SURVEY ON DISTRIBUTED DATA STORAGE SCHEMES IN WIRELESS SENSOR NETWORKS

Neenu M. Nair

PG Scholar, Department of CSE, KarunyaUniversity
Coimbatore, Tamil Nadu, India
neenumnair@gmail.com

J. Sebastian Terence

Assistant Professor, Department of CSE, KarunyaUniversity
Coimbatore, Tamil Nadu, India
jsebinfo@gmail.com

Abstract

The most important goal of Distributed Data Storage schemes in Wireless Sensor Networks is to efficiently distribute data across the WSN. Distributed data storage can play a vital role in improving data availability, security, energy efficiency and network lifetime of wireless sensor networks. Many researchers have been proposed various techniques to store data in a distributed manner. This paper describes a survey on distributed data storage schemes in Wireless Sensor Networks. We have classified these schemes into mainly two categories namely fully distributed data storage [FDDS] and data-centric storage [DCS]. Then, these schemes are further classified into four categories under the constraints topology, security, load-balancing and reliability. Advantages and disadvantages of each schemes also studied and we made the comparison of each schemes with different constraints.

***Keywords*:** Wireless sensor networks; Distributed data storage; Data availability; Security; Network lifetime; Energy efficiency.

1. Introduction

A wireless sensor network (WSN) consists of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. [Akyildiz *et al*. (2002)] A WSN typically has little or no infrastructure. It consists of a number of sensor nodes working together to monitor a region to obtain data about the environment. Today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on. In such applications one of the major challenge is where and how to store the sensed data [Yick *et al*. (2013)]**.** Data storage in WSNs mainly falls into two categories, namely centralized data storage and distributed data storage [Gonizzi *et al*. (2013)] Data availability, security, query processing and data retrieval, network lifetime, energy efficiency are the major challenges faced by data storage in wireless sensor networks.

In this paper, we discuss about various distributed data storage where information is stored on more than one node, often in a replicated fashion in wireless sensor networks shown in figure 1**.** There are two main approaches: data-centric storage and fully distributed data storage [Gonizzi *et al*. (2013)]**.**In a fully distributed data storage approach, all nodes contribute equally to sensing and storing. In data- centric storage approach some distinguished storage nodes are responsible for collecting data. Both the schemes make use of various techniques for distributed data storage. And each technique is characterized by different properties like topology, security, load-balancing and reliability.

The paper is organized as follows: Section 2 presents the challenges in data storage in wireless sensor networks. Section 3, 4 and 5 classifies the distributed data storage in wireless sensor networks and the advantages and disadvantages of each scheme are discussed. The conclusion of the paper is given in section 6.

2. Problem Statement

Data storage in WSNs mainly falls into two categories, namely centralized data storage and distributed data storage. In the former case, data are sensed, processed, aggregated and managed at a central location, usually a sink. In the latter case, after a sensor node has generated some data, the node stores the data locally or at some

designated nodes within the network, instead of immediately forwarding the data to a centralized location out of the network.

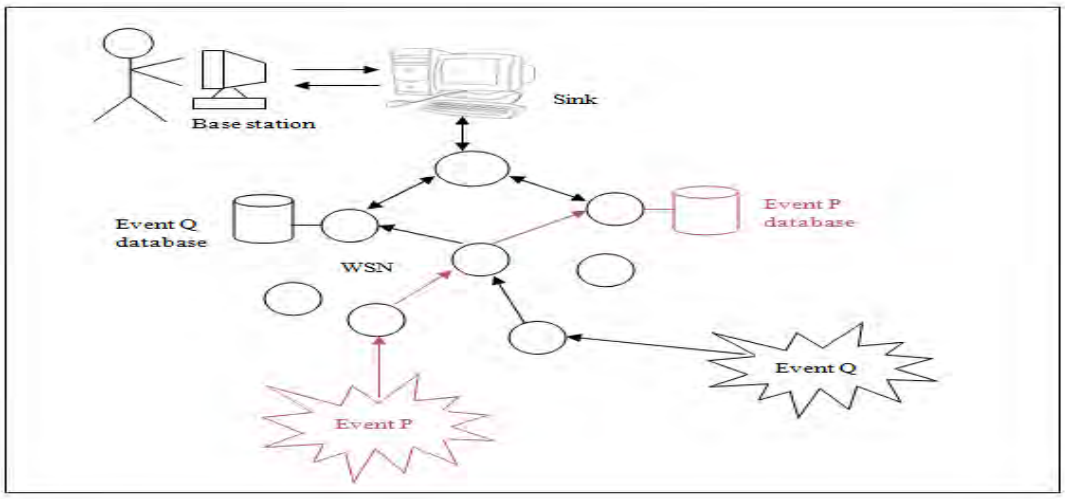

Fig. 1. Distributed Storage

Data availability, security, query processing and data retrieval, network lifetime, energy efficiency are the major challenges faced by data storage in wireless sensor networks. Since sensor nodes are more prone to failure, data loss will occur in WSNs. As a result of these data availability in WSN becomes very low. Use of data replication mechanisms will help to avoid such situations. Security of data stored either locally or externally is also an issue in WSN. It is easy for the attacker to access data from compromised nodes if WSN didn't support any security mechanisms. Adopting static sink node in distributed data storage for data retrieval will cause to reduce network life time, since static sink result in energy hole problem [Liu *et al.* (2010)], [Maia *et al.* (2013)], in which nodes closer to the sink typically consume more energy due to data relaying from other nodes in the network. Hence, disconnections may happen in the network.

3. Distributed Data Storage Schemes [DDS]

In WSN, a number of schemes are used for distributed data storage. The DDS can be mainly classified into fully distributed data storage [FDDS] and data-centric storage [DCS], which can be further classified in to topology based DDS, security based DDS, load-balancing based DDS and reliability based DDS. This classification is as shown in Fig. 2.

4. Fully Distributed Data Storage [FDDS]

In this approach, all nodes contribute equally to sensing and storing. All nodes try to store the sensor readings locally and, then, delegate other nodes in the WSN to store newly collected data as soon as their local memories are full. Fully distributed data storage can be categorized into mainly four classes as such as 1) Topology based FDDS, 2) Security based FDDS 3) Load- balancing based FDDS, and 4) Reliability based FDDS.

4.1. *Topology based FDDS*

In this approach data storage in wireless sensor networks are based on the topology of the network. Most commonly tree topologies are adopted. Mesh topology are also introduced in some special cases. Some examples are given as follows.

4.1.1. *ProFlex*

The main objective of ProFlex [Maia *et al.* (2013)] is to introduce distributed data storage for heterogeneous wireless sensor networks with mobile sink. It is a probabilistic and flexible data storage schemes. ProFlex constructs multiple data replication structures. When compare with related protocols, ProFlex has an acceptable performance under message loss scenarios, decreases the overhead of transmitted messages, and decreases the occurrence of the energy hole problem. The protocol is composed of three phases: tree construction, importance factor distribution and data distribution. Tree topology is responsible for making multiple replication structures. Advantages of ProFlex include 1.Reduced message loss, 2.Decrease the overhead of transmitted messages, 3.Decrease occurrence of energy hole problem and 4.Applicable to large scale WSN. Guarantee to security of data is the main disadvantage of ProFLex.

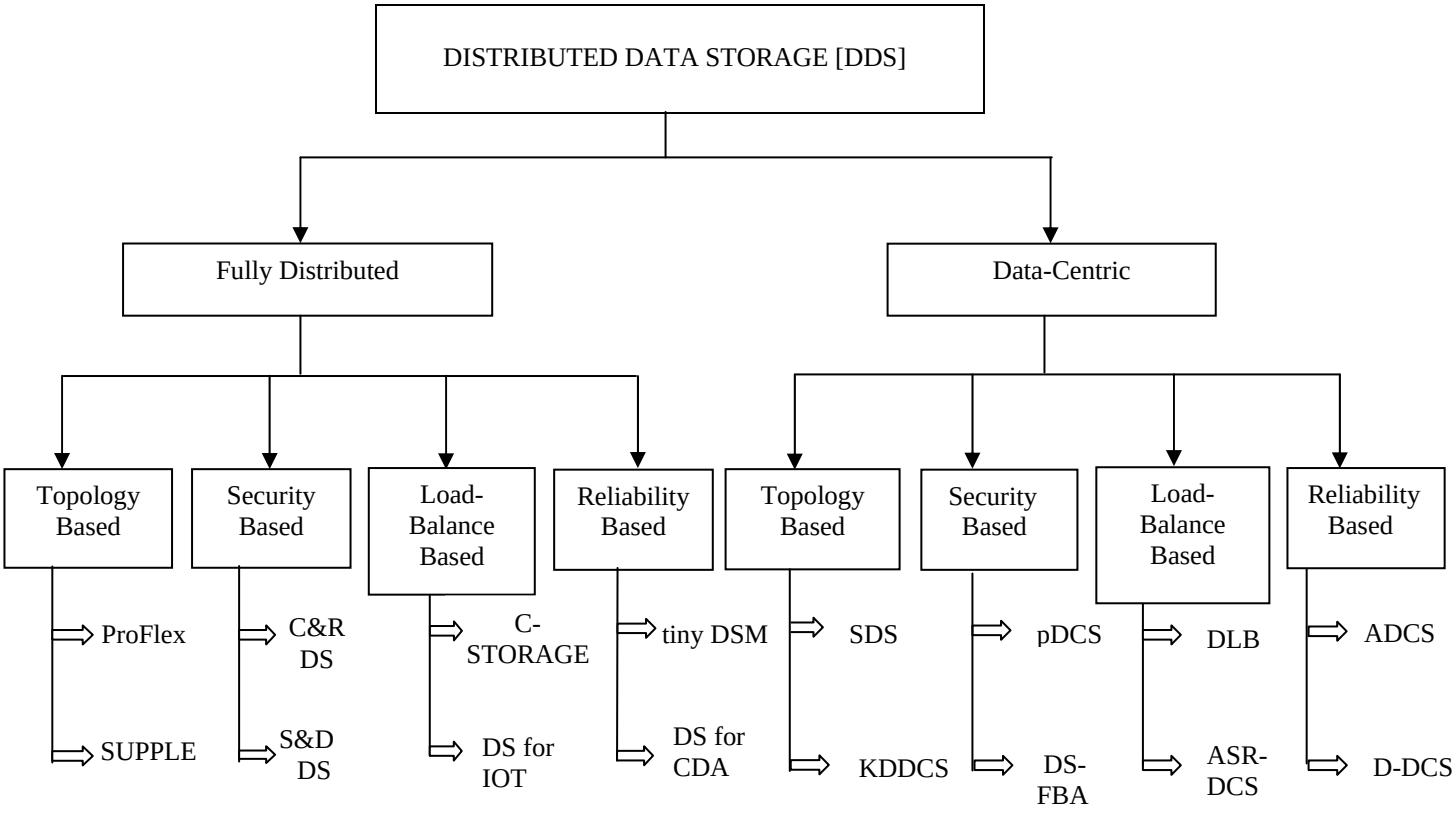

Fig. 2. Distributed data storage schemes in WSN

4.1.2. *SUPPLE*

A flexible probabilistic data dissemination protocol [Viana *et al*. (2010)] for WSNs that considers static or mobile sinks. The Supple protocol has three phases: tree construction, weight distribution, and data replication. This protocol was introduced to overcome the drawbacks of Deep [Vecchio et al. (2010)] and RaWMS [Bar-Yossef *et al.* (2008)] protocols. Apart from ProFLex SUPPLE uses single multiplication structure using tree topology. The first phase is a tree construction initiated by a central sensor node of the sensing area. The central sensor node is responsible for receiving and replicating the collected data in the network. The second phase assigns weights to nodes, which represent the probability of a node storing data. In the last phase, the sensor nodes send their data to the central node and this node replicates each data to particular number of times using the tree infrastructure and according to its storage probability. Advantages of supple include 1.Self organizing network, 2.Low communication overhead, and 3.Data availability. Disadvantages of supple are message overhead and high energy consumption.

4.2. *Security based FDDS*

Security based fully distributed data storage perform distributed data storage by considering security and privacy of data as the main constraint. Several research papers are there which focus on security while data storing. Some examples are given as follows.

4.2.1. *C&R-DS (Confidential and Reliable Data Storage)*

The objective of C&R-DS [Kusuma *et al.* (2013)] is to introduce a technique that prevents attackers from gain information from sensor collected data. To preserve confidentiality introduce some encryption mechanism, so that data at the storage node is not available to attacker. A Two-tiered sensor network consists of three types of nodes: sensors, storage nodes, and a sink. Sensors are inexpensive sensing devices with limited storage and computing power. They are often massively distributed in a field for collecting data. Storage nodes are powerful wireless devices that are equipped with much more storage capacity and computing power than sensors. Each sensor periodically sends collected data to its nearby storage node. Attackers are more motivated to compromise storage nodes thus algorithm to provide confidentiality and Algorithm to provide reliability are introduced for secure data storage. The advantages include 1.Confidentiality, 2.Reliability, 3.Splitting of data gives a) network band width b) network overhead c) increase efficiency and 4.Autherization.Disadvantages with C&R-DS are

1.Data loss, 2.Storage node failure, 3.Not fault tolerant, 4.Only applicable to small scale network and 5.Not energy efficient.

4.2.2. *S&D-DS (Secure, dependable and publicly verifiable distributed data storage)*

S&D-DS scheme can provide secure, dependable and publicly verifiable distributed data storage in UWSNs even in the presence of node compromise and Byzantine failure [Wei *et al.*, (2010)].These secure and dependable data distributed storage schemes make use of secret sharing and Reed-Solomon code. Such a scheme is resilient for random fault and node compromise, with communication and storage efficiency maintained. This paper present a generic technique called two granularity linear code (TGLC), which can verify distributed data's integrity publicly and efficiently, i.e., in a distributed manner and with low communication and storage overhead without original data. A family of schemes for secure and dependable data storage is Replication based scheme (RepS), Secret sharing based scheme (SSBS), Advanced hybrid scheme (HybridS). The advantages include 1.Confidentiality, 2.Integrity, 3.Availability, 4.Fault-tolerant and 5.Overcome byzantine failure. The main disadvantages of S&D-DS are 1.Storage Overhead 2.Communication overhead and 3.Computation overhead.

4.3. *Load-balancing based FDDS*

These schemes perform fully distributed data storage based on load-balancing using different approaches. Such schemes address the problem of low-memory capacity of sensor nodes in WSN. Some examples which provide load-balancing is given as follows.

4.3.1. *C-STORAGE (Distributed Data Storage Employing Compressive Sensing)*

The main objective of this paper is to introduce a novel and fully distributed data storage scheme referred to as CStorage for wireless sensor networks employing compressive sensing (CS) [Talari *et al.* (2011)] techniques. In CStorage, Ns nodes from N >> Ns total nodes disseminated their readings employing probabilistic broadcasting throughout the network; hence all nodes acquire a random compressed sample of data. Next, a data collector needs to collect only M << N measurements to restore all N data utilizing CS. An efficient and flexible data storage algorithm referred to as compressive sensing data storage (CStorage), which considerably reduces the number of required transmissions for distributed data storage in WSNs. The advantages include 1.Low transmission overhead and 2.Efficient query processing. The disadvantage with CS storage is no security of data introduced in case of compromising nodes which motivates the attacker.

4.3.2. DS for IOT

The main objective of this paper is to introduce a low complexity distributed data replication mechanism to increase the resilience and storage capacity of an IoT-based surveillance system [Gonizzi *et al.* (2013)] against node failure and local memory shortage due to increase in the load. In order to prevent data losses due to nodes' failures or memory shortages, nodes cooperate in the following way. A data acquired by a node is stored in several nodes. This consists copying and distributing replicas of the same data to other nodes with some available memory. Information about memory availability is periodically broadcasted, by each node, to all its neighbors. In order to create a replica of a stored data, a node selects, according to its neighbors' memory table, the ''best'' neighbor using a selection criterion. Greedy algorithm is used here for the distributed data storage. The advantages include 1.Low complexity, 2.Energy efficient. 3. Resilience against node failure and memory shortage. Disadvantages with this scheme are 1.Uncontrolled number of replicas lead to data loss.2.No data availability.

4.4. *Reliability based FDDS*

Reliability based fully distributed data storage concentrate on how we can achieve robustness in distributed storage, so that data availability can also be increased to an acceptable level. Some paper focusing on reliability is given as follows.

4.4.1. tinyDSM

tinyDSM [Piotroski *et al.* (2009)] is highly reliable data storage that assures data availability. It addresses the WSN resource problems and disappearing of nodes by providing a data redundancy in the system. The solution specifies the quantity and quality of the data replication. Ensuring fast and reliable access to the data stored in a WSN requires redundant data storage. In order to assure data availability in case of disappearing or sleeping nodes the data redundancy is needed. The quantity tells about the number of replicas of an event data that will not lead to overhead caused by their distribution and the problem of the replica consistency. Quality ensures whether changes in original data are also updated in all the replicas or not. The advantages include 1.Consistent and reliable data storage, 2.Easy query processing and 3.Data availability. Disadvantages with tinyDSM are 1.No security, and 2.No load balancing.

4.4.2. DS for CDA (Distributed storage schemes for controlling data availability)

This paper addresses the problem of introducing sufficient redundancy [Yulong *et al.* (2013)] with minimal communication cost to a network such that the entire network data can be retrieved after a failure. The high unreliability of sensor nodes decreases the data availability. The replica management systems can provide very high data availability in the distributed systems. This paper provides energy-efficient replica placement for increasing data availability and increase the network lifetime. This is achieved through the use of failure models. Using failure models and replica placement problem an optimal placement equation is generated and finally develop a heuristic algorithm, which adopts a greedy approach and provides near-optimal results under varying conditions. The advantages include 1.Not expensive, 2.Data availability, 3.Energy efficient replica placements, 4.Reliabilty and 5. Minimum communication cost. The high storage cost of such schemes make it impractical to use in real time applications is one of the main disadvantage.

5. Data Centric Storage [DCS]

In data-centric storage approach some distinguished storage nodes, e.g., determined by a hash function, are responsible for collecting a certain type of data. DCS can be categorized into mainly four classes as such as 1) Topology based DCS, 2) Security based DCS,3) Load- balancing based DCS, and 4) Reliability based DCS.

5.1. *Topology based DCS*

In topology based data-centric storage data storage in wireless sensor networks are based on the topology of the network. Most commonly tree topology is adopted.

5.1.1. *SDS (spatial-temporal Similarity Data Storage)*

Distributed SDS (spatial-temporal Similarity Data Storage) provides efficient spatial-temporal and similarity data searching service [Shen *et al.* (2011)] and is applicable for both static and dynamic WSNs. It distributes event data in such a way that the distance between WSN neighborhoods represents the similarity of data stored in them. It uses tree based data storage since the maintenance of the two-dimensional spatial-temporal storage space is difficult due to node mobility. This tree structure is efficient under both static and dynamic environments. Here the tree root is the head of the zone that is responsible for maintaining the tree structure. The second level consists of virtual nodes Virtual nodes are responsible for non overlapping spatial slices of the entire space interval. The virtual nodes are not real nodes and function to help keep the tree structure. Further, the leaves in the tree are real nodes that store data. For robust maintenance of the structure, constitute all nodes under one virtual node into a ring structure by adding a link between the first node and the last node. Advantages of SDS include 1.Load balancing, 2.Reduce overhead and 3.Fast data searching. Disadvantages with SDS are 1) High delay for construction of tress and event storage and 2) No security provided for data.

5.1.2. *KDDC (K-D trees based DCS)*

In KDDCS [Aly *et al.* (2006)] scheme, the refinement of regions in the formation of the K-D tree has the property that the numbers of sensors on both sides of the partition are approximately equal. As a result of this, the K-D tree will be balanced; there will be no orphan regions present. In KDDCS, the storage of events will be roughly uniform over the sensors. KDDCS avoids the formation of storage hot-spots arising in the sensor network due to irregular sensor deployment or irregular events distribution. The advantages include 1.Minimal overhead, 2.Data persistence, 3.Increase QoD and 4.Energy efficient. Disadvantages with KDDCS are 1.Delay in processing query, 2.No security and 3.Suitable to only small scale networks.

5.2. *Security based DCS*

In security based data-centric storage, giving more importance to security and privacy of data during storage and query processing, several paper are there to tell about how we can achieve security using different techniques. Some related papers are given as follows.

5.2.1. *pDCS (Security and Privacy Support for DCS)*

pDCS, a privacy-enhanced DCS network [Shao *et al.* (2013)] to address these security problems. pDCS is the first one to provide security and privacy to data-centric sensor networks. Here even if an attacker can compromise a sensor node and obtain all its keys, he cannot decrypt the data stored in the compromised node. pDCS system assumes that a sensor network is divided into cells where each pair of nodes in neighboring cells can communicate directly with each other. A cell head coordinates all the actions inside a cell. Here assume that in a pDCS network the goal of an attacker is to obtain the event data of his interest. To achieve this goal, an attacker may launch the following attacks. Passive Attack, Query Attack, Readout Attack, Mapping Attack. Readout attack and the mapping attack are more preferable to the attacker. The requirements to be met for addressing the readout attack and the mapping attack are Event Data, Backward Event Privacy, Forward Event

Privacy, and Query Efficiency. The advantages include 1.Security and privacy of data, 2.Confidentiality and 3.Efficient query processing. Disadvantages with pDC are 1. Less data availability and 2. Node can compromise to attacker.

5.2.2. DS-FBA (Data Storage Security against Frequency-based Attacks)

This paper tell about a data encryption strategy based on 1-to-n substitution via dividing and emulating techniques such that an attacker cannot derive the mapping relationship between the encrypted data and the original data based on their knowledge of domain values and their occurrence frequency. This method [Liu a *et al*. (2010)] used for solving frequency based attacks. If the attacker knows the exact frequency of some or all original data values and utilizes such knowledge to crack the data encryption by matching the encrypted data values with original data values based on their frequency distribution. Call this kind of attack as frequency-based attack. Frequency-based attacks are especially harmful in distributed data storage. The advantages include 1.Security with low overhead, 2.Low computational cost and 3.Confidentilality of data. More complexity is the main disadvantage with DS-FBA, since it is using 1-to-n encryption.

5.3. *Load-balancing based DCS*

These schemes perform data centric storage based on load-balancing using different approaches. Such schemes address the problem of low-memory capacity of sensor nodes in WSN thus data availability can be increased. Some examples which provide load-balancing is given as follows.

5.3.1. DLB (A Grid-based Dynamic Load-balancing Approach)

The objective here is to introduce a grid-based DLB [Liao *et al.* (2009)] approach that relies on two schemes: A cover-up scheme to deal with the problem of a storage node whose memory space is depleted and multi-threshold levels to achieve load balancing in each grid. DLB divides the whole network into a grid with cells of the same size in such a way that all the nodes inside a cell are within one hop distance. Each grid is numbered with positive coordinates (x, y) called grid IDs. A sensor node can calculate its grid ID with the help of some equations. Each node has a virtual grid ID and virtual co-ordinates that are initially equal to the actual grid ID and co-ordinates. Initially, each node broadcasts a message within its grid by limited broadcast to exchange the information to construct a Grid_Node table. A producer node uses the hash function on the event type to map the event type into a grid and transform the event type into a grid ID using the above equation. The center of the grid is called a grid point. The node, after detecting an event, sends a Put packet to the grid ID and uses GPSR to forward this packet to the node closest to the grid point. The advantages include 1.Avoid hot spot storage, 2.Load balancing, 3.QoD and 4.Energy efficient. The disadvantages with DLB are 1.No security and 2.Less data availability.

5.3.2. *ASR (An Adaptive Method for Structured Replication)*

The main objective is to bring load-balancing and scalability to the network as well as its ability to adapt itself to network conditions. SR-DCS achieves load balancing in storing events by adding different replicas of storage nodes, thereby bringing longer life span to sensor nodes. In order to improve query and storage costs and reduce the number of dead nodes, the author have made SR-DCS adaptive. ASR-DCS provides load-balancing in the network, reduces energy consumption in hotspot nodes and distributes communication traffic load when the event frequency is high. Two thresholds are defined for this method. If event frequency exceeds the first threshold, storage node will create the first level of hierarchy and event data are sent to first-level replicas. If event frequency also exceeds the second threshold, first-level replicas will act like the root node and will create the second level of hierarchy. Upon the return of the network to its normal state and the decline in the event frequency, replica nodes of each level will be merged into their immediate upper-level root node [Hejazi *et al.* (2011)] .The advantages of these schemes are 1.Load balancing, 2.Scalability and 3.Network lifetime increases. Disadvantages with ASR-DCS are 1.Hot spot storage problem and 2.No security.

5.4. *Reliability based DCS*

Reliability based data centric storage concentrate on how we can achieve robustness in distributed storage, so that data availability can also be increased to an acceptable level. Some paper focusing on reliability is given as follows.

5.4.1. *ADCS (Adaptive Data-Centric Storage)*

Adaptive data centric storage [Babaei *et al.* (2013)] offers a hybrid method which dynamically determines network conditions such as the rate of query and event production for each event type. Based on the network conditions, decision about where to store the event is done at the sink. This method can solve the hot-spot problem in the wireless sensor network in an effective way. ADCS uses a decision function to select an appropriate method for storing data i.e. either external storage or DCS for a certain event. The decision function

is used in every period to broadcast selected method to the whole network. Decision making about the way of storage is done in the sink and in a centralized manner. If ratio of rate of event production to query is equal or less than threshold then distributed method is used. If this ratio is greater than threshold, the centralized method is used. If the way of storage of that event is centralized, the sink itself responds, otherwise it sends the query to the relevant area. The advantages include 1. No hot spot storage problem, 2.Energy efficient and 3.Network life time increases. Disadvantages with ADCS include 1. Less data availability, 2.No data security and 3.Sink node failure will lead to appropriate decision making problems since sink is responsible for decision making.

Table 1. Comparison Of distributed data storage schemes in WSNs.

Main Classification	Sub classification	Title	Data Availability	Security	Energy efficient	Network lifetime
Fully Distributed Data Storage [FDDS]	Topology Based	ProFlex	Y	N	Y	Y
		SUPPLE	Y	N	N	Y
	Security Based	C&R- DS	N	Y	N	N
		S&D –DS	N	Y	Y	N
	Load-Balancing Based	C-STORAGE	N	N	Y	Y
		DS for IOT	Y	N	N	Y
	Reliability Based	TinyDSM	Y	N	N	N
		DS for CDA	Y	N	Y	Y
Data centric Storage [DCS]	Topology Based	SDS	N	N	Y	Y
		KDDCS	N	N	Y	N
	Security Based	Pdcs	N	Y	Y	N
		DS-FBA	N	Y	Y	Y
	Load-Balancing Based	DLB	N	N	Y	Y
		ASR	Y	N	Y	Y
	Reliability Based	ADCS	Y	N	N	Y
		D-DCS	Y	N	Y	N

5.4.2. *D-DCS (Dynamic Data-Centric Storage)*

Dynamic DCS [Cuevas *et al. (*2013)] brings distributed data storage by periodically change home nodes over the time based on periods of fixed duration called epochs. This makes it possible to perform temporal queries to previous home nodes in order to retrieve information from the past. Original DCS does not provide long-term storage for sensor events since it does not distribute the storage load among network nodes. For changing the home nodes, divide the time into periods of a fixed duration called epochs. During an epoch all events are stored in the selected home nodes. Therefore, a node will only overwrite old events after being chosen as a replica multiple times in several different epochs, thus extending sensor event availability. The advantages include

1.Long term storage system, 2.Easy access of historical data and 3.Energy efficient. Disadvantages with D-DCS are Hot spot storage problem, 2.High cost, 3.Wrong initialization of epochs leads to data loss.

6. Conclusion

In this paper we studied different distributed data storage schemes in wireless sensor networks and we classified these techniques into mainly two types namely fully distributed data storage (FDDS) and data centric storage (DCS). In FDDS all nodes contribute equally to sensing and storing while in DCS some distinguished storage nodes are responsible for collecting a certain data. In each of these classifications the techniques can be again classified into topology based, security based, load-balancing based and reliability based distributed data storage schemes. The topology based data storage performs distributed data storage based on the topology of the network and the security based data storage adopts some data storage schemes that support security features. The load-balanced based distributed data storage uses grid like architecture to achieve load balancing and we can achieve robustness in distributed storage through reliability based distributed data storage. Finally we made a comparison between various distributed data storage schemes (shown in Table 1) under various constraints like data availability, security, energy efficiency and network lifetime.

References

[1] An-Feng Liu, Wu Xian-You, Chen Zhi-Gang , Gui Wei-Hua (2010), "Research on the energy hole problem based on unequal cluster-radius for wireless sensor networks", Computer Communications 33 (3) 302–321.

[2] Ali Talari, Nazanin Rahnavard (2011), "CStorage: Distributed Data Storage in Wireless Sensor Networks Employing Compressive Sensing", IEEE Globecom 2011 proceedings.

[3] Angel Cuevas, Manuel Uruen, Gustavo de Veciana, Ruben Cueva (2013), "Dynamic Data-Centric Storage for long-term storage in Wireless Sensor and Actor Networks", Springer Science+Business Media New York 2013.

[4] C Viana, T.Herault, T.Largillier, S.Peyronnet, F.Zaı¨di (2010), "Supple: a flexible probabilistic data dissemination protocol for wireless sensor networks", 13th ACM International Conference on Modeling.

[5] Guilherme Maia, Daniel L. Guidoni a, Aline C. Viana b, Andre L.L. Aquino c, Raquel A.F (2013), "A distributed data storage protocol for heterogeneous wireless sensor networks with mobile sinks", Ad Hoc Networks 11 1588–1602.

[6] Haiying Shen, Lianyu Zha (2011), "A Distributed Spatial-Temporal Similarity Data Storage Scheme in Wireless Sensor Networks", IEEE Transaction on mobile computing, VOL. 10, NO. 7, JULY 2011.

[7] Hongbo Liu a, Hui Wang, Yingying Chen (2010), "Ensuring Data Storage Security against Frequency-based Attacks in Wireless Networks", In: Proceedings of the IEEE International Conference on Pervasive Computing and Communications.

[8] Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci (2002), "Wireless sensor networks: a survey", Computer Networks 38 (4) 393–422.

[9] J. Yick, B. Mukherjee, D. Ghosa (2008), "Wireless sensor network survey", Computer Networks 52 -2292–2330.

[10] Krzysztof Piotroski, Peter Langendoerfer and Steffen Peter IHP (2009), "tinyDSM: A Highly Reliable Cooperative Data Storage For Wireless Sensor Networks", 978-1-4244-4586-8/09/$25. 00 ©2009 IEEE.

[11] Kusuma K V, Prasad M R (2013), "Confidential and Reliable Data Storage in WSN", Volume 3, Issue 4, April 2013 ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Software Engineering.

[12] M. Vecchio, A.C. Viana, A. Ziviani, R. Friedman (2010), "Deep: density-based proactive data dissemination protocol for wireless sensor networks with uncontrolled sink mobility", Elsevier Computer Communication33 (8) (2010).

[13] Min Shao, Sencun Zhu, Wensheng Zhang, and Guohong Cao (2007), "pDCS: Security and Privacy Support for Data-Centric Sensor Networks", ACM International Workshop on Wireless Sensor Networks and Applications.

[14] Mohamed Aly, Kirk Pruhs, Panos K. Chrysanthis (2006), "KDDCS:A Load Balanced In Network DataCentric Storage Scheme for Sensor Networks" , *CIKM'06*, November 5–11, 2006, Arlington, Virginia, USA.

[15] Pietro Gonizzi , Gianluigi Ferrari , Vincent Gay b (2013), "Data dissemination scheme for distributed storage for IoT observation systems at large scale" Information Fusion xxx (2013) xxx–xxx.

[16] [Pooya Hejazi, Iran Hamed, Hassanzadeh Amin (2011), "An Adaptive Method for Structured Replication Data centric Storage in Wireless Sensor Networks", Proceedings of the 5th International Conference on IT & Multimedia.

[17] Ren Wei, Ren Yi and Zhang (2010), "Secure, dependable and publicly verifiable distributed data storage in unattended wireless sensor networks", Science China Information Sciences.

[18] Sepehr Babaei, Masoud Sabaei (2011), "Adaptive Data-Centric Storage in Wireless Sensor Networks", 978-1-61284-840-2/11/$26.00 ©2011 IEEE.

[19] Shen Yulong, Xi Ning, Pei Qingqi, Ma Jianfeng (2013), "Distributed storage schemes for controlling data availability in wireless sensor networks", Seventh International Conference on Computational Intelligence and Security.

[20] Wen-Hwa Liao , Kuei-PIng Shih , Wan-Chi Wuaa (2009), "A grid-based dynamic load balancing approach for data-centric storage in wireless sensor networks", Computers and Electrical Engineering 36 (2010) 19–30.

[21] Z. Bar-Yossef, R. Friedman, G. Kliot (2008), "RaWMS – random walk based lightweight membership service for wireless ad hoc networks", ACM Transactions on Computer Systems 26 (2008) 5:1–5:66.