ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

A Survey on Secure Data Aggregation Techniques in Wireless Sensor Networks

N.Vidhya[1] Dr.P.Sengottuvelan[2]

[1]Research Scholar, Dept of Computer Science, Bharathiar University, Coimbatore, India

[2]Associate Professor, Dept of Computer Science, Periyar University PG Extension Center, Dharmapuri, India

ABSTRACT: Wireless Sensor Networks (WSN) consists huge number of sensor nodes usually set up in isolated and hostile area that are limited sensing, computation and communication capabilities. Due to resource limited sensor nodes, need to focus to decrease the amount of data communication. Data aggregation is the process in which information is gathered and expressed in a summary form in order to decrease the amount of data communication in the network. To improve energy efficiency of sensor network, Data aggregation protocols aim to merge and sum up data packets of several sensor nods and also classify and filter data from the compromised nodes. This paper retrieves about techniques available in data aggregation with security.

KEYWORDS: Data aggregation, security, energy efficiency, architecture, synopsis diffusion, attack resilient, cluster.

I. INTRODUCTION

The components of sensor node are microcontroller, transceiver, external memory, power source and one or more sensors. WSNs are thickly deployed sensor nodes in an application area for examination, care agriculture, smart homes, automation, vehicular traffic management, environment monitoring and disaster finding. Sensor nodes are limited in battery control, cost and memory and physical size. In WSN, research has been done in energy efficient hardware and protocol design, identifying alternate power sources, distributed detection techniques, multihop protocols, scheduling, layer optimization, node localization, security issues and data aggregation. Each sensor nodes is required to be capable of sensing, processing and communicating the processed data to the neighboring nodes to form a network. This paper spotlight the techniques used in Data aggregation. The main goal of Data aggregation is to join and aggregate data in an energy efficient style so that the lifetime of network is improved. Data aggregation is defined as the process of aggregation of data from the multiple sensors to eliminate unnecessary transmission and provide combined information to the base station. Base station send queries to the network, instead of sending each sensor nodes data to base station, one of the sensor nodes called data aggregator, collects the information from its neighboring nodes, aggregates them and sends the aggregated data to the base station over a multihop path.

II. LITERATURE REVIEW

Data aggregation can divide into two types 1) Reactive and 2) Proactive. Reactive protocols react to specific queries question by the node in the network. The answers are revisit to the issuer of query. Proactive protocols always provide the value of a number of aggregate to some or all nodes in the network, to follow reasonably quick changes in the network topology or in the value being aggregated. Data aggregation reduces the number of data transmissions, so that it improves the bandwidth and energy consumption in the network. On the other hand, data aggregation results in alterations in sensor data and it's challenging task to provide data authentication along with data aggregation. The problem like conflicts, The Data aggregation and security protocols must be designed to perform better data aggregation without sacrificing security. Both data aggregation and security are critical for wireless sensor networks. In existing secure data aggregation protocols,

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

data aggregators decrypt every message, aggregate the message and encrypt the aggregation result before forwarding it. While these data aggregation protocols protect data integrity and improve bandwidth and energy utilization of the network, also negatively affect other performance metrics like delay and data confidentiality. Recently, several protocols are proposed with resilient against attacks and confidentiality, integrity. In WSNs, a large amount of sensor nodes gather application specific information from the surroundings information is moved to a central base station. Gathered information are processed, analyzed, and used by the application in the Base Station. The main goal of data aggregation is to enlarge the network life span by reducing the resource utilization of sensor nodes. There are two types of data aggregation 1) Address Centric (AC), query is routed to a specific address or a given sensor based on the address specified in the query. 2) Data Centric(DC), based on the condition specified in the query, all sensors satisfying that condition need to reply and therefore the query is broadcast to all the nodes in the network.

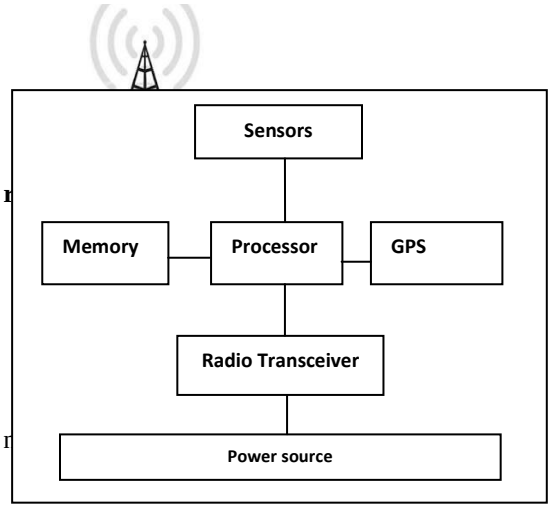

Fig. 1 - Components of WSN Node

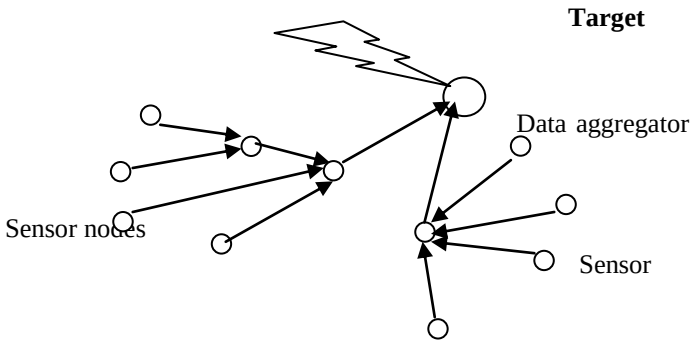

Fig. 2 - Data aggregation in Wireless Sensor Network

The design of an well-organized data aggregation protocol is a difficult task because the protocol must assures energy efficiency, data accuracy, latency, fault tolerance, and security. Several protocols are used to achieve data aggregation technique with how packets are routed in the network. So that the structural design of sensor networks play a vital role in the performance of special data aggregation protocol.

Table 1: Performance metrics of Data Aggregation

S.No	Metrics	Uses
1	Energy Efficiency	Its used for increase the efficiency of the network
2	Network lifetime	Increasing lifetime of network
3	Data Accuracy	It means correctness of data
4	Latency	Delay between data sending and receiving. Less delay.
5	Communication overhead	Complexity of the network and depends on the aggregation method.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

Data Aggregation Function

- Sum = $f(S_1,S_2,.....S_n) = \sum S_i$. $(i = 1,2....n)$
- Avg = $f(S_1,S_2,.....S_n) = \sum S_i / n.$ $(i = 1,2,...n)$
- Median = $f(S_1,S_2,.....S_n) = \sum S_r$. $(r = (n+1)/2)$
- Min = $f(S_1,S_2,.....S_n) = \min\{ S_i | i= 1.....n\}$
- Max= $f(S_1,S_2,.....S_n) = \max\{ S_i | i= 1.....n\}$
- count = $f(S_1,S_2,.....S_n) = |\{ S_i | i= 1.....n\}|$

III. SECURITY REQUIREMENTS OF WIRELESS SENSOR NETWORKS

Traditional network do not have security issues like WSN. So that the security is an important issue in WSN that should be investigate. Let us discuss important security issues in WSN and how these security issues are related with data aggregation process. Fig.3. Explain interaction between wireless sensor network security and data aggregation process [4].

3.1. Data confidentiality

Confidentiality is equivalent to privacy. Confidentiality is planned to prevent sensitive information from reaching the incorrect people, while making sure that the exact people can get it. Access must be controlled to those who are allowed to view the data in question. In WSN data confidentiality guarantee whether the information accumulated in a node is protected against illegal access. Confidentiality is often a measure of the ability of the system to protect its data. Sensor node should not leak its readings to neighboring nodes. Most of the time sensor node transmits highly sensitive data, therefore it is extremely important to build secure channel among sensor nodes. Routing of information must be confidential in certain cases as malicious nodes can use this information to degrade the networks performance. In data aggregation protocols usually cannot aggregate encrypted data. Such protocols decrypt and encrypt the aggregated data before broadcast to the nodes, it causes in delay and energy consumption bet prevent end to end data confidentiality.

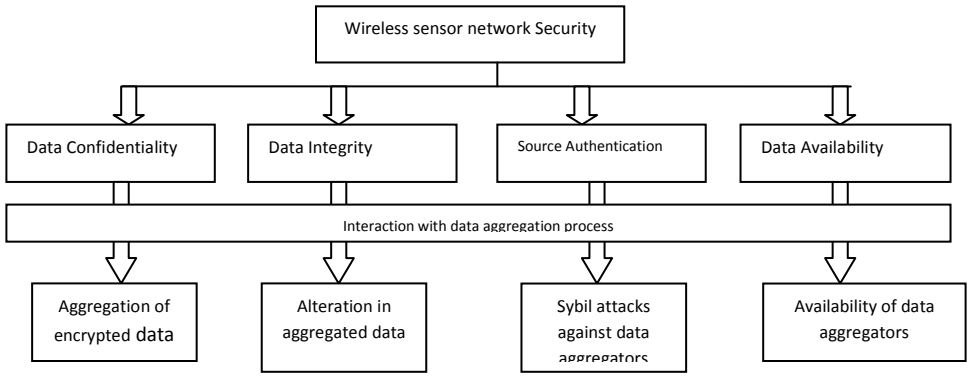

Fig. 3 - Interaction between data aggregation process and security requirement

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

3.2. Data integrity

Data integrity assured that a message being transferred is never corrupted. Integrity engage maintain the steadiness, truth and honesty of data in the entire network. Compromised node just alter messages to prevent network from functioning properly. Message authentication codes are used to avoid data integrity. Data aggregation results in alterations of data, so that it's not possible for end to end integrity. Providing data integrity is not enough for wireless communication because compromised nodes are capable to listening to transmitted messages and replay them later on to disrupt the data aggregation results.

3.3. Secure Authentication

Sensor needs authentication mechanisms to identify maliciously injected or spoofed packets. Secure authentication permits a sensor node to ensure the identity of the peer node. A compromised node may launch data to its data aggregator under several fake identities so that the honesty of the aggregated data is corrupted. Faking multiple sensor node identities is called Sybil attack and it poses significant threat to Data Aggregation Protocols. Sender and receiver share a secret key to calculate the message authentication code for all transmitted data. Data aggregators need relay authentication which requires more complex techniques.

3.4. Availability

Availability assures the survivability of network services against Denial-Of-Service (DOS) attacks. A DOS attack can launch at any layer of a wireless sensor network and may disable the injured party node permanently. For example, in a battlefield surveillance application, if the availability of some sensor nodes cannot be provided, this may lead an opponent to attack. WSNs are deployed with high node redundancy to tolerate such availability losses. Data aggregators collect the data of a number of sensor nodes and send the aggregated data to the base station. Availability of data aggregator is more important than regular sensor nodes. In WSN, intruder launches DOS attacks with the aim of preventing data aggregators from performing their task so that some part of the network losses its availability

IV. DATA AGGREGATION

The architecture of sensor network is classified into Flat and Hierarchical network. The approaches of Data aggregation are 1) Centralized Approach: only one sensor play a role of aggregator node and all other sensor nodes are connected to that aggregator node. 2) Decentralized approach: All sensor nodes perform aggregator function to the sensed data. All nodes have same priority to aggregate the sensed data. 3) In network Aggregation Approach: One or more node can be aggregator node i.e. means sub aggregator node. This approach aggregates multiple data into single data. It improve network lifetime and reduce size of transmitted data on the network.[2].

Flat Networks

In flat network, each sensor node have equal role and with equal battery power. In such network data aggregation is achieved by data centric routing where the sink usually sends a query message to the sensors via flooding and sensors which have data corresponding to the query send reply messages back to the sink. Data aggregation is performed by different nodes along the multi-hop path.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

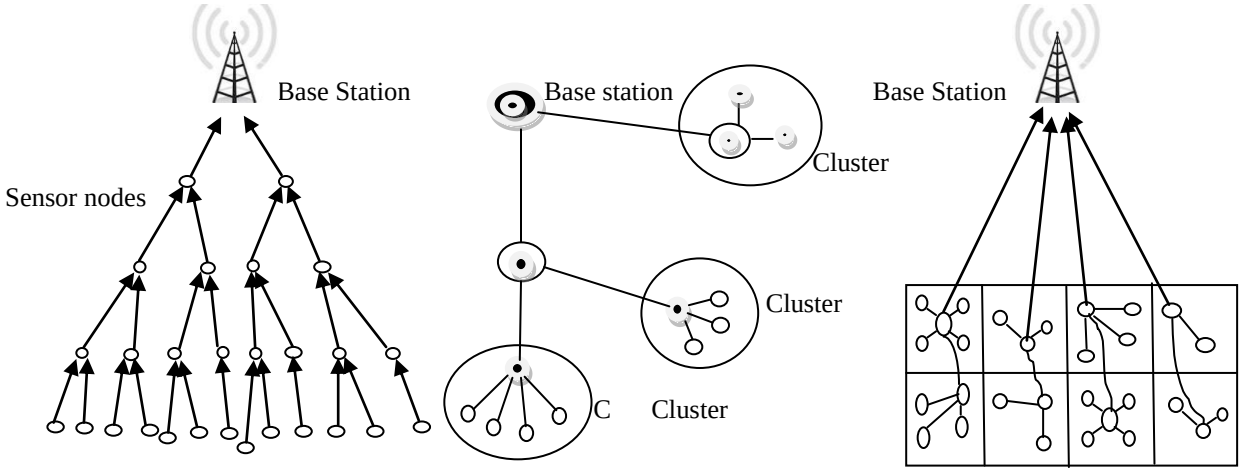

Fig 4. Tree based, Cluster based and Chain based Data Aggregation in Wireless sensor networks

Data aggregation routes are formed only in regions that have data for transmission. The failure of sink node may result in the break down of entire network. Higher latency is involved in data transmission to the sink via a multi hop path

SPIN (Sensor Protocols for Information via Negotiation)

SPIN is based on data-centric routing which has three types of messages. 1) ADV- When a node has data to send; it advertises this message containing meta-data. 2) REQ- A nodes send this message when it wishes to receive some data. 3) DATA – Data message contains the data with meta-data header. Advantages of SPIN is topological changes are localized so each node needs to know only its neighbors. Disadvantages of SPIN are not scalable and do not guarantee the delivery of data.

Directed diffusion

It is Data Centric routing. A node requests data by sending interests for named data. Query is transferred into an interest it broadcasted to neighbor nodes. When a node collects the interest, it initiates its sensors and reports the collected data. Intermediate nodes aggregate the data from several sensors. The feature of Directed Diffusion is interest and data and aggregation process are determined by localized interaction that is message exchange between neighbors or nodes.

Hierarchical Networks

Hierarchical networks involve data combination at unique nodes, which decrease the number of messages pass on to the sink. This advances the energy efficiency of the network. Data Aggregation executed by cluster heads or a leader node. Overhead involved in cluster or chain formation throughout the network. Sensor nodes succeed small range transmissions to the cluster head because of lower latency.

Tree based Approach

A tree based approach is based on the centralized approach. It consists a multi level hierarchy or tree on the underlying graph. Each node sends its state information to its parent that performs local aggregation and, in turn sends the aggregated

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

results upwards eventually reaching the root. The loss of a single node can interrupt the tree. A unit of the tree, [example node] aggregates required information received from its children in its sub tree and sends aggregation to its parent. All combined values will reach the top or the root which is responsible for network management and information processing. In case of a failure, a spanning tree can be built. The following keys Accuracy, Efficiency, Scalability, Robustness, Maintenance, Convergence time are addressed for the tree based aggregation protocols.

Cluster Based Approach

In cluster based data aggregation protocols, sensor nodes are subdivided into clusters. In each cluster, a cluster head is chosen in order to aggregate data locally and transmit the aggregation result to the base station. Cluster heads create a tree structure to transmit aggregated data by multihop through other cluster heads which results in significant energy savings.

Chain Based Approach

Chain Based Approach is the chain sensor among each node is attributed to a suppositional cell by location information of nodes. Suppositional cell take turn as cluster head for the data aggregation and transmit to a close neighbor. A node is designated the chain's head randomly and cluster head aggregate the data along with a chain cell and then transmit to the sink node. Gathered data moves from node to node and a designated node transmits to the BS or sink node. Data gathering, aggregation and transmission include two parts 1) Within a Suppositional Cell – there is a node who takes charge of data gathering and aggregation in the cell. The cluster leader within the cell also need receive data from cluster leaders in other cells, which are aggregated and transferred to cluster leaders in other cells or to sink node directly. 2) Between Suppositional cells or Sink node – collected data by the cluster head are transmitted to the sink node. This work takes turns to be completed by cluster heads between all cells

V.DATA AGGREGATION PROTOCOLS WITH SECURITY CONCERN

Data Aggregation Protocol must satisfy security requirements. Data aggregators must decrypt each message, aggregate the message according to the equivalent aggregation function and encrypt the aggregation result before forwarding it. Some security mechanisms are used to detect node misbehavior (dropping, modifying or forging messages, transmitting false aggregate value). Security needs of Data aggregation is Confidentiality of Data, Integrity of Data, Freshness of Data, Secure node localization, Source Authentication. The following protocols are discussed about data aggregation process in various approaches.

LEACH (Low Energy Adaptive Clustering Hierarchy) Protocol

Heinzelman et al. proposed an energy conserving cluster formation protocol called LEACH is the best example for cluster based approach. In LEACH [15], cluster heads act as data aggregation points. LEACH protocol is distributed and sensor nodes organize themselves into clusters for data fusion. The protocol consists of two phases. In first phase the setup state - cluster structures are formed. In second phase the steady state - cluster heads aggregate and transmit the data to the base station. Cluster head advertisements are broadcasted to sensor nodes and sensor nodes join the clusters based on the signal strength of the advertisement messages. A predetermined fraction of nodes f, elect themselves as the cluster head during the setup phase. All elected cluster heads broadcast a message to all the other sensors in the network informing that they are the new cluster heads. All non cluster head nodes which receive this advertisement decide which cluster they belong to based on the signal strength of the message received. LEACH employs randomization to rotate the cluster heads and achieves a factor of eight improvement compare to the direct approach in terms of energy consumption.

HEED (A Hybrid, Energy Efficient, Distributed Clustering Approach)

HEED is proposed by Younis et al. [7].The goal of HEED is,

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

1. Prolonging network lifetime by distributing energy consumption,
2. Terminating the clustering process within a constant number of iteration,
3. Minimizing control overhead and
4. Producing well distributed cluster heads.

The main theory in HEED is the availability of multiple power levels at sensor nodes. Cluster head selection is based on a combination of node remaining energy of each node and a secondary parameter which depends on the node closeness to its neighbors or node degree. The cost of a cluster head is defined by its Average Minimum Reach Ability Power (AMRP). AMRP [7] is the average of the minimum power levels required by all nodes within the cluster range to reach the cluster head.

Energy Efficient and Balanced Cluster-Based Data Aggregation Algorithm for wireless sensor Networks (EEBCDA)

It was proposed by Yuea et al [21]. The EEBCDA is also divided into rounds and every round consists of a setup phase and a steady state phase, also there is a network partition phase before the first round. The network is divided into rectangular regions firstly, called swim lanes, then each swim lane is further partitioned into smaller rectangular regions, called grids. Cluster Head (CH) is selected based on the node with the maximal residual energy of each grid. The grids are away from the BS are bigger and have more nodes to participate in CHs rotation. The network is divided into unequal size of rectangular grids and generates cluster head based on the energy level of sensor nodes and also rotate among the nodes in each grid respectively. The grid in which the cluster head consumes more energy can lead sensor nodes to the cluster head rotation and also share energy load.

Energy Efficient Unequal Clustering (EEUC)

It was proposed by Li et al in order to solve the problem of hot spots. The hot spot problem is linked to the early loss of CH nodes which are close to the BS. The CHs close to the BS have to pass on more loads in addition to the data of their own cluster. EEUC is a distributed CH competitive algorithm; the sensor nodes have the same initial energy. The tentative CHs are selected with the same probability with predefined threshold. The selection is primarily based on the residual energy of each node. Once the CHs are finalized, they start broadcasting. The nodes join to the CHs that are closest to them. CH will choose an adjacent node with less distance to the BS and more residual energy in order to extend the network lifetime and reduce wireless channel interference. The advantages are, EEUC tries to solve the hot spot problem by forming smaller clusters near the BS and also it introduces a method for relay node selection that reduces wireless channel interference.

Greedy aggregation

Intanagonwiwat et al. was proposed greedy aggregation scheme [18] based on tree based aggregation approach. This is novel approach that adjusts aggregation points to increase the amount of path sharing, reducing energy consumption. To construct a greedy incremental tree, a shortest path is established for only the first source to the sink whereas each of the other sources is incrementally connected at the closet point on the existing tree. In this approach, each tentative sample also contains energy for delivering this sample from the source to the current node. Also, each source of the existing tree generates an on-tree incremental cost message which corresponds to each new tentative sample received. This incremental const message is only sent and updated along the aggregation tree toward the sink. To find the closest point on the tree, the incremental energy cost field can be updated only by closer nodes. The greedy aggregation can achieve up to 45% energy saving in high density networks without unfavorably impacting latency.

Tiny AGgregation (TAG)

Madden et al. was proposed TAG, based on shortest path tree based aggregation in ad-hoc networks [19]. It is proposed for data collection and aggregation. Also it distributes and executes aggregation queries in the sensor network in a time and power efficient method. In TAG, user send a queries for data aggregation from a powered, storage-rich base station.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

Operators implement the query through the network and sensors route data back towards the user through a routing tree rooted at the base station. Advantages of TAGs are reducing communication bandwidth. It's designed for monitoring applications and allows an adjustable sleep schedule for sensor nodes. Parent node allows their children node about waiting time for transmission and parent node cache their children data to prevent from data loss.

Energy Aware Distributed Heuristic (EADAT)

Ding et al. was proposed an EADAT to construct and maintain a data aggregation tree in sensor networks [17]. The algorithm is initiated by the sink which broadcasts a control message. The sink acting the role of the root node in the aggregation tree. The control messages have five fields- Sensor ID, parent, residual power, status – leaf or non leaf and number of hop count from the sink. After getting control message for the first time, a sensor node set up its timer. The sensor node which has higher residual power and shorter path to the sink as marked as parent. This information is known to nodes through the control message. When the timer times out, the node increases its hop count by one and broadcasts the control message. If a node receives a message indicating that its parent node other nodes are marks itself as a non leaf node. This process carry on until each node broadcasts once and aggregation result is send to the sink.

Power Efficient Data Gathering Protocol for Sensor Information Systems (PEGASIS).

Lindsey et al. was proposed an PEGASIS based on Chain based Data Aggregation approach. In PEGASIS [14], nodes are prearranged into a chain for data aggregation. The nodes can form a chain by make use of a greedy algorithm or the sink can decide the chain in a centralized manner. Greedy chain formation assumes that all nodes have global knowledge of the network. The outermost node from the sink initiates chain formation and at each step, the closest neighbor of a node is elected as its successor in the chain. In each data gathering round, a node receives data from one of its neighbor, fuses the data to its own and transmits the fused data to its other neighbor along the chain. Eventually the leader node transmits the aggregated data to the sink.

Chain Routing With Even Energy Consumption (CREEC)

Shin et al. was proposed CREEC, In Chain establishment[20], BS calculates the cumulative forwarding energy and sorts all nodes according to the decreasing order of cumulative forwarding energy and classifies them to three node levels. Level 1 node is assigned as two leaf node in the chain. A level 1 or level 2 node is given a chance to preoccupy a very short adjacent link. In next stage, generates a chain using the constrained Kruskal's algorithm. It picks up the shortest link and the selected link is added to the current working chain under construction one by one until no more selection is possible. In next level all non optimum greedy algorithm have a bad property to have long links at a few of last choices. CREEC updates chains in every super round and builds new chain to save energy at deleted nodes.

Synopsis Diffusion for Robust Aggregation

Nath et al. proposed Synopsis Diffusion, [6] that enables robust, highly accurate estimations of duplicate sensitive aggregates. This approach uses a ring topology based on multi-path routing schemes with duplicate insensitive in-network aggregation scheme. Its accurately compute aggregate (count, sum). Count – Number of nodes in the network. Sum – Number of information collected by the node in the network. The aggregate computation is defined by three functions on the synopsis.

- **Synopsis Generation** SG () - take a sensor reading and generates a synopsis representing that data.
- **Synopsis Fusion** SF () - takes two synopses and generates a new synopsis.
- **Synopsis Evaluation** SE () - translates a synopsis into the final answer.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

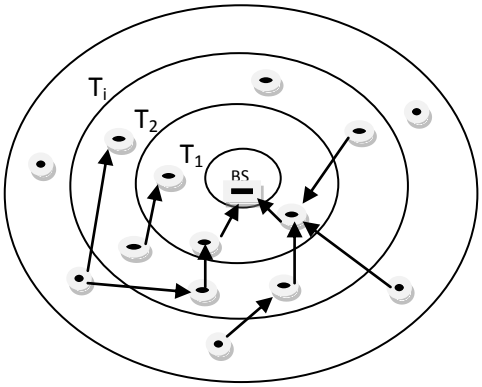

Fig 5: Synopsis Diffusion over a Ring Topology

Synopsis diffusion has two phases – 1) **distribution phase** in which the aggregate query is flooded through the network and an aggregation topology is constructed and 2) **aggregation phase** where the aggregate values are continually routed toward the querying node. Synopsis diffusion stay away from double-counting through the use of order- and duplicate-insensitive (ODI) synopses that compactly summarize intermediate results during in-network aggregation.

Attack Resilient Algorithm for Data Aggregation

Roy et al. was proposed Attack Resilient Algorithm [3] to filter attacks from compromised node. This algorithm identifies true values and filter data's from compromised nodes. It's has two phases - 1) In first phase the BS derives a beginning approximation of the aggregate based on minimal authentication information (MAC) received from the nodes. 2) In second phase, the BS request more confirmation information(MAC) from subset of nodes, this subset is determined by the estimate of the first phase. At the last part of the second phase, the BS can filter out the false contribution of the compromised nodes from the aggregate. Attack resilient algorithm assures the successful data aggregation even in the presence of attack. Still compromised node tries to attempt to inject false MAC in the first phase to inject false data in the aggregation process

VI. DISCUSSION

Data aggregation is process of collecting information from surrounding area based on the query arrives from base station and respond/send data to the base station. Wireless Sensor Network is a collection of nodes which are communicating each other also reply to the Base station. WSNs are applied in various areas but suffer problem like speed, security, complex to configure, affected by surrounding area. Many authors proposed various protocols and techniques to over come those problems but still WSNs experience more problems like survival in critical area, energy efficiency, security, etc. Some nodes in this network attacked by the hackers and it turn into compromised node. Compromised node attempts to inject false data in the network. These processes degrade the overall performance of the network. Data aggregation is efficient technique to increase network lifetime with energy efficiency. Security is one of the concerns in data aggregation process to corrupt the system. Studies show that to achieve efficient data aggregation in WSN, need to propose a protocol for data aggregation with energy efficiency and security. Protocol must recognize false data and compromised node and revoke that node. Protocol assures high level MAC to protect network from hackers.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

VII. CONCLUSION

This paper is studied about security requirements and data aggregation techniques in wireless sensor networks. In addition, it reviewed about tree based, cluster based and chain based approach for data aggregation and its protocols. Basically important requirement of WSN are excellent security with high energy efficiency. Previous research authors proposed excellent data aggregation protocol with security in different network architecture and also achieved energy efficiency. These protocols are very efficient in static networks in which the structure of network will not change. Still security, communication overhead and energy efficiency are important issues in data aggregation. False data are inserted in data aggregation process by the compromised nodes and it's tough to detect. Also the compromised node uniformly distributed in the network leads communication overhead. Hence the development of light burden observing mechanisms for secure data aggregation process is an interesting problem for future research.

REFERENCES

[1] Ankit Tripathi, Sanjeev Gupta, Bharti Chourasiya, "Survey on Data Aggregation Techniques for Wireless Sensor Networks" in International Journal of Advanced Research in Computer and Communication Engineering Vol 2, July 2014.
[2] Jyoti Rajput, Naveen Garg, " A Survey on Secure Data Aggregation in Wireless Sensor Network" in International Jouranl of Advance Research in Computer Science and Software Engineering – Vol 4,Issue 5, May 2014.
[3] Sankardas Roy, Sanjeev Setia, Susil Jojodia, " Attack Resilient Hierarchical Data Aggregation in Sensor Network" in ACM – SASN'06, October 30,2006.
[4] Suat Ozdemir, Yang Xiao, "Secure data aggregation in wireless sensor networks: A comprehensive overview "in Elsevier Computer Networks (2009) 2022-2037.
[5] Sankardas Roy, Sanjeev Setia, Sushil Jajodia, "Secure Data Aggregation in Wireless Sensor Networks: Filtering out the Attackers Impact" in IEEE transaction on Information Forensics And Security, Vol 9, No 4, April 2014
[6] Suman Nath, B.Gibbons, Srinivasan Sesan, R.Anderson, "Synopsis Diffusion for Robust Aggregation in Sensor Networks" in ACM –SenSys '04, November 3-5, 2004.
[7] Ossama Younis, Sonia Fahmy, "HEED: A Hybrid, Energy Efficient, Distributed Clustering Approach for Ad Hoc Sensor Networks" in IEEE Transactions Vol. 3 No. 4, 2004.
[8] Jia Guo, Jian'an Fang, Xuem in Chen, "Survey on Secure Data Aggregation for Wireless Sensor Networks" 978-1-4577-0574-8/11 IEEE
[9] Xiaoyan Wan and Jie Li, "Energy Efficient Secure Data Aggregation Framework in Wireless Network" 978-1-4244-5213-4/092009 IEEE
[10] Suat Ozdemir, Yang Xiao, "Integrity protecting hierarchical concealed data aggregation for wireless Sensor networks" in Elsevier Computer Networks 55 (2011) 1735 – 1746.
[11] Santar Pal Singh and S.C.Sharma, "A Survey on Cluster Based Routing Protocols in Wireless Sensor Networks" in Elsevier / Procedia Computer Science 45 (2015) 687-695
[12] Honguan Li, Kai Lin, Keqiu Li, " Energy efficient and high accuracy secure data aggregation in wireless sensor networks" in Elsevier Computer Communication 34 (2011) 591-597
[13] Rajagopalan, Ramesh and Varshney, Pramod K, "Data aggregation techniques in sensor networks: A survey" (2006). Electrical Engineering and Computer Science. Paper 22.
[14] Stephanie Lmdsey and Cauligi S. Ragavendra "PEGASIS: Power-Efficient Gathering in Sensor Information Systems" in IEEE - 2002
[15] Wendi Rabiner Heinzelman, Anantha Chandrakasan and Hari Balakrishnan, "Energy Efficinet Communication Protocol for Wireless Microsnsor Networks" in Proceedings fo 33rd Hawaii International Conference On System Science – 2000.
[16] Mukesh Kumar Jha, T.P.Sharma, "A New Approach to Secure Data Aggregation Protocol for Wireless Sensor Network" in International Journal on Computer Science and Engineering Vol. 2, No.5, 2010.
[17] Ding.M, Xiusen Cheng, Guoliang X, "Aggregation tree construction in Sensor Networks" in IEEE 2003
[18] C.Intanagonwiwiat, Deborah Estrin, Ramesh Govindan, J.Heidemann, "Impact of network density on data aggregation in wireless sensor networks" in IEEE 2002.
[19] Samuel Madden, Michal J.Franklin and Joseph M.Hellerstein, Wei Hong, "TAG: a Tiny Aggregation Service for Ad-Hoc Sensor Networks ", in ACM 2002.
[20] Jisoo Shin and Changjin Suh, "CREEC: Chain Routing with Even Energy Consumption," in IEEE Communications and Networks, 2011, pp.17-25.
[21] Jun Yuea, Weiming Zhang, Weidong Xiao, Daquan Tang, Jiuyang Tang, " Energy Efficient and Balance Cluster – Based Data Aggregation Algorithm for Wireless Sensor Networks " in Elsevier Procedia Engineering" in Elsevier Ltd 1877-7058 – 2011

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

BIOGRAPHY

N.Vidhya is working as Asst Professor in Thanthai Hans Roever College, Perambalur and Research Scholar in Bharathiar University, Coimbatore. She has completed MCA in Bharathiar University, Coimbatore and ME in Computer Science and Engineering in Anna University, Trichy. She is currently doing research in Wireless Sensor Network and published research paper in international journals.

Dr.P. Sengottuvelan is working as Associate Professor, Dept of Computer Science, Periyar University PG Extension Center, Dharmapuri. He is Research Advisor in Bharthiar University. After He did M.Sc in Computer Technology, He got ME computer science and Engineering. He has more than 15 years Research experience. He has published research papers in international and national journals and international and national conference.