals. In the subsequent section, we analyze and compare such protocols.

II. Secure Data Aggregation Protocols

A. SDA: Secure Data Aggregation [4]

Secure Data Aggregation (SDA) protocol is resilient to both: intruder devices and single device key compromise. This protocols works within the memory, power and computation limits of sensor nodes. This protocol focus on adversary who wants to corrupt the information produced by the sensor nodes rather than on those who places its own nodes in the network and use them to transmit the false values. Maximum processing is being done at the base station which makes the security mechanism very lightweight. SDA covers integrity rather than confidentiality. Two ideas which make this protocol more secure are aggregation delay and authentication delay. No sensor readings are aggregated at the next immediate node, rather forwarded unchanged and aggregated at the second node. This increases the integrity but if both parent and child are compromised, readings can be altered. This protocol saves resources because authentication is done after some time delay rather than immediately. It uses a µTESLA protocol for authentication of messages transmitted by base station and achieves asymmetry from clock synchronization and delayed key disclosure. Thus, this scheme offers data integrity, freshness and authentication.

B. SIA: Secure Information Aggregation [5]

For large sensor networks, authors proposed a framework using aggregate-commit-prove approach which is suitable for secure aggregation. This approach has three phases: first is data aggregation i.e. gathering the data from different sensor nodes and computing the aggregation result locally; second is commitment i.e. committing the collected data using Merkle hash-tree construction and the third phase is reporting & proving in which aggregation results are reported to the base station after its correctness is proved. It is assumed that by constructing efficient random sampling techniques and interactive proofs, user can be able to verify that the value finally produced by the aggregator node is very much close to the true value. This was probably the first paper that can handle the corrupted aggregator as well as some of the corrupted sensor nodes. This proposed framework provides resistance against a special type of attack called stealthy attack. In this attack, the attacker forces the user to accept false aggregation results, which are different from the results actually computed by the sensor nodes. It works on the forward secure authentication scheme in which attacker is not able to modify any reading recorded locally by the sensor node before the attacker makes the sensor node corrupt. Three different types of nodes are working in this scheme: a base station, a home server and normal sensor nodes. Assumption is made that an unique id is given to each sensor node. A secret cryptographic key is shared with home server and another key with the aggregator. Furthermore, it is assumed that a set of uncorrupted sensor nodes in the network can reach each other via paths composed of only uncorrupted sensor nodes. Thus data integrity, data authentication, data freshness, and data confidentiality are provided by SIA.

C. ESPDA: Energy-Efficient and Secure Pattern-based Data Aggregation Protocol [6]

In ESPDA, author proposed a protocol to provide energy-efficient data aggregation together with secure data communication in wireless sensor networks. It is a cluster-based data aggregation protocol. In ESPDA, cluster-head first broadcasts the pattern seed to the sensor nodes and requests them to send the corresponding pattern.code. These pattern codes are generated using the secret pattern seed sent by cluster-head. These patterns are analyzed by the pattern comparison algorithm at the cluster-head. If multiple sensor nodes send the same pattern code to the cluster-head because of sensing the common data, then only one of them is permitted to transfer the data. Thus, data aggregation is performed even before the actual data is transmitted from the sensor nodes.

ESPDA also provides security because it aggregates data by pattern codes, and therefore there is no need even for the cluster heads to know about the contents of the data. Data transmitted to the base station in encrypted form without any need to decrypt it in the middle, ESPDA employs a Non-blocking Orthogonal Variable Spreading Factor (NOVSF) code hopping technique. Sensor nodes compute a node-specific-secret-key (NSSK) using their unique secret built-in key and a session key broadcasted by the base station. This NSSK is used for the encryption and decryption of the data during transmission. Thus, ESPDA is an energy-efficient, bandwidth efficient, and secure protocol. It provides data freshness and confidentiality.

D. SecureDAV: A Secure Data Aggregation and Verification Protocol [7]

In this paper, author proposed a cluster-based data aggregation protocol in which aggregated data is signed for improving the data integrity. In public key cryptosystems, bootstrapping is not a favorable solution because of resource poor sensor nodes. An elliptic curve cryptosystems (ECC) is therefore used for establishing cluster keys using verifiable secret sharing because of its smaller keys, power to compute fast and need of lesser resources like reduced space, bandwidth and processing power. A secret cluster key is shared among each sensor within a cluster. Each cluster head receives the sensor readings from all nodes in corresponding cluster, aggregates the data and broadcasts the computed average to nodes again. Now every node compares its reading with the average and calculate the difference. If it is less than a threshold, node will partially sign the average value and send it to the cluster head. Cluster head now combines all such partial signatures received from

different nodes, combines them to form a full signature and send it along with the average reading to the base station. At the base station, validity of this signature is verified which ensures authenticity of the protocol. The integrity of the readings is ensured using Merkle Hash Tree avoiding over-reliance on cluster-heads. Thus data confidentiality, data integrity and authentication are provided in this protocol.

E. SRDA: Secure Reference-Based Data Aggregation Protocol [8]

Rather than sending the raw detected information, in this information collection procedure, nodes sends the differential information i.e. difference between the detected information and the reference esteem. Reference value is taken as the normal estimation of past sensor readings. Every sensor node first sense the information from environment, then figures the differential information, encodes it, and send it to the cluster head. SRDA gives a key circulation plan with low memory overhead to build up secure correspondence joins in the system and to save the energy. It executes variable quality security at various levels of the hierarchy i.e. the security level of the system is bit by bit expanded as the information is flown out to higher level cluster head. RC6 with flexible parameters is utilized to execute expanded security levels.

In this manner, SRDA fuses both information collection and security ideas together in cluster based remote sensor system. At long last, a correlation is made with ESPDA and demonstrated the upgrades accomplished by SRDA over ESPDA. SRDA provides data confidentiality, data freshness, and authentication.

F. CDA: Concealed Data Aggregation [9]

In paper, authors addressed the problem of aggregating encrypted data in WSN. They proposed a protocol this called CDA, in which an additive and multiplicative homomorphic encryption scheme is used to allow the aggregator to aggregate encrypted data. In this approach, every sensor node shares the same key with the base station. So it doesn't give assurance to the security of separately detected information in light of the fact that once a sensor node is bargained, it prompts the decoding of different sensors information. In this protocol, every sensor node parts its information into "d" parts (where d<=2) and encode them using the basic key which it shared with the base station and send these parts to the aggregator node. Aggregator totals the encoded sensor information with different sensors scrambled information in light of security homomorphism property and sends this collected result to the sink. This totaled information is decoded at the sink utilizing the same key utilized for the encryption. The developers of this protocol have applied the privacy homomorphism (PH), proposed by Domingo Ferrer, in which encrypted data is directly computed and is suitable to aggregation function average and movement detection. There are some disadvantages of this protocol such as its vulnerability to replay attack and malicious aggregation, expensive encryption, additional communication overhead, and also this protocol does not address the problem of non-response ID. The authors of this protocol argued that the security level of this protocol is reasonable, but Wagner proved that PH is unsecured against chosen plain text attacks. Thus, CDA ensures only data confidentiality.

G. SDAP: Secure Hop-by-Hop Data Aggregation Protocol [10]

Authors proposed a protocol which can endure more than one attacked node and depends on commit-and-attest and divide-and conquer standards. This universally useful information aggregation protocol has three stages. Initial step is tree development and question dispersal, in which an aggregation tree is built and along these lines all nodes recognize their parents, after which the base station scatters the total inquiry message through the tree. Second step is probabilistic gathering and information collection, in which SDAP utilizes the divide-and-conquer guideline to separate the system tree into various intelligent sub-trees taking into account a probabilistic gathering method which depends on group leader selection. Then it generates one group aggregate from each group by hop-by-hop aggregation. Any group cannot deny its aggregate because of commit-and – attest principle of SDAP. The third step is verification and attestation, in which the content of data packet and the authenticity of leader are verified first. After that, using a multiple-outlier detection algorithm, suspected groups are identified by the base station. These suspected groups has to undergone through a attestation process to prove the correctness of their group aggregate.

This protocol has advantages such as it is applicable on multiple aggregation functions, adjustable detection rate, provides data confidentiality, data integrity and source authentication. On the other side transmission overhead and energy utilization of this protocol is high.

H. SELDA: Secure and Reliable Data Aggregation [11]

This protocol is based on the fact that how much trustworthy are the normal sensor nodes and the nodes which are playing the role of data aggregator. Higher the trustworthiness of nodes, higher the security and reliability even in the presence of compromised sensor nodes. In the initial stage, a web of trust is generated by exchanging the reputation values among sensor nodes. Reputation values of neighboring sensor nodes is calculated using Beta Distribution Function. Honest sensor nodes are always having higher reputation values than the compromised nodes. This helps in determining the safe paths to data aggregators those are reliable. In the next step, taking the reputation value of data aggregator as reference, data of each sensor node is weighted and for this, Reliable Data Aggregation (RDA) algorithm is used. In the final step, data transmission is done

through multiple paths to reduce the forged data and selective forwarding attacks.For this purpose, a multi path data transmission algorithm is used which is secure enough to select some paths based on their reliability and keeps the quantity and identity of the selected paths secret. The sensor node transmit its data to data aggregator over those selected secure paths which ensures the secure data delivery to data aggregators. Thus, in SELDA, reliability of the aggregated data is increased with minimum communication overhead.

I. SEDAN: Secure and Efficient protocol for Data Aggregation [12]

Two hops verification mechanism of data integrity is the base of this protocol. In this mechanism, each node can verify immediately the integrity of its two hops neighbor's data and the aggregation of the immediate neighbors. Thus useless transmission of bogus data is avoided and energy consumption is reduced. Secret between any two hops neighbors is shared using "two hops pair-wise key" without any information to the intermediate node. While transmitting data, each node calculates a MAC with the grandparent using this key.Since this key is not known to the immediate neighbor, integrity is maintained and updated values are known only to the grandparent.

This scheme assumes a tree communication topology and its process consists of five steps. The first step is "key establishment", in which all the needed pair-wise keys are established. Second step is "data authentication", in which a node send the data accompanying its ID, sequence number, One hop and Two Hop MAC . The third step is "one-hop data integrity verification", in which a node after receiving the data packet from child node, verifies its one hop MAC to validate the origin of the packet and stores the rest of the information. The fourth step is "authentication of aggregated data", in which the data received from all child nodes is aggregated by each node and one hop MAC and two hops MAC of this aggregated result is calculated and send to its parent node. The final step is "two-hops data integrity verification", in which the grandparent node verifies the two hop MACs of each of its grandchildren and also computes the correct aggregation value of its child node. Then it compares its calculated value with the value generated by its child node. Thus, without delay, all the faulty aggregation values can be detected in SEDAN.

J. RSDA: Reputation-based Secure Data Aggregation [13]

Authors proposed another protocol that integrates reputation system in data aggregation functionalities so as to upgrade the system lifetime and the exactness of aggregated information. RSDA is made out of two types of nodes: a base station and ordinary sensor nodes. The objective territory, where RSDA is actually implemented, is separated into littler non-covering cells of equivalent zones. In the bootstrap duration, each sensor node finds its neighboring nodes and computes the shared keys and cell keys because this is the only duration in which there are no chances of any kind of attack. After monitoring the behavior of other nodes in the same zone, each sensor node computes the reputation value for them. In light of the figured reputation values, one of the sensor nodes is chosen to be the Cell Representative. The final data aggregation procedure starts when the base station broadcasts a query message to every cell. The cell representative confirms its cell reading, aggregate it with other readings and make it forward to the upper cell. After receiving the answer for its query, base station finds the information regarding the events in the field.

RSDA is equipped for recognizing traded off nodes and afterward ignore them which achieves its two primary objectives: develop the system lifetime and secure the accuracy of the collected information. Other than information exactness and accessibility, it additionally gives other security services, for example, data integrity, data freshness and authentication. It provides resistance to selective forwarding attack, replay attack, and stealthy attack. But it suffers from the node compromise attack.

K. SEEDA: Secure End-to-End Data Aggregation [14]

SEEDA is a secure data aggregation protocol in which two confidentiality requirements are considered. First one is generic confidentiality in which no access to the data is given to those sensor nodes which are not participating in aggregation mechanism. Another one is end-to-end confidentiality in which sensor nodes which are participating in aggregation, have no access to the already aggregated data. Three types of nodes: sink node, sensor nodes, and aggregator nodes, are arranged in a m-ary tree with sink node at root.

The best features of hop-by-hop and end-to-end aggregation schemes are used in this protocol ensuring end-to-end data privacy and minimum transmission data. A tree of height h is built in starting phase of node deployment and the levels are given 0,1,2…….h with sink node at level 0. Nodes at level h are the leaf nodes and they sense the data and encrypt it using secret key. This encrypted data is transmitted to the h-1 level where aggregator node adds it with its own data and computes the aggregate. For nodes which are not responding anymore, message value 0 is added to the aggregated data. Also the numbers of such nodes is appended to the message. This process is repeated at all the higher levels upto level 1. At level 0, the message is decrypted by sink node and average is computed. This protocol has reduced number of bits transmission on an average.

L. EEHA: Energy-Efficient and High-Accuracy Secure Data Aggregation [15]

The main goal of this protocol is to achieve highly accurate aggregated data while focusing on the low consumption of battery. The focus of this protocol is to make it secure from eavesdropping attack in which attacker tries to captures the private information passing through the wireless channel. This protocol consists of three types of nodes: base station, intermediate nodes, and leaf nodes. The process starts with the construction of aggregation tree, which is a directed tree formed by the combining all paths from the sensor nodes to the sink node. Then the leaf nodes adopt "slicing and mixing" strategy in which they slice their private data into pieces, and send these pieces to different neighbors while one piece is kept by itself. All the leaf nodes wait for a certain time and then mix (or sum) all the received slices and the slice of its own for a new result. This result is encrypted and sent to the intermediate node. The intermediate node aggregates the received data and its own sensor reading, & then forward it to its parent. The result is propagated level by level up the tree and reaches the root, at which the final data is the summation of all the sensors data. In this protocol, the "slicing and mixing (assembling)" is only implemented at the leaf level nodes of the tree, hence reducing the communication overhead, which in turn, leads to less message collision resulting high level of aggregation accuracy. EEHA is very energy-efficient because of the low communication overhead. Leaf nodes use slicing and assembling technique for data privacy while intermediate nodes use aggregation functions.

M. IPHCDA: Integrity Protecting Hierarchical Concealed Data Aggregation [16]

This protocol provides data integrity and confidentiality and also allow aggregation of data hierarchically encrypted with different keys . Hierarchical data aggregation is achieved using message authentication codes (MAC) and privacy homomorphic encryption scheme. IPHCDA assumes a group based network deployment in which a public/private key pair is assigned to each group (public key to sensor nodes and private key to base station). Every sensor node of a region also shares a unique MAC key with the base station.

Each sensor node sense the data, encrypts it with public key of its corresponding region and sends the results to data aggregator node. Aggregator node, using the shared symmetric key, calculate the MAC of the received encrypted data. using the XOR function, MAC of each region is combined and then sent to the base station. While decrypting the data, base station classifies aggregated data using the encryption keys and verifies its MAC, thereby achieving data integrity. IPHCDA provides resistance to various attacks such as ciphertext analysis, known plaintext attack, replay attack, unauthorized authentication, forge packets, and physical attacks.

N. RCDA: Recoverable Concealed Data Aggregation for Data Integrity [17]

This protocol is also called "recoverable" protocol because the base station in this protocol is capable of recovering all the data which normal sensor nodes generate even after the process of aggregation by cluster heads. Authenticity and Integrity of sensed data can be verified at base station and also any aggregation function can also be applied. RCDA is a cluster-based aggregation protocol, in which network is partitioned into different clusters, each one having a cluster head whose responsibility is to collect and aggregate the sensed data. In this protocol two RCDA schemes have been proposed: RCDA-HOMO for homogeneous networks and RCDA-HETE for heterogeneous networks.

In RCDA-HOMO, there are four procedures. The first is "Setup" in which all the necessary secrets for the base station and sensors are prepared and installed. The second procedure is "Encrypt-Sign" which is performed by sensors before sending their sensed data to cluster-head. The third procedure is "Aggregate" which is performed by cluster-head once it receives all results from its members, and then sends the final result to base station. The last procedure is "Verify", in which the base station first extracts individual sensing data by decryption of aggregated data and then verifies the integrity and authenticity of decrypted data.

RCDA-HETE has two types of sensors: L-Sensors (low-end sensors) and H-Sensors (high-end sensors). H-sensors are having stronger computation ability and stable power supply and therefore act as cluster-heads. In RCDA-HETE, there are five procedures. The first is "Setup" procedure in which H-Sensor and L-Sensor are loaded with necessary secrets. When L-sensors wants to send the data which they sensed, to the corresponding H-sensors, the second procedure "Intra-cluster Encrypt" is employed. In the third procedure "Inter-cluster Encrypt", each H-Sensor node aggregates the received data, encrypts it and sign the results.. The fourth is "Aggregate" procedure which is activated if an H-Sensor receives cipher texts and signatures from other H-Sensors on its routing path. The last is "Verify" which ensures the integrity and authenticity of each aggregated data.

O. CRSR Secure Data Aggregation Algorithm [18]

This algorithm utilizes cluster based information conglomeration method by utilizing LEACH-KED calculation to form clusters. CRSR plays out the four phases of operation i.e. C-Challenge the companions, R-Rate the companions, S-Share companions, R-Routing through companions. The initial three phases of the calculation are occasionally rehashed while the last stage is executed at whatever point required. This calculation begins with the testing procedure in which trusted nodes are recognized by sending an underlying

test. The nodes which finish the test discover place in the companion rundown and rest are moved to the question mark list which contains data about the malicious nodes. At that point the second stage comes in which the companions are evaluated on a scale of zero to ten on the premise of the measure of information they exchange through themselves and as indicated by the rating of different companions which is acquired amid the companion list sharing procedure. At that point the phase of sharing the companions comes, in which any node can request a companion sharing solicitation, and after companion sharing difficulties are started for those nodes which were not in the companion list. The last stage is directing through companions in which, when a node needs to transmit information, it initiates a route request message. At the point when the destination node gets the route request, it sends route reply and its public key. On getting the route reply message, the source hub assesses the best route with the large number of trusted companions to transmit the information. An ad-hoc on demand distance vector (AODV) routing protocol is utilized for transmitting information safely to the destination. The information to be sent is encoded by utilizing Diffie-Hellman algorithm to improve secure routing. Along these lines the odds of man-in-the-middle attack and eavesdropping are enormously diminished. Henceforth, this protocol gives an effective method for information transmission even within the sight of malicious nodes by recognizing them and putting into question mark list.

P. PEPPDA: Power Efficient Privacy Preserving Data Aggregation [19]

For time bound and secure applications having limited resources , this data aggregation scheme provides data freshness, privacy and authenticity of individual sensed data and confidentiality and accuracy of the aggregated data. Using slicing and assembling operations on the nodes at leaf level , privacy is achieved. Encrypted data aggregation is used for data confidentiality. Each node's secret key and its ID pair is used for message authentication.. Data Freshness is achieved through changing the encryption key for every session.

Three types of nodes are considered in this protocol: base station (sink or query station), intermediate nodes (aggregators), and leaf nodes (normal sensor nodes). This protocol consists of four steps. First is aggregation tree construction which is done using TAG protocol. In the second step, slicing is performed where each node at leaf level, senses the data, slice it into pieces, encrypts it using the session key from the base station and send these slices (one is kept to itself) to neighbors after appending the node ID. The third step is mixing. All the nodes receives encrypted slices and sums up them using privacy homomorphism technique. Aggregation is done at fourth and final stage. The aggregation result passes to the upper levels sequentially until it reached to the base station where it is decrypted using the decryption key and the aggregated result is generated.

Q. EESSDA: Energy-Efficient and Scalable Secure Data Aggregation [20]

There is no need of encryption and decryption operations in this protocol during the process of data aggregation. Secure channel establishment and slicing of data at leaf nodes is used to secure data aggregation process. There are three types of nodes considered in this protocol: the Sink, intermediate nodes, and leaf nodes. This protocol adopts a random key distribution mechanism which consists of three phases: key pre-distribution (each node selects k keys from key-pool to form a key ring), shared-key discovery (a secure link is established between neighbors which share common key), and path-key establishment (secure link is established by two or more multihop if no common key is shared between neighboring nodes).

EESSDA consists of five steps. The first step is "aggregation tree construction", in which the network is organized as a tree rooted at the sink node where each sensor node has a shortest routing path to the sink and also all the parent-child nodes share a common key. The second step is "secure channel establishment", in which each intermediate node establishes a secure channel with its parent or child node by sharing a common secret random number and also each leaf node establishes a secure channel with its parent node and neighbors. The third step is "slicing", in which leaf node slices its data into pieces before sending to parent node so as to ensure the confidentiality of data but one of the slices is kept at the leaf node itself. The fourth step is "assembling and mixing", in which all nodes wait for a certain time to receive all slices and then each leaf node aggregates the data received from different slices and the slice of its own to make a new result. The final step is "aggregation", in which leaf node sends the new result to its parent (intermediate node) through secure channel. After receiving all data from child and leaf nodes, intermediate node performs an aggregation function to get a new result which is further forwarded to its parent through secure channel. The process goes on and hence the final aggregation result reaches the sink.

EESSDA provides privacy by the use of secure channel and slicing & assembling technology. It is an energy efficient protocol as it does not require the encryption/decryption in the processing of data aggregation. The amount of traffic is reduced in this protocol which results in high accuracy of aggregation because the chances of data packets collision are reduced.

R. ECIPAP: Efficient Confidentiality and Integrity Preserving Aggregation Protocol [21]

In this paper, authors proposed an efficient aggregation protocol which preserves integrity and confidentiality. It is assumed that an aggregation tree is already set up in the deployment phase or if not already set up, then TAG can be used to build such tree-based network. Before the deployment of sensor nodes in the monitory area, a large integer, a private key and a unique ID is shared with base station by every node.

This protocol has three phases: query dissemination, aggregation of data , and checking the results. In the first phase, base station broadcasts a query message along with a random number to all the network nodes by using an authenticated method μTESLA. On receiving the query message, sensor nodes store it in their RAMs and then start the data aggregation phase. Next, it generates temporary keys so as to encrypt these parameters. Then message authentication code is computed by the sensor node and a data tuple is prepared which contains the encrypted parameters and MAC of that node. This data tuple is sent to the parent node. The parent node then aggregates the data tuples received from its child nodes along with the data tuple created by itself. This result is then transmitted to the next higher level of the tree and eventually the final result is transmitted to the base station. In the result-checking phase, the base station first decrypts the message and then broadcasts the aggregated tuple down to the whole network using authenticated method. The intermediate sensor nodes aggregates the received authentication messages and aggregate them using MAC aggregation function. The base station also calculates this authentication message with its own data stored before network deployment. These two messages are then compared to verify if all the sensing data is added to the final aggregation result. The base station accepts this aggregation result only if it passes the verification phase.

III. COMPARISON TABLE

TABLE I. Comparison of various secure data aggregation protocols

Protocol	**C**	**I**	**A**	**F**
SDA (2003)	×	✓	✓	✓
SIA (2003)	✓	✓	✓	✓
ESPDA (2003)	✓	×	✓	✓
SecureDAV (2004)	✓	✓	✓	×
SRDA (2004)	✓	×	✓	✓
CDA (2005)	✓	×	×	×
SDAP (2006)	✓	✓	✓	✓
SELDA (2007)	×	✓	✓	✓
SEDAN (2007)	×	✓	✓	✓
RSDA (2008)	×	✓	✓	✓
SEEDA (2010)	✓	×	✓	✓
EEHA (2011)	✓	×	✓	✓
IPHCDA (2011)	✓	✓	✓	✓
RCDA (2012)	✓	✓	✓	✓
CRSR (2013)	✓	×	✓	✓
PEPPDA (2013)	✓	×	✓	✓
EESSDA (2013)	✓	×	×	×
ECIPAP (2014)	✓	✓	✓	✓

C-Confidentiality, I-Integrity,

A-Authentication, F-Freshness

IV. CONCLUSION & FUTURE SCOPE

This paper provides brief description of various secure data aggregation protocols in wireless sensor networks. Additional with this, a comparison of various design issues of these secure data aggregation protocols is also given. By using this data, required secure data aggregation protocols for various wireless sensor network applications can be easily chosen.

REFERENCES

[1] Jose J., Jose J., and Jose F., "A Survey on Secure Data Aggregation Protocols in Wireless Sensor Networks", in International Journal of Computer Applications, Volume 55, no. 18, October 2012.
[2] Patil N. S., Patil P. R., "Data Aggregation in Wireless Sensor Network", in IEEE International Conference on Computational Intelligence and Computing Research, Tamilnadu College of Engineering Coimbatore, India,2010.
[3] Ozdemir S., Xio Y., "Secure Data Aggregation in Wireless Sensor Networks: A Comprehensive Overview", in Journal of Computer Networks, Elsevier, Volume 53, Issue 12, pp. 2022–2037, August 2009.
[4] Hu L., Evans D., "Secure Aggregation for Wireless Networks", in International Symposium on Applications and the Internet ,Orlando, Florida, USA, pp. 384-391, 27-31 January 2003.
[5] Przydatek B., Song D., Perrig A., "SIA: Secure Information Aggregation in Sensor Networks", in proceedings of the 1st International Conference on Embedded Networked Sensor Systems, Los Angeles, CA, USA, pp. 255-265, November 05 – 07, 2003.
[6] Cam H. et al. , "ESPDA: Energy-Efficient and Secure Pattern-Based Data Aggregation for Wireless Sensor Networks", in Computer Communications, Elsevier, Volume 29, Issue 4, pp. 446–455, February 2006.
[7] Mahimkar A., Rappaport T. S., "SecureDAV: A Secure Data Aggregation and Verification Protocol for Sensor Networks", in IEEE Conference on Global Telecommunications, Volume 4, pp. 2175-2179,29 Nov. – 3 Dec. 2004.
[8] OzgurSanli H., Ozdemir S., Cam H., "SRDA: Secure Reference-Based Data Aggregation Protocol for Wireless Sensor Networks", in IEEE 60th Conference on Vehicular Technology, VTC2004-Fall, Volume 7, pp. 4650–4654, 26-29 September 2004.
[9] Girao J., Schneider M., Westhoff D., "CDA: Concealed Data Aggregation in Wireless Sensor Networks", in IEEE International Conference on Communications, Volume 5, pp. 3044-3049, 16-20 May 2005.
[10] Yang Y. et al., "SDAP: A Secure Hop-by-Hop Data Aggregation Protocol for Sensor Networks", in Journal of ACM Transactions on Information and System Security (TISSEC), Volume 11, Issue 4,Article No. 18, New York, USA, July 2008.
[11] Ozdemir S., "Secure and Reliable Data Aggregation for Wireless Sensor Networks", in proceedings of 4th International Symposium, UCS 2007, Tokyo, Japan, pp. 102-109, 25-28 November 2007,.
[12] Bagaa M. et al., "SEDAN: Secure and Efficient Protocol for Data Aggregation in Wireless Sensor Networks", in proceedings of 32nd IEEE Conference on Local Computer Networks, pp. 1053-1060, 15-18 October 2007.
[13] Alzaid H., Foo E., Nieto J. G., "RSDA: Reputation-based Secure Data Aggregation in Wireless Sensor Networks", in proceedings of 9th IEEE International Conference on Parallel and Distributed Computing, Applications and Technology, pp. 419-424, 1-4 December 2008.
[14] Poornima. A. S., Amberker B. B., "SEEDA: Secure End-to-End Data Aggregation in Wireless Sensor Networks", in proceedings of 7th IEEE International Conference on Wireless and Optical Communications Networks (WOCN) , pp. 1-5, 6-8 September 2010.
[15] Li H., Lin K., Li K., "Energy-Efficient and High-Accuracy Secure Data Aggregation in Wireless Sensor Networks", in Journal of Computer Communications, Elsevier, Volume 34, Issue 4, pp. 591–597, 1 April 2011.
[16] Ozdemir S., Xiao Y., "Integrity Protecting Hierarchical Concealed Data Aggregation for Wireless Sensor Networks", in Journal of Computer Networks, Elsevier, Volume 55, Issue 8, pp. 1735–1746, June 2011.
[17] Chen C. M. et al., "RCDA: Recoverable Concealed Data Aggregation for Data Integrity in Wireless Sensor Networks", in IEEE Transactions on Parallel and Distributed Systems, Volume 23, Issue 4, pp. 727-734,August 2011.
[18] Lathamanju R., Senthilkumar P., "CRSR Algorithm: A Secure Data Aggregation Algorithm in WSN", in International Journal of Advanced Research in Electronics and Communication Engineering, Volume 2, Issue 9, September 2013.
[19] Jose J., Princy M., Jose J., "PEPPDA: Power Efficient Privacy Preserving Data Aggregation for Wireless Sensor Networks", in IEEE International Conference on Emerging Trends in Computing, Communication and Nanotechnology, pp. 330-336, 25-26 March 2013.
[20] Wang T., Qin X., Liu L., "An Energy-Efficient and Scalable Secure Data Aggregation for Wireless Sensor Networks" in International Journal of Distributed Sensor Networks, Hindawi Publications, Article ID 843485, Volume 2013(2013).
[21] Zhu L. et al. , "An Efficient Confidentiality and Integrity Preserving Aggregation Protocol in Wireless Sensor Networks", in International Journal of Distributed Sensor Networks, Hindawi Publications, Article ID 565480, Volume 2014(2014).