Secure Aggregated Routing Protocol in WSN – A Review

Anuradha M P
School of Computer Science, Engineering and Applications
Bharathidasan University, Tiruchirapalli, TamilNadu
620 023, India.

Gopinath Ganapathy
School of Computer Science, Engineering and Applications
Bharathidasan University, Tiruchirapalli, TamilNadu
620 023, India.

ABSTRACT

Wireless sensor Networks (WSN) require secure aggregated routing of sensor data transmitted from source node to the sink node for most of its applications. Several existing routing protocols are explained in this paper with aggregation for WSN's are explored. The main objective of this paper provides the importance of secure aggregated routing algorithms for WSN to collect process and aggregate the data from sensors in an energetic conservative manner. Hence the network performance is enhanced. This paper scrutinizes the relationship between aggregation, routing and security issues in WSN. This survey covers a wide range of key issues in routing protocols based on its own evaluation metrics such as throughput, Packet delivery ratio, network lifetime, energy conservation, complexity, scalability and efficiency. In this work, the routing protocols, and its associated parameters are discussed along with the parameters based on the literature survey open research problem and further research directions in the future related to aggregate routing in WSN are discussed.

Keywords: WSN, LEACH, Aggregation.

1. INTRODUCTION

WSN is a wireless network consisting of nodes [1] with limitations in aspects such as power and memory. Routing [2] is the data processing techniques among the sensor node to improvise the performance of the network. Routing involves passing the data through several intermediate nodes to the sink node. Traditional routing techniques [3] do not perform well in WSN because in wireless network, bandwidth is considerable, but in WSN bandwidth is inadequate and unpredictable. Energy consumption [2] of sensor node is an important concern in WSN. The main objective of routing is to achieve optimality, simplicity, minimal overhead, robustness, stability, speed and flexibility. The design of routing protocols [3] in sensor networks is altered by many critical and disputing factors. These are Node deployment: In self-organized method the nodes are scattered in a random manner. If the sensors are not uniformly distributed optimal clustering becomes mandatory to authorize energy efficient network operation. Energy considers: Sensor node lifetime strongly depends on the battery lifetime. In a multi-hop WSN each node will act as a sender as well as a router. Data Reporting Model: These protocols are highly inclined by the data reporting model with respect to route stability and energy utilization. Data aggregation: Due to proximity many sensor nodes will send similar packets. The number of transmission is reduced by allowing redundant data transmission from many nodes for aggregation. Aggregation involves duplicate suppression, maxima, minima and average. Fault tolerance may require rerouting of packets so routing protocol must form a new link to route the data. It needs multiple level of redundancy.

1.1 Architecture Based Routing Protocols:

Routing Protocols [3] are classified according to the structure of the sensor network, which is very important for the intended operation. These protocols are Flat-based routing, Hierarchical-based routing and Location-based routing.

1.1.1Flat-Based Routing: Flat based routing [3] is required in case of a large number of sensor nodes; every node has a significant role in this routine. Energy Aware Routing (EAR) Direct Diffusion (DD), Minimum Cost Forwarding Algorithm (MCFA), Sensor Protocols for Information via Negotiation (SPIN) and Active Query forwarding In sensor network (ACQUIRE) are comes under Flat-based routing protocols. In direct diffusion, the concept of data centric routing is used to aggregate received data from many sources by reducing the redundant data. This data centric approach will find routes from various sources to a particular destination. Initially, all the Sensor nodes measure the events when occurred and create an information gradient in their neighborhood. If a sink node wants to collect the information about the event, it will broadcast the interests of the network by hop to hop communication. Intermediate nodes propagate these interests. Interests are nothing but the query/ tasks which required by the network. After getting the interests, the node sends the gradient about that to the respective node. The gradient refers to an attribute value and to a certain direction. If the gradient satisfies the interests, that path is reinforced to prevent further flooding. If the sink node receives data from the sources, it will refresh and re-sends the interests periodically. In this each node has the ability to perform the aggregation. It is based on on-demand queries sent by the sink node. The major advantages of this method are all communications are neighbor to neighbor without addressing node and each node can do aggregation along with caching the data. The problem with this method is that, it is not suitable for monitoring. In ACQUIRE (Active Query Forwarding in Sensor Networks), initially BS sends the query to each node, and then the nodes try to respond partially to the query from base station through utilizing the information pre-cached. This information's are then forwarded to other sensor node. If the information pre-cached is not recently updated, then the node will collect the data from the neighboring node within hopes.

1.1.2 Hierarchical-Based Routing:

Cluster based routing or hierarchical- based routing [4], [5], [6] is an energy effective routing technique. It works on a scheme under which the node with highest energy is randomly selected for transmitting and processing the sensed data. The nodes with low power are used for sensing and transmitting information within the cluster to cluster heads. This type of routing techniques contributes in terms of network scalability, less energy consumption and lifetime. Hierarchical Power-Active Routing (HPAR), Hierarchical Cluster Based Routing (HCR), Threshold sensitive energy efficient sensor network protocol (TEEN) and Power efficient gathering in sensor information systems (PEGASIS) are some examples of hierarchical-based routing protocols.

LEACH (Low Energy Adaptive Cluster Hierarchy) [4], [5] is a self- organizing, adaptive clustering protocol. It is based on TDMA based MAC protocol which is used to provide data aggregation with energy efficient communication. Each node follows stochastic (random) algorithm at each round to become CH. The information is transmitted from node to CH and from CH to BS. Aggregation works are carried out by CH. Random CH selection in each round with rotation. Within clusters, TDMA is preferred and CDMA is used across the clusters. To reduce collisions, inter cluster and intra clusters are used. LEACH assumes all the nodes having the ability to act as CH. The major advantage is, it organizes entire network distributed without any global knowledge, less power consumption because of aggregation by cluster heads. The disadvantages are that it assumes each and every node in the network with equal energy and transmits this data will cause battery drainage and all the nodes should adhere to both TDMA and CDMA techniques. Hierarchical cluster- based routing , clusters are organized only for a short span time termed as round. A round has two phases; election as well as data transfer phase. Here in election phase all the nodes are organized into different set clusters and these cluster heads consist of a headset. While in data transfer phase, the head set node will only involve in long range communication with the base station from cluster head. TEEN (Threshold sensitive energy efficient protocol) [5] is a reactive protocol because the nodes react immediately to sudden and drastic changes in the value of a sensed attribute. At every change of CH, that information can be broadcasted to its members. It is event driven protocol for time critical applications. There are two threshold levels are used for this routing. They are hard and soft threshold. Both are threshold values sensed. Hard threshold is the sensed value. Soft threshold is the small change in the sensed value of CH, that information can be broadcasted to its members. It is event driven protocol for time critical applications. There are two threshold levels are used for this routing. These attribute is nothing but the small change in the value of sensed attribute. In APTEEN, a node should sample and transmit data even if it does not send data for count- time CT specified by CH. CT refers that the time taken between two corresponding reports by a node. The advantages are reducing no. of transmissions, the disadvantages are more overhead and complexities in cluster formation and threshold based functions. PEGASIS (Power Efficient Gathering in Sensor Information System) [6] is used in network lifetime extension; nodes need to communicate with BS. The main objective is nothing but enhancing the nodes lifetime by collaborative technique. Bandwidth consumption is reduced in communication because of local coordination between nodes is possible. It avoids formation of clusters. Here only single node is utilized for transmitting data to BS instead of many nodes. Signal strength is used to measure the distance between two nodes. The aggregated data will be transmitted to BS by nodes in the chain. Every node in the chain will get turn for sensing data to BS. Advantages are improved performance gain; limit the no. of transmissions and eliminating overhead of Dynamic Cluster formation and the disadvantages are delay due to nodes at long distance and leader becomes bottleneck.. Scalability is the big issue.

1.1.3 Location-Based Routing:

This type of architecture is utilized where the sensor nodes are deployed randomly in a particular area of interest and these nodes are generally known by the geographic position [3]. The distance between nodes is analyzed by the signal strength between these nodes and coordinates are estimated by information exchange between the neighboring nodes. Geographic and energy aware routing (GEAR) [9] and Geographic distance routing (GEDIR) [9] are the examples of location-based routing networks. Geographical and Energy Aware Routing (GEAR) is the advanced form of direct diffusion routing. This allows the interests from one region only and restricts interests from other regions. It conserves more energy when compared to direct diffusion. Each and every node has both cost for estimation and learning. Cost of estimation will be the combined cost of remaining energy and length to arrive at destination. The alteration of the estimated cost results in learning cost. Any node in the absence of neighbors is called as a hole. It there is no hole in a network, learned cost and an estimated cost will be equal. As soon as the destination receives the packet, the cost of learning flips one hop consistently. It is used for the route setup for the incoming packets. It forwards the packet within the region as well as towards the region.

2. Aggregation Based Routing Protocol:

This section the aggregation [6], [9] based routing protocol is discussed. The aggregation based routing enhances the quality of routing among the sensor nodes. Some of the aggregation routing protocols are as follows:

2.1COUGAR:

It is one of the data centric protocols [7] used for huge distributed system. It follows in-network data aggregation. In this routing, query layer is used which lies between network and application layer. Cluster leader is used perform data aggregation and send the aggregated data to BS and sets the query plan based on generating queries. The drawbacks are increased overhead, failure of leader nodes, requires more synchronization.

2.2 TAG:

Tiny Aggregation Service (TAG) [7] is a data-centric framework for efficient data aggregation. To attain this, parent nodes should allow the other children nodes to realize the time required for transmission. as well as parent nodes reserve the data of their children to avert from data failure. Precisely, the message transmission from the base station takes place at the distribution phase and it needs its sensor nodes to systemize routing tree for the base station to send its request easily. In this approach every message has a field denoting the distance from the root to node which is sending. Usually it considers as zero at the root level and if any node that does not have any level but receives message, then it will assign its own level starting from zero. This will be incremented basically from a level of one and consigns the sending node as parent node. Until all the process lasts in all the sensor nodes in the network joins the tree has a parent. This message seasonally continual to keep the structure of tree renewed. Advantage of Tag protocol is used to monitor applications and admits a flexible sleep schedule for sensor nodes. The disadvantage of TAG is not accurate and it has low efficiency. Nevertheless, like numerous referred to tree based aggregation aware routing algorithm, the TAG approach requires a large number of messages swap to preserve the tree.

2.3 Secure Hop-by-Hop Data Aggregation Protocol [7], [8]**:** In WSN, an important concern is security. There exists some link between security needs and data aggregation process. The (DOS) Denial of service is a major problem in wireless networks and it may disable the node constantly leading to some redundancy and also allowing the availability losses. SDAP [7], [8] affords data confidentiality, source authentication and data integrity. In SDAP hop-by-hop aggregation process more faith is placed in higher level nodes because the large number of data manipulated in this node. Sometimes the compromised nodes produce some fake data and this form a drastic change in the final result.. SDAP form sub trees by randomly dividing the topology tree, those sub trees are similar in size. By this approach, higher level nodes reduce the potential threat to security by another compromised high level node. This envisioned protocol performs the authentication and encryption in sensed data and after decrypting then it is transmitted to the base station. At every middle node, the data aggregation takes place so the energy efficiency is improvised. Due to incompatible target both the data aggregation and security protocol [9] must be structured together and can be accomplished without reassuring security.

2.4 EADAT: The protocol experiments formulated on Energy-Aware Distributed Aggregation Tree protocol [10]. The base station, which initiates the tree that is forming the root of the aggregation, disseminates the control message which contains five fields: ID, parent, power, status, and hop-count. Each sensor node consists of separate id and aggregation tree contains parent node, the path length, which defines the number of hops from the sink. This message forwards the sensor nodes up to once the message broadcast by each node and leads to an aggregation tree set up at the base station. By monitoring the sensor node energy level [10], [11], there is a higher probability to get the higher residual power in sensor nodes to grow into a non-leaf node so the simulation results display this protocol protract network lifetime and conserves more energy. In EADAT, tree structure, routing is followed to select the active non-leaf nodes. There is some traffic load occurring in the construction of tree aggregation and chomp energy. By describing the overhead effects computation of the energy utilization by EADAT control message is done and matching it with the entire system.

2.5 Tree based Data Aggregation [11]: The protocols in this class are based on the hierarchical manner. The method involving less complexity for data aggregation from the source towards the sink node is to nominate some special nodes, which will function as aggregation points in a predefined direction during data forwarding. Aggregation [11] comes into picture when a node of the tree experiences the arrival of data packets from two or more source nodes. This particular node then performs aggregation by combining the data received by its own data the data of and pass on exactly one data packet to its neighbors which is its successor in the tree in sense lower in the hierarchy. The major defect in this approach is that when a data packet is lost accounted to channel wreckage, the data from the entire sub tree will be lost. Therefore, this requires a structure for fault tolerance for ensuring reliability in forwarding the aggregated data. Despite the fact, there is a high cost requirement for maintenance of the hierarchical structure in vital networks and the scarcity in the strength of the system, if it is prone to damage; these methods are in particular suited for designing aggregation function [12] for optimality and enhancing the energy management efficiency while facilitating the data aggregation in the in-between nodes. In utmost cases, a shortest path routing tree is built by the tree-based protocols. This approach is on the basis, using the shortest path routing every node encounters an event, and announces the information collected to the sink node. The Directed Diffusion algorithm which is proposed for attribute-based routing wherein there is an opportunistic data aggregation.

2.5 DRINA: Data Routing for In-network Aggregation [16]: The primary motive of DRINA is to maximize the data aggregation with the inclusion of shortest path routing to the sink node.

Phase 1 [16]: Construction of Hop Tree: The phase is initiated by the sink node forwarding the Hop Configuration Message (HCM) to all the nodes in the network with the aid of flooding technique. The two segments of the HCM message: ID and Hop to Tree. ID stands for the node identifier that initiated or imparted the HCM and Hop to Tree is the hop distance by which passing of HCM occurs. The Hop to Tree value is initialized to 1 at the sink node. Verification of Hop To Tree value is done by each node upon receiving the HCM and checks whether the value is less than the value stored in Hop To Tree and on the condition that the value of First Sending is true, then the value of the Next Hop variable is updated with the field ID value of the HCM else if the condition is false, then it means that the HCM is already received by the node by SPT. The node drops the HCM message received. These steps take place frequently, until the configuration of the whole network occurs. Earlier to the occurrence of the first event, there is no routes established and the smallest distance to the sink is the value the Hop to Tree variable retains. After an event has occurred, it will contain the smaller of two values, i.e. firstly the initial value and secondly the occurred event hop distance: and the value that it finally it contains is the smallest distance to the sink measured in hops. **Phase 2 [16]:** Formation of Cluster: The leader election algorithm is started at the moment when an event is sensed by one or many nodes. Such nodes will take part in the election and the leader is one which is closest to the sink or the closest to existing established route. If a tie arises then the node with the smallest value of ID becomes eligible or taking energy level as another criterion. The result of the election process is that one node which satisfies the criteria becomes the leader node and the other node which detects an occurrence of an event becomes the Collaborators. The task accomplished by the coordinator is receiving the information gathered by the collaborators and forward it towards the sink. The key aspect this algorithm is that the information from all the nodes which representing the same action will be stored or aggregated at the coordinator. **Phase 3 [16]:** Formation of Routing Sequence and Updating of Hop Tree: The new route is established by the coordinator for the event distribution which is implemented by means of sending a route establishment message to its corresponding Next Hop node. On receiving this message, the Next Hop node retransmits the route establishment message to its Next Hop and the updating of hop tree starts. The above steps are replicated until the sink or a node belonging to an existing route is reached. The routes are established by taking the best nearby node at every hop. The best neighbor is chosen on the basis of two factors: 1) the shortest path to the sink on the occurrence of the first event. 2) When subsequent events occur, the best neighbor node is one which is closer to the sink in terms of already established route. By this way the maximization of aggregation points occurs. The resulting route is the tree that establishes the connection between the coordinator and the sink. By HCM message concept we ensure control flooding such that the whole cost of this infrastructure equals the flooding. To ensure reliability of data transmission a route repair mechanism is implemented which is discussed in the next section.

2.6 DBMAC [15]: To solve the problems of well-organized data aggregation trees WSN is a different approach called Delay Bounded Medium Access Control (DBMAC) is introduced. This protocol combines routing and MAC protocol mechanisms to accomplish data aggregation. The main aim of DBMAC scheme is to obtain a reduction in latency for delay bounded applications and to improvise energy efficiency by enhancing the advantage of data aggregation mechanisms. DBMAC introduces the carrier sense multiple access with collision avoidance (CSMA/CA) mechanism. By considering the advantage of CTS messages of other nodes, the sensor nodes can select the relay node in the middle of nodes that consist of some packets to broadcast in the containing queue. Hence the aggregation efficiency is increased in the network as well as information in that path is formed as single packet.

2.7 Information Fusion-based Role Assignment (InFRA) [15]: The algorithm forms a cluster for event containing only the nodes that are discoverable. Here cluster head will combine all the data in the cluster and forwards towards the cluster head. The main objective of InFRA algorithm is to find the shortest path to reduce the information fusion. Group coordinate system is used here to reduce the information fusion, hence once the cluster is formed then the sink node will elect the shortest path towards the sink node. Advantage of InFRA algorithm is fusion based aggregation. Disadvantage of this algorithm is for arrival of each and every event should be broadcasted to the entire network to notify other nodes in the network about the new arrival and to revise the collected information in the coordinates. This in case raises the communication cost and reduces the scalability.

2.8 Shortest Path Tree [15]: Shortest path tree is a data aggregation protocol and it is proposed for Data centric routing protocol. SPT based data aggregation protocol promotes about the energetic awareness of the parent nodes. In this protocol the selection of the parent node is done based on the distance of sensor nodes to the BS and their energy level. The merits of the shortest path tree protocol are aggregation protocols that it considers information theory as routing metric. The disadvantage of SPT is not accurate and it is less efficient too.

2.9 RDAT [15]: In wireless networks a unique, fast data aggregation and transmission protocol, which is based on functional reputation. This protocol improves dependability of data aggregation and transmission by defining sensor node action and displaying corresponded function status. RDAT provides a fault tolerant Reed-Solomon coding technique that occupies on multi path data transmission algorithm to certify the actual data transmission to the base station, and simulation also denotes the reliability of data transmission and aggregation in the occurrence of impaired nodes. In this protocol, security is certified for particular data aggregators using functional reputation and weighing sensor data using sensing functional reputation, so follow in addition uses a multipath transmission algorithm that is designed on routing functional reputation. There is firsthand information about neighboring node, obtain with the help of sensor nodes, which supervise the neighborhood and also each sensor node retrieves good and bad performance of its neighbors on a table referred to a stable of functional reputation. Normally it is not applicable for aggregators to verify the correctness of sensor node's data. Sometimes neighboring nodes get overlapped and data sensed are correlated, the neighbor, it is reading of local outlier, false data injection attacks are detected. During a false data reports are transmitting it may induce false data and to deceive the base station. By using the density of sensor nodes the threshold value is determined depending on application. RDAT to make sure of the consistent data transmission to the base station and this protocol is not generous, so making the operation of protocol RDAT is realistic.

2.9 EEHA[15]: Energy-efficient and high accuracy technique for data aggregation. This technique has included consideration of the three issues: communication overhead, aggregation accuracy and protection of privacy and appraise to project the tradeoffs among them. This protocol technique has reduced bandwidth, energy utilization and also improves data accuracy [11], [12], provides data privacy. Four steps involved: aggregation tree construction, slicing, mixing and aggregation. In this technique combines both from sensor nodes to form a data aggregation tree and path and are not required to shortest paths. The aggregation tree [13], [14] is optimized and the network is routed to base station. Each leaf arbitrarily chosen set of nodes within the hops and leaf then forms slices into private data and in mixing step aggregation tree leaves waiting for some time, which assure that all slices are accepted, and then decryption takes place and add all the accepted slices finally slice left by it to execute a result. In aggregation step encrypted the result and then transmit to parent, the accepted results are forwarded by their children and intermediate node perform the operation of aggregation here we determined the time interval difference because the parent node wait for a long time than child nodes, and finally we got an overall sensor reading and accepted data encryption takes place then transmit to parent node at that time is elapsed. The target of the protocol is that the sensor can calculate an absolute aggregation final value and the private sensor value is released to another sensor. Data privacy [11], [12] is different for both the leaf and intermediate node there is no occurrence of collisions, more energy efficient protocol.

2.10 SMART [15]: The pattern of Slice-Mix-Aggregate (SMART) for excessive aggregation functions, which assures data privacy through data ‘‘slicing and assembling” method [11], [12]. Each node should slice the sensor readings arbitrarily into some number of pieces, and one piece has kept itself while the remaining is distributed confidentially to other nodes. This will result in communication overhead in turn increases the collision between messages.

2.11 SRDA [14], [15]: Secure Reference-Based Data Aggregation (SRDA) protocol is projected for cluster based WSN. In SDRA the data obtained from sensing are compared with some set of predefined reference values and values which are different are only transmitted. The set of reference values are taken on basis of the previous values. Whereas, aggregation minimizes the number of packet being transmitted by reducing the size of packets transmitted. This will increase energy saving. Usually the aggregation algorithms [11], [12], sensors broadcast the raw data to all nodes. This will waste the bandwidth. Some data which are same are already stored in the nodes. The raw data sensed is compared with the predefined sensed value and only the difference is ransmitted. Therefore, differential aggregation has greater possibility to decrease the amount of data to be broadcasted from sensor nodes to cluster heads. The shortcoming of SRDA is that they do not allow intermediate nodes to do data aggregation.

2.12 CDAP [13], [14]: Concealed data aggregation protocol makes use of the privacy homomorphism to present hierarchical concealed data aggregation in the network. Once the network deployed, each AGGNODE determines pairwise keys with its neighboring nodes. These nodes can send their readings to the AGGNODE securely. Each AGGNODE increase its neighbor for sensor readings during the collection phase. AGGNODE obtains the encrypted data from its neighboring node. The data is encrypted using a symmetric key encryption algorithm. The received data is decrypted and aggregated and further it encrypts the aggregated data using a privacy homomorphic encryption algorithm. Only the base station is capable of decrypting the data using its private key. On the other hand, it improves the aggregation, energy efficiency and usage of bandwidth networks whilst affording secure communication.

Table 1: Comparisons of Evaluation Parameters of Routing Protocols

Protocol	Mobility	Data Aggregation	Scalability	Power Usage
Spin	Possible	Yes	Limited	Limited
Directed Diffusion	Limited	Yes	Limited	Limited
Cougar	No	Yes	Limited	Limited
Acquire	Limited	Yes	Limited	N/A
Leach	Fixed Bs	Yes	Good	Maximum
Teen & Apteen	Fixed Bs	Yes	Good	Maximum
Pegasis	Fixed Bs	No	Good	Maximum
Hcr	No	No	Good	N/A
Gear	Limited	Limited	No	No

Table 2: Advantages and Disadvantages of Existing Routing Protocols

Protocol	Advantages	Disadvantages
Shortest Path Tree	Data aggregation protocols that consider information theory as routing metric.	Not Accurate, Low Efficiency
Tiny Aggregation Service (TAG)	Specifically designed for monitoring applications and allows an adjustable sleep schedule for sensor nodes.	Not Energy Efficient, Does not alter the network structure
Information Fusion-based Role Assignment (InFRA)	A fusion based aggregation	Less Efficient
LEACH	Randomization to evenly distribute the energy expenditure among the sensor nodes.	Not optimized one
HEED	Average Minimum Reachability Power (AMRP). AMPR is used to estimate the communication cost in each cluster.	Additional Computational overhead
Secure Reference-Based Data Aggregation (SRDA) protocol	Raw data sensed by sensor nodes are compared with reference data values and then only the difference data are transmitted.	Do not allow intermediate nodes to perform data aggregation
Secure Hop-by-hop Data Aggregation Protocol (SDAP)	Compared to low-level sensor nodes, more trust is placed on the high-level nodes (i.e., nodes closer to the root) during a normal hop-by-hop aggregation process in a tree topology.	Not dynamic
Energy-efficient and secure pattern based data aggregation ESPDA	Uses pattern codes to perform data aggregation. That is extracted from the actual data in such a way that every pattern code has certain characteristics of the corresponding actual data.	Pattern matching is difficult.
Concealed Data Aggregation (CDA)	Sensor nodes share a common symmetric key with the base station	Easy way of Access

3. CONCLUSION

In this work the design issues and various routing protocols [11], [12] related to the improvement of mobility, position awareness, data aggregation, scalability and energy usage are discussed. These surveys [11], [12] are used to identify the drawbacks of existing routing protocols, and also used to develop the proposed framework model. The comparisons of evaluation parameters of routing techniques of existing routing protocols are summarized in Table 1 and Table 2 respectively. Based on the detailed survey in existing routing protocols, the following problems are identified. In existing routing protocol, finding and maintaining the routes between the sensor nodes in WSN are time consuming process. The existing routing protocols the attention of unexpected variations in node status, recurrent and volatile changes in network structure are very difficult. The data organization and data management in sensor node is an important practice in WSN. The sensor nodes are controlled in energy and bandwidth. The sensor nodes are very large in WSN; it is not possible to use the global addressing scheme for sensor nodes which leads the additional overhead of ID maintenance. The sensor nodes are strongly reserved in energy, computational rate, and storage dimensions. Routing challenges and design issues are Node deployment, Energy consumption without losing accuracy, Data Reporting Model, Fault Tolerance, Scalability, Connectivity, Coverage, Data Aggregation and Quality of Service. Those factors will really affect the routing process in WSNs. The single routing protocol does not cover all the design issues. The single routing protocol does not provide the optimal route and does not afford maximum network lifetime, resource awareness &use of metadata. Some routing protocols that use a single path and thereby does not focus Route Repair Mechanism. An existing routing protocol is enhanced for the limited capabilities of the nodes but does not consider security. Existing routing protocols does not concentrate the total number of messages for setting up a routing tree, number of covering routes, aggregation rate, and reliability.

4. REFERENCES

[1]. I.F. Akyildiz, I.H. Kasimoglu, “Wireless sensor and actor networks: research challenges, Ad Hoc Network”, 2004, 351–367.

[2]. V. Mhatre, et. al., Design guidelines for wireless sensor networks: communication, clustering and aggregation," Ad Hoc Networks Journal, Elsevier Science, 2(1), 2004, 45-63.

[3]. E. Stavrou, A. Pitsillides, A survey on secure multipath routing protocols in WSN’s, Comput. Network. 54, 2010, 2215–2238.

[4]. M. J. Handy, M. Haase, D. Timmermann, “Low Energy Adaptive ClusteringHierarchy with Deterministic Cluster-Head Selection,” In Proc.4th International Workshop on Mobile and Wireless Communications Network, USA, 2002, Vol. 1, pp. 368-372.

[5] J. Lotf, M. Bonab, S. Khorsandi, “A Novel Cluster-based Routing Protocol with Extending Lifetime for Wireless Sensor Networks,”In Proc. 5th IFIP International Conference on Wireless and OpticalCommunications Networks (WOCN08), East Java Indonesia, Surabaya,2008, pp. 1-5.

[6]. D. A. Vidhate, A. K. Patil, S. S. Pophale, “Performance Evaluation of Low Energy Adaptive Clustering Hierarchy Protocol for Wireless Sensor Networks,” In Proc. International Conference and Workshop on Emerging Trends in Technology (ICWET 2010)TCET, Mumbai, India, 2010, pp. 59-63.

[7]. L. Villas, A. Boukerche, R.B. de Araujo, and A.A.F. Loureiro, “Highly Dynamic Routing Protocol for Data Aggregation in Sensor Networks,” Proc. IEEE Symp. Computers and Comm. (ISCC), pp. 496-502, http://dx.doi.org/10.1109/ISCC.2010.5546580, 2010.

[8]. Hongjuan Li, Kai Lin, Keqiu Li, “Energy-efficient and high-accuracy secure data aggregation in wireless sensor networks”, Computer Communications 34, 2011, 591–597.

[9]. Agnius, L., V. Arunas and K. Egidijus, 2010. A Survey of Wireless Sensor Network Interconnection to External Networks. Springer Science, Business Media B.V., DOI: 10.1007/978-90-481-3662-9_7.

[10]. K. Lu, L. Huang, Y. Wan, H. Xu, Energy-efficient data gathering in large wireless sensor networks, in: Second International Conference on Embedded Software and Systems, 2005, pp. 5–10.

[11]. Ozdemir, Yang Xiao, “Secure data aggregation in wireless sensor networks: A comprehensive overview”, Computer Networks 53 ,2009, 2022–2037.

[12]. E. Fasolo, M. Rossi, J. Widmer, and M. Zorzi, “In-network Aggregation Techniques for Wireless Sensor Networks: A Survey,” IEEE Wireless Comm., vol. 14, no. 2, , 2007 pp. 70-87.

[13]. L.A. Villas, A. Boukerche, R.B. Araujo, and A.A. Loureiro, “A Reliable and Data Aggregation Aware Routing Protocol for Wireless Sensor Networks,” Proc. 12th ACM Int’l Conf. Modeling, Analysis and Simulation of Wireless and Mobile Systems (MSWiM), pp. 245-252.

[14]. SudipMisra, P. Dias Thomasinous, “A simple, least-time, and energy-efficient routing protocol with one-level data Aggregation for wireless sensor networks”, Journal of Systems and Software 83, 2010, 852–860.

[15] Hemant Sethi, R. B. Patel, ‘EIRDA: An Energy Efficient Interest based Reliable Data Aggregation Protocol for Wireless Sensor Networks’ International Journal of Computer Applications (0975 – 8887), Volume 22– No.7, May 2011.

[16] Leandro Aparecido Villas, Azzedine Boukerche, Heitor Soares Ramos, Horacio A.B. Fernandes de Oliveira, Regina Borges de Araujo, and Antonio Alfredo Ferreira Loureiro, ‘DRINA: A Lightweight and Reliable Routing Approach for In-Network Aggregation in Wireless Sensor Networks’, IEEE Transactions on Computers, vol. 62, no. 4, April 2013.