Journal of Electronic and Electrical Engineering
ISSN: 0976–8106 & E-ISSN: 0976–8114, Vol. 1, Issue 2, 2010, pp-01-08

A review on data aggregation techniques in wireless sensor network

Vaibhav Pandey, Amarjeet Kaur and Narottam Chand
Department of Computer Science & Engineering, National Institute of Technology, Hamirpur, HP, India
v20pandey@gmail.com, mail4amarjeet@gmail.com, nar@nitham.ac.in

Abstract- Wireless sensor networks (WSNs) consist of many sensor nodes. These networks have huge application in habitat monitoring, disaster management, security and military, etc. Wireless sensor nodes are very small in size and have limited processing capability with very low battery power. This restriction of low battery power makes the sensor network prone to failure. Data aggregation may be effective technique in this context because it reduces the number of packets to be sent to sink by aggregating the similar packets. In this paper we put our attention into various data aggregation algorithms in wireless sensor network. Data aggregation technique increases the lifetime of sensor network by decreasing the number of packets to be sent to sink or base station. Here, we first explore the data aggregation algorithms on the basis of network topology, then we explore various trade offs in data aggregation algorithms and finally we highlight security issues in data aggregation.

I. INTRODUCTION

Wireless sensor networks (WSNs) consist of several sensor nodes and one or more base station (BS) or sink. Sensor nodes have limited processing capability and low power battery. It has also a sensing element and a transceiver. Sensor nodes sense the physical environment and send the data in the form of signals to the base station. The sensor nodes are usually scattered in a sensor field as shown in Figure1. Each of these scattered sensor nodes has the capabilities to collect data and route data back to the sink. Data are routed back to the sink by a multihop infrastructure less architecture through the sink as shown in Figure 1. While sending the data by its transceiver some amount of energy is consumed. Sensor nodes have less amount of energy so energy conservation is the important factor in sensor network. Data aggregation is the good technique to save the precious energy of sensor nodes. Usually in a sensor network thousand of sensor nodes are deployed for area monitoring. Most of them sense the environment and send the data to the base station and at base station and we have to combine all the information for the desired output. If we aggregate the data before reaching the base station we can potentially decrease the number of packets in the network so we will have to send less number of packets to base station and that can save the energy of sensor nodes. These types of data aggregation are called In-Network data aggregation where packets are combined before reaching the base station. We can define the data aggregation as follows, Data aggregation techniques explore how the data is to be routed in the network as well as the processing method that are applied on the packets received by a Node. They have a great impact on the energy consumption of nodes and thus on Network efficiency by reducing number of transmission or length of packet. Elena Fosolo *et al.* in [1] defines the in-network aggregation process as follows: "In-network aggregation is the global process of gathering and routing information through a multi-hop network, processing data at intermediate nodes with the objective of reducing resource consumption (in particular energy), thereby increasing network lifetime."

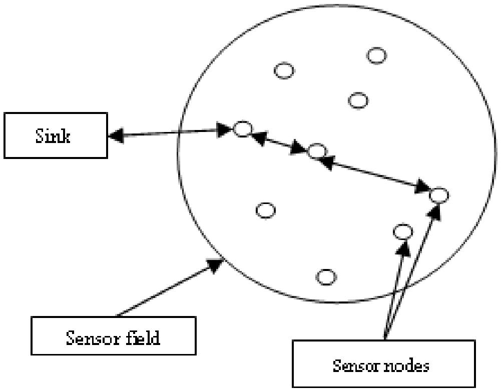


Fig. 1-Sensor network

II. DATA-AGGREGATION TECHNIQUES IN WIRELESS SENSOR NETWORKS

Data gathering is defined as the systematic collection of sensed data from multiple sensors to be eventually transmitted to the base station for processing. Since sensor nodes are energy constrained, it is inefficient for all the sensors to transmit the data directly to the base station. Data generated from neighboring sensors is often redundant and highly correlated. In addition, the amount of data generated in large sensor networks is usually enormous for the base station to process. Hence, we need methods for combining data into high-quality information at the sensors or intermediate nodes which can reduce the number of packets transmitted to the base station resulting in conservation of energy and bandwidth. This can be accomplished by data aggregation. Data aggregation is defined as the process of aggregating the data from multiple sensors to eliminate redundant transmission and provide fused information to the base station [2]. Data aggregation usually involves the fusion of data from multiple sensors at intermediate nodes and transmission of the aggregated data to the base station (sink) so we can conclude that data gathering is to collect the data from neighbor node to be sent to sink and data aggregation is process of removing redundancy among them. Data aggregation can be categorized on the basis of network topology, network flow, quality of services and many more. In this paper we have put our attention on network topology based data aggregation technique as shown in figure 2. We can divide the data aggregation technique into parts: structure based and structure free. Structure based data aggregation can be further divided into four parts flat network based, cluster based, tree based and grid based.

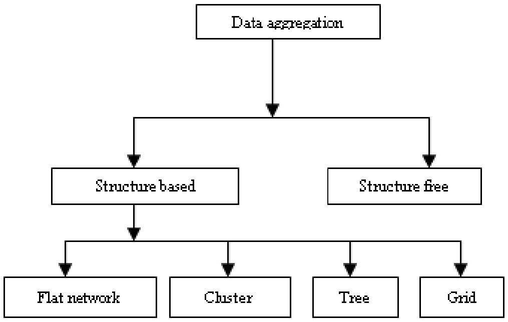


Fig. 2- Taxonomy of Data Aggregation

A. Data Aggregation In Flat Networks

In flat networks, each sensor node plays the same role and is equipped with approximately the same battery power. In such networks, data aggregation is accomplished by data centric routing where the sink usually transmits a query message to the sensors, for example, via flooding and sensors which have data matching the query send response messages back to the sink. The choice of a particular communication protocol depends on the specific application at hand. In the rest of this subsection we describe these protocols and highlight their advantages and limitations.

a. Flooding and Gossiping

Flooding and gossiping [31] are two classical mechanisms to relay data in sensor networks without the need for any routing algorithms and topology maintenance. In flooding, each sensor receiving a data packet broadcasts it to all of its neighbors and this process continues until the packet arrives at the destination or the maximum number of hops for the packet is reached. On the other hand, gossiping is a slightly enhanced version of flooding where the receiving node sends the packet to a randomly selected neighbor, which picks another random neighbor to forward the packet to and so on.

b. Directed diffusion

Directed diffusion (DD) [4] is a popular data aggregation paradigm for wireless sensor networks. It is a data-centric and application-aware paradigm, in the sense that all data generated by sensor nodes is named by attribute-value pairs. Such a scheme combines the data coming from different sources enroute to the sink by eliminating redundancy and minimizing the number of transmissions. In this way, it saves the energy consumption and increases the network lifetime of WSNs. In directed diffusion, the base station requests data by broadcasting interests, which describes a required task to be implemented by the network. The interest is defined using a list of attribute-value pairs such as name of objects, interval, duration and geographical area. Each node receiving the interest can cache it for later use. As the interest is broadcasted through the network hop-by-hop, gradients are setup to draw data satisfying the query towards the requesting node. A gradient is a reply link to the neighbor from which the interest was received. It contains the information derived from the received interest's fields, such as the data rate, duration and expiration time. Each sensor that receives the interest sets up a gradient toward the sensor nodes from which it received the interest. This process continues until gradients are setup from the sources all the way back to the base station. In this way, several paths can be established, so that one of them is selected by reinforcement. The sink resends the original interest message through the selected path with a smaller interval, hence reinforcing the source node on that path to send data more frequently.

c. SPIN

SPIN [5] is among the early work to pursue data centric routing mechanism. The idea behind SPIN is to name the data using high-level descriptors or meta-data. Before transmission, metadata are exchanged among sensors via a data advertisement mechanism, which is the key feature of SPIN. Each node upon receiving new data, advertises it to its neighbors and interested neighbors, i.e. those who do not have the data, retrieve the data by sending a request message. SPIN's meta-data negotiation solves the classic problems of flooding such as redundant information passing, overlapping of sensing areas and resource blindness thus, achieving a lot of energy efficiency. There is no standard meta-data format and it is assumed to be application specific, e.g. using an application level framing. There are three messages defined in SPIN to exchange data between nodes. These are: ADV message to allow a sensor to advertise a particular meta-data, REQ message to request the specific data and DATA message that carry the actual data.

d. Rumor routing

Rumor routing [6] is another variation of Directed Diffusion and is mainly intended for contexts in which geographic routing criteria are not applicable. Generally Directed Diffusion floods the query to the entire network when there is no geographic criterion to diffuse tasks. However, in some cases there is only a little amount of data requested from the nodes and thus the use of flooding is unnecessary. An alternative approach is to flood the events if number of events is small and number of queries is large. Rumor routing is between event flooding and query flooding. The idea is to route the queries to the nodes that have observed a particular event rather than flooding the entire network to retrieve information about the occurring events. In order to flood events through the network, the rumor routing algorithm employs long-lived packets, called agents. When a node detects an event, it adds such event to its local table and generates an agent. Agents travel the network in order to propagate information about local events to distant nodes. When a node generates a query for an event, the nodes that know the route, can respond to the query by referring its event table. Hence, the cost of flooding the whole network is avoided. Rumor routing maintains only one path between source and destination as opposed to Directed Diffusion where data can be sent through multiple paths at low rates.

e. Gradient-Based Routing

Gradient-Based Routing [7] is another version of directed diffusion, which aims to distribute traffic evenly throughout the network in order to increase the network lifetime. The key idea is to memorize the number of hops when the interest is diffused through the whole network. As such, each node can calculate a parameter called the height of the node, which is the minimum number of hops required to reach the base station. The difference between a node’s height and that of its neighbor is considered the gradient on that link. A packet is forwarded on a link with the largest gradient.

B. Data aggregation in Hierarchical Networks

A flat network can result in excessive communication and computation burdens at the sink node, resulting in a faster depletion of its battery power [2]. The death of the sink node breaks down the functionality of the network. Hence, in view of scalability and energy efficiency, several hierarchical data-aggregation approaches have been proposed. Hierarchical data aggregation [2] involves data fusion at special nodes, which reduces the number of messages transmitted to the sink. This improves the energy efficiency of the net work. In the rest of this subsection we describe the different hierarchical data-aggregation protocols and highlight their main advantages and limitations.

C. Data Aggregation in Cluster-Based Network

In energy-constrained sensor networks of large size, it is inefficient for sensors to transmit the data directly to the sink. In such scenarios, sensors can transmit data to a local aggregator or cluster head which aggregates data from all the sensors in its cluster and transmits the concise digest to the sink. This results in significant energy savings for the energy-constrained sensors. Figure 3 shows a cluster-based sensor network organization. The cluster heads can communicate with the sink directly via long range transmissions or multihoping through other cluster heads. Recently, several cluster-based network organization and data-aggregation protocols have been proposed. In this section we discuss various clustering protocols.

a. LEACH

LEACH [8] protocol is the first clustering protocol. It provides a conception of round. LEACH protocol runs with many rounds. Each round contains two states: cluster setup state and steady state. In cluster setup state, it forms cluster in self-adaptive mode; in steady state, it transfers data. The time of second state is usually longer than the time of first state for saving the protocol payload.

b. E-LEACH

Fan el. Al. [9] proposes a new protocol Energy-Leach which improves the CH selection procedure. Like LEACH protocol, E-LEACH protocol also devided into rounds, in the first round, every node has the same probability to turn into CH, that mean nodes are randomly selected as CHs, in the next rounds, the residual energy of each node is different after one round communication and taken into account for the selection of the CHs. That mean nodes have more energy will become a CHs rather than nodes with less energy.

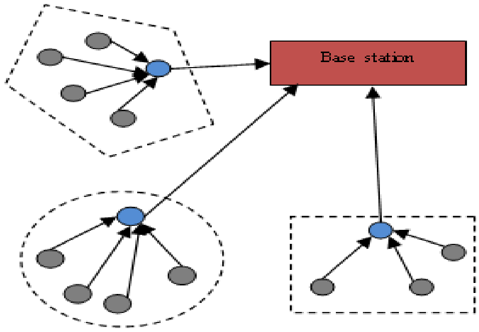


Fig. 3- Cluster **B**ased Data Aggregatiomn

c. TL-LEACH

In the LEACH protocol CH collects the information from cluster member nodes and after aggregation sends the information directly to the base station. CH might be located far away from the base station in that case it would be more energy consuming to send the information directly to the base station and CH will die quickly than other nodes. A new version of LEACH called Two-level Leach has been proposed in [10]. In this protocol; CH collects information from cluster member and in spite of sending it to directly base station it sends it to another CH that lie between the CH and BS as a relay station.

d. M-LEACH

In LEACH CH sends the aggregated information directly to the base station that is more energy consuming. In M-LEACH [11] multi-hop communication is selected among CH. Then, according to the selected optimal path, these CHs transmit data to the corresponding CH which is nearest to BS. Finally, this CH sends data to BS. M-LEACH protocol is almost the same as LEACH protocol, only makes communication mode from single hop to multi-hop between CHs and BS.

e. LEACH-C

Wendi *et al.* [12] proposed LEACH-C protocol which uses a centralized algorithm. LEACH-C protocol can produce better performance by dispersing the cluster heads throughout the network. During the set-up phase of LEACH-C, each node sends information about its current location (possibly determined using GPS) and residual energy level to the sink. In addition to determining good clusters, the sink needs to ensure that the energy load is evenly distributed among all the nodes. To do this, sink computes the average node energy, and determines which nodes have energy below this average. The steady-state phase of LEACH-C is identical to that of the LEACH protocol.

f. V-LEACH

In the LEACH protocol the CH is always on receiving data from cluster members, aggregates these data and then sends it to BS that might be far away from the BS. The CH may die earlier than other nodes because of receiving, sending and overhearing. When the CH dies cluster becomes useless because data sensed by sensor nodes will not be aggregated and also will not be sent to BS. In V-LEACH [13] protocol, besides having a CH in the cluster, there is a vice-CH that takes the role of the CH when the CH dies because the reasons we mentioned above. By doing this, cluster nodes data will always reach the BS; no need to elect a new CH each time the CH dies. This will extend the overall network life time.

D. Chain-Based Data Aggregation

In cluster-based sensor networks, sensors transmit data to the cluster head where data aggregation is performed. However, if the cluster head is far away from the sensors, they might expend excessive energy in communication. Further improvements in energy efficiency can be obtained if sensors transmit only to close neighbors. The key idea behind chain-based data aggregation is that each sensor transmits only to its closest neighbor. Lindsey *et al.* [14] presented a chain-based data-aggregation protocol called Power-Efficient Data Gathering Protocol for Sensor Information Systems (PEGASIS). In PEGASIS, nodes are organized into a linear chain for data aggregation. The nodes can form a chain by employing a greedy algorithm or the sink can determine the chain in a centralized manner. Greedy chain formation assumes that all nodes have global knowledge of the network. The farthest node from the sink initiates chain formation and, at each step, the closest neighbor of a node is selected as its successor in the chain. In each data-gathering round, a node receives data from one of its neighbors, fuses the data with its own, and transmits the fused data to its other neighbor along the chain. Eventually, the leader node which is similar to cluster head transmits the aggregated data to the sink. Figure 4 shows the chain-based data-aggregation procedure in PEGASIS. Nodes take turns in transmitting to the sink. The greedy chain formation approach used in may result in some nodes having relatively distant neighbors along the chain. This problem is alleviated by not allowing such nodes to become leaders.

E. Tree-Based Data Aggregation

In a tree-based network, sensor nodes are organized into a tree where data aggregation is performed at intermediate nodes along the tree and a concise representation of the data is transmitted to the root node as shown in the figure 5. Tree-based data aggregation is suitable for applications which involve in-network data aggregation. An example application is radiation-level monitoring in a nuclear plant where the maximum value provides the most useful information for the safety of the plant. One of the main aspects of tree-based networks is the construction of an energy efficient data-aggregation tree. Various tree data aggregation algorithms have been proposed in the literature. An Energy-Aware Data Aggregation Tree (EADAT) algorithm is proposed in [15]. The base station (root) sends a broadcast control message periodically. Upon receiving this message for the first time, each node will start a timer. The expiration time is inversely proportional to the node's residual energy. The timer is refreshed when a node receives this message during the timer count down

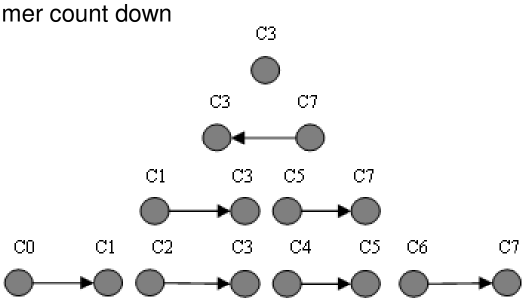
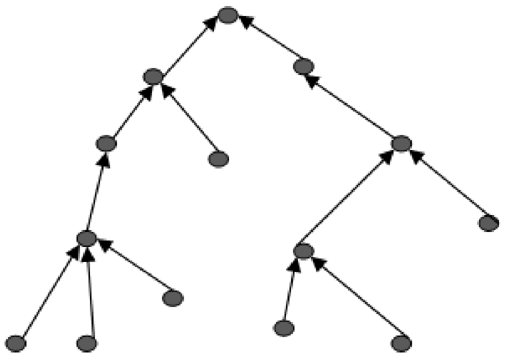


Fig. 4-Chain based data aggregation

E-Span, [16] is an energy-aware spanning tree algorithm. In E-span, the source node which has the highest residual energy is chosen as the root. Other source nodes choose their corresponding parent node among their neighbors based on the information of the residual energy and distance to the root. If there are multiple neighbors with equal distance, the node which has most remaining energy is selected as parent. As Espan protocol considers distance as main parameter and remaining energy as second, the network coverage is not high; because in some cases the nodes with low remaining energy are selected as parent. After local aggregation and data transmission, the remaining energy of these nodes is finished quickly. This causes the node failure and network cannot coverage region completely.



F. Grid-Based Data Aggregation

Vaidhyanathan *et al.* [18] have proposed two data-aggregation schemes which are based on dividing the region monitored by a sensor network into several grids. They are: grid-based data aggregation and In-network data aggregation. In grid-based data aggregation, a set of sensors is assigned as data aggregators in fixed regions of the sensor network. The sensors in a particular grid transmit the data directly to the data aggregator of that grid. Hence, the sensors within a grid do not communicate with each other. In-network aggregation is similar to grid-based data aggregation with two major differences, namely, each sensor within a grid communicates with its neighboring sensors. Any sensor node within a grid can assume the role of a data aggregator in terms of rounds until the last node dies.

III. STRUCTURE FREE DATA AGGREGATION

In structure free data aggregation we do not maintain any structure. This method is very useful in event based application where event region changes very frequently and if we use structure based approach then we have to maintain the structure again and again. In structure free environment because we do not maintain any structure we don't have to reconstruct the structure at the time of node failure or the changing of event region. There are two main challenges in performing structure free data aggregation. First, as there is no pre constructed structure, routing decisions for the efficient aggregation of packets need to be made on-the-fly. Second, as nodes do not explicitly know their upstream nodes, they cannot explicitly wait on data from any particular node before forwarding their own data. The benefit of this approach is that we don't have to maintain the structure all the time whereas in structured environment we have to reconstruct the structure at the time of when some nodes fail due to energy failure. The first work about the structure free data aggregation can be found in [19]. First, the authors observe that packets need to be aggregated early on their route to the sink for efficiency. Based on this observation, they propose and model a MAC layer protocol for spatial convergence called Data-Aware Anycast (DAA). Second, they observe that, if some nodes wait for other nodes to send data, it can lead to efficient aggregation. They study the impact of Randomized Waiting (RW) for improved data aggregation. In DAA a source node sends the RTS packet to all of its neighbors with RTS it also attach the type of data it has sensed. After receiving the RTS only those neighbor nodes send CTS packet that have same type of data. After receiving the CTS from more than one neighbor, source node selects only one of them according to instantaneous channel condition. DAA is based on MAC layer anycasting where we have the situation to select only one next hope among many. DAA improves the performance of data aggregation in comparison to structured approaches. If we use DAA with the RW it further improves the performance.

IV. HANDLING TRADE-OFFS IN DATA AGGREGATION

The performance of data-aggregation protocols are characterized by performance measures such as energy consumption, latency, and data accuracy. There is usually a trade-off between the different objectives. In this section we describe approaches for handling the trade-offs in data-aggregation schemes. Boulis *et al.* [20]

have studied the energy-accuracy trade-offs for periodic data-aggregation problems in sensor networks. They have considered a problem in which the sensors provide periodic estimates of the environment. A distributed estimation algorithm has been developed which uses the "max" aggregation function. Some of the unique features of the proposed estimation algorithm are scalability with the network architecture and time synchronization between the nodes is not required. All nodes have an estimate of the global aggregated value.

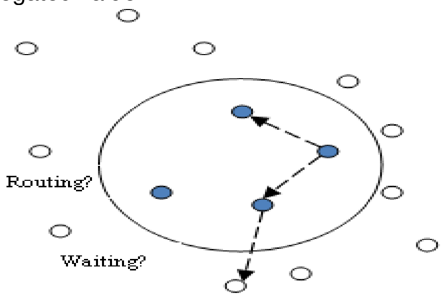


Fig. 6-Structure free data aggregation

The key idea of their approach is a threshold-based scheme where the sensors compare their fused estimates to a threshold to make a decision regarding transmission. However, in the absence of prior information about the physical environment, setting the threshold is a nontrivial task. The threshold can be used as a tuning parameter to characterize the tradeoff between accuracy and energy consumption. The main advantage of the proposed approach is that it does not depend on a hierarchical tree structure for performing data aggregation. Instead, every node has the global information about the aggregated data. The main disadvantage of the approach is that the functionality of the fusion algorithm depends on the aggregation function. Hence the fusion algorithm is not applicable for a wide range of aggregation functions such as "average," "count" or "min." Duarte-Melo *et al.* [21] have studied the transport capacity of data gathering sensor networks with different communication organizations. The hierarchical and flat organizations of sensor networks were compared in terms of capacity and energy consumption. They have discussed the trade-offs between capacity and energy consumption for data-aggregation applications in which every sensor sends an equal amount of original data to the sink. In the flat architecture, nodes communicate with the sink via multihop routes by using peer nodes as relays. In the hierarchical structure, nodes are organized into clusters where the cluster heads serve as simple relays for transmitting the data. For a hierarchical network, where cluster heads have the same transmission capacity as the sources, the minimum requirement on the number of clusters has been obtained for achieving the upper bound on the throughput. The main finding of their study is that higher throughput can be achieved by using clustering at the cost of the extra nodes functioning as cluster heads.

V. SECURITY ISSUES IN DATA AGGREGATION

In the data aggregation of WSN, two security requirements, confidentiality and integrity, should be fulfilled. Specifically, the fundamental security issue is data confidentiality, which protects the sensitive transmitted data from passive attacks, such as eavesdropping. Data confidentiality is especially vital in a hostile environment, where the wireless channel is vulnerable to eavesdropping. Though there are plenty of methods provided by cryptography, the complicated encryption and decryption operations, such as modular multiplications of large numbers in public key based cryptosystems, can use up the sensor's power quickly [22]. The other security issue is data integrity, which prevents the compromised source nodes or aggregator nodes from significantly altering the final aggregation value [23]. Sensor nodes are easy to be compromised because they lack expensive tampering-resistant hardware, and even that tampering-resistant hardware might not always be reliable. A compromised node can modify, forge or discard messages. Generally, two methods can be used for secure data aggregation in WSN: hop-by-hop encrypted data aggregation and end-to-end encrypted data aggregation. In the former, data is encrypted by the sensing nodes and decrypted by the aggregator nodes. The aggregator nodes then aggregate the data and encrypt the aggregation result again. At last the sink node gets the final encrypted aggregation result and decrypts it. In the latter, the intermediate aggregator nodes haven't decryption keys and can only do aggregations on the encrypted data. Girao *et al.* [24] have analyzed the two main practical issues involved in implementing data encryption at the sensors, namely, the size of the encrypted message and the execution time for encryption at the sensors. Privacy homeomorphisms (PHs) are encryption functions which allow a set of operations to be performed on encrypted data without the knowledge of decryption functions. In [24], a PH has been used to analyze the feasibility of security implementation in sensors. PHs use a positive integer d >2 for computing the secret key. The size of the encrypted data increases by a factor of d compared to the original data. Hence, in light of minimizing packet overhead, d should be chosen in the range between two and four, as suggested in [24]. Execution times for encryption operation at the sensors increase with d. For instance, when d = 2, the execution time for encryption of one byte of data is 3481 clock cycles on a MICA2 mote which increases to 4277 clock cycles when $d = 4$ as reported in [24]. MICA2 motes cannot handle the computation for $d > 4$. Hence, the trade-off between security and computation complexity should be considered when implementing data encryption schemes on sensors. Other main aspect of security in sensor networks is the establishment of secret keys between the sensor and the base station. Perrig *et al.* [25] have proposed security protocols for sensor networks which address the key establishment problem. In the approach proposed in [25], all nodes trust the base station at the network creation time and each node is given a master key which is shared with the base station. To achieve authentication between a sensor and base station, a message authentication code (MAC) is used. The keys for encrypting the data and computing the MAC are derived from the master key using a pseudo random function. All keys derived using this procedure, are computationally independent. Hence, if an attacker hacks the key, it would not help in determining the master key or any other key. In scenarios where a key is compromised, a new key can be derived without transmitting confidential information. Cam *et al.* [26] have developed an energy efficient and secure pattern-based data-aggregation protocol (ESPDA) for sensor networks. They have demonstrated the advantages of ESPDA compared to conventional data-aggregation techniques with respect to energy, bandwidth efficiency and security. In ESPDA, the sensor nodes send the pattern codes to the cluster head for data aggregation. The sensor data is transmitted to the sink in an encrypted form without being decrypted anywhere in the transmission path. ESPDA aims at achieving energy efficient data aggregation with secure data communication. Each sensor node executes the pattern generation (PG) algorithm to generate the pattern code. The cluster head uses a pattern comparison algorithm to analyze the patterns.

VI. CONCLUSION

We have presented a comprehensive survey of data-aggregation algorithms in wireless sensor networks. Here we first present the taxonomy of data aggregation based on network topology. Then we present the comprehensive study various data aggregation algorithm. All of them focus on optimizing important performance measures such as network lifetime, data latency, data accuracy, and energy consumption. Efficient organization, routing, and data-aggregation tree construction are the three main focus areas of data-aggregation algorithms. We have described the main features, the advantages and disadvantages of various data aggregation algorithm. Then we put emphasis on various trade offs in data aggregation algorithms and at the end we review security issues in data aggregation in WSN. Most of the existing work has mainly focused on the development of an efficient routing mechanism for data aggregation. However, the performance of the data-aggregation protocol is strongly coupled with the infrastructure of the network. There has not been significant research on exploring the impact of heterogeneity and mode of communication (single hop versus multihop) on the performance of the data-aggregation protocols. Although, many of the data-aggregation techniques discussed look promising, there is significant scope for future research. Combining aspects such as security, data latency, and system lifetime in the context of data aggregation is worth exploring.

REFERENCES

[1] Fasolo E., Rossi M., Widmer J. and Zorzi M. (2007) *IEEE Wireless communication.*

[2] Ramesh Rajagopalan and Pramod K. Varsney(2009) Journal IEEE Transactions on Wireless Communications, Volume 8 Issue 7, doi>10.1109/TWC.2009.060484.

[3] Hedetniemi S. and Liestman A. (1988) *Networks: An International Journal* Vol. 18 no. 4 pp. 319–349.

[4] Chalermek Intanagonwiwat, Ramesh Govindan, Deborah Estrin, John Heidemann, and Fabio Silva “Directed Diffusion for Wireless Sensor Networking”

[5] Heinzelman W., Kulik J., Balakrishnan H. (1999) *Proceedings of the 5th Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom_99)*, Seattle, WA, August 1999.

[6] Braginsky D., Estrin D. (2002) *Proceedings of the First Workshop on Sensor Networks and Applications (WSNA)*, Atlanta, GA.

[7] Schurgers C. and Srivastava M.B. (2001) *Energy Efficient Routing in Wireless Sensor Networks. In MILCOM Proceedings on Communications for Network-Centric Operations: Creating the Information Force, McLean, VA*.

[8] Wendi Rabiner Heinzelman, Anantha Chandrakasan, and Hari Balakrishnan (*2000*) *Energy-Efficient Communication Protocol forWireless Microsensor Networks” Proceedings of the 33rd Hawaii International Conference on System Sciences – 2000.*

[9] Fan Xiangning, Song Yulin (2007) *International Conference on Sensor Technologies and Applications.*

[10] Loscri V., Morabito G., Marano S. (2005) Vehicular Technology Conference, VTC-2005, Volume: 3,1809-1813.

[11] Yuhua Liu, Yongfeng Zhao, Jingju Gao, (2009) *International Joint Conference on Artificial Intelligence.*

[12] Wendi B. Heinzelman*,* Anantha P. Chandrakasan and Hari Balakrishnan (2002) *IEEE Transactions on Wireless Communications*, Vol. 1, No. 4.

[13] Bani Yassein M., Al-zou'bi A., Khamayseh Y., Mardini W. (2009) *JDCTA: International Journal of Digital Content Technology and its Applications*, Vol. 3, No. 2, pp. 132-136.

[14] Lindsey S., Raghavendra C. and Sivalingam K. M. (2002) *IEEE Trans. Parallel and Distributed Systems*, vol. 13, no. 9, 924–35.

[15] Min Ding, Xiuzhen Cheng, Guoliang Xue, (2006) *Proceeding Mobility '06 Proceedings of the 3rd international conference on Mobile technology, applications & systems, ISBN:1-59593-519-3, doi> 10.1145/ 1292331.1292391*

[16] Marc Lee, Vincent W.S. Wong (2006) *Computer Communications* 29(13-14): 2506-2520.

[17] Tan H. O. and Korpeoglu I. (2003) *SIGMOD Record*, vol. 32, no. 4, 66–71.

[18] Vaidhyanathan K. et al. (2004) *Technical Report, OSU-CISRC-11/04-TR60, Ohio State University*.

[19] Kai-Wei Fan, Sha Liu, and Prasun Sinha (2007) *IEEE Transaction On Mobile Computing*, 6, 8.

[20] Boulis A., Ganeriwal S. and Srivastava M. B. (2003) *1st IEEE Int'l. Wksp. Sensor Network Protocols and Applications, USA*.

[21] Duarte-Melo E. J. and Liu M. (2003) *Computer Networks: the Int'l. J. Computer and Telecommun. Net.,* 43, 4.

[22] Perrig A., Szewczyk R., Wen V., Cullar D., and Tygar J. D. (2001) *Proceedings of the 7th Annual ACM/IEEE Internation Conference on Mobile Computing and Networking (MobiCom)*, Rome, Italy, 189-199.

[23] Hu L. and Evans D. (2003) *Workshop on Security and Assurance in Ad hoc Networks*.

[24] Duarte-Melo E. J. and Liu M. (2003) *Computer Networks: the Int'l. J. Computer and Telecommun. Net.*, 43, 4.

[25] Girao J., Weshoff D. and Schneider M. (2005) *IEEE Int'l. Conf. Commun.*, 5, 3044–49.

[26] Przydatek B., Song D. and Perrig A. (2003) *Proc. ACM Conf. Embedded Networked Sensor Systems*.