A REVIEW ON UNIQUE KEY ASSIGNMENT AND RELIABLE ROUTING SCHEMES OVER WSNs

Gaurav Sharma * , Vikrant MAnocha *, Shanu MAlhotra#

[*] *Asst. Professor, Dept. of Computer Science and Engg.*
MMU, Mullana, India .
[#] *Asst. Professor, Dept. of Computer Science and Engg.*
ISTK, Yamuna nagar, India

ABSTRACT

In the current decade, wireless sensor networks are emerging as a peculiar multi-disciplinary research area. In WSNs, lower sensing ranges result in dense networks, which bring the necessity to achieve an efficient key management and reliable routing protocols subject to power constraints. WSNs may contain one or more base stations to collect sensed data and possibly relay it to a central processing and storage system. Unique Key allocation is usually not applicable in a sensor network due to the massive production of cheap sensor nodes, the limited bandwidth, and the size of the payload. Several solutions have been proposed for locally unique ID assignment in WSN in order to reduce the communication overhead, which is not desirable due to the limited power supply in a sensor node. In this paper, we study the possible key assignment schemes for WSNs to assign the local unique Key's to the wireless sensor nodes. The main emphasis in this paper is to preserve more power by means of delaying key assignment conflict and routing resolution until necessary in WSNs and present the possible schemes and techniques by which we can increase robustness of WSNs.

Keyword : - WSN, ID, MAC .

I. INTRODUCTION

The birth of wireless communications dates from the late 1800s, when M.G. Marconi did the pioneer work establishing the first successful radio communication systems have been developing and evolving with a furious pace. Wireless having no wired connection, using wireless media for communication. Sensor device having some sensing capability, like sensing the humidity. Network collection of different types of nodes like sensor nodes , routers, printers etc. A WSN consists of a large number of sensor nodes in hundreds or thousands. Each sensor node consists of different components which work together to act like as sensor and can sense for some particular application. Wireless sensors are generally equipped with data processing and communication capabilities. The sensing circuitry measures ambient conditions related to the environment surrounding the sensor and transform them into an electric signal. Processing such a signal reveals some properties about objects located and the events happening in the vicinity of the sensor. The sensor sends such collected data, usually via radio. The single most critical requirement for widespread adoption of such networks is power efficiency since battery replacement is not a viable option for such large wireless networks. Other challenges are the ultra-small size and per-unit device cost constraints, which are required to make such networks economically viable. These challenges necessitate advances in many different areas, some of which include sensors, radio architectures, circuit design techniques, sensor data processing and communication protocols. A WSN is composed of three main functional units: a sensing unit, a communication unit and a computing unit. General architecture of a wireless sensor network is, as shown in figure 1. In addition to regular sensor nodes, a WSN can contain one or more sink nodes. These sink nodes interact with wireless sensor nodes to collect sensed data and serve as a relay to the outside world. A sink node has a similar architecture to that of a regular node. The main difference is that a sink node does not have a sensing unit. A sink node is also considered, by default, to have an unlimited energy source, and therefore, there is no need to model a

battery to characterize its energy consumption. However, with minor changes, the user could choose to attach a battery to the base station in the same way as for a regular sensor node.

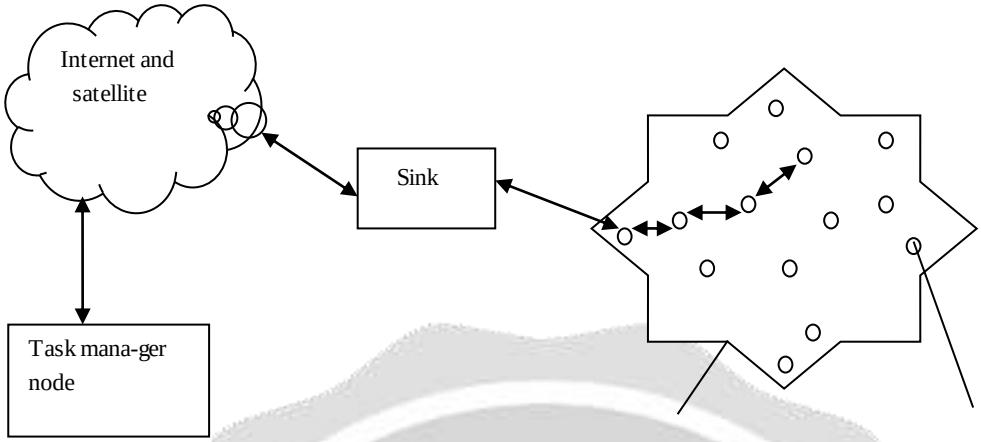

Figure 1: General architecture of a wireless sensor network.

Regardless of the specific application, there are several common observations related to the design of any WSN.

- Energy is a scarce resource in the network. However, minimizing energy consumption does not necessarily prolong the network's lifetime, nor does it ultimately supports the QoS constraints imposed by the specific application.
- The WSN design includes finding the best trade-offs between the application's goals and the network's capabilities.
- The number of active wireless sensor nodes should be minimized such that redundancy in sensor readings is minimized, while providing satisfactory quality of data.
- WSN design is directed by the type of sensor nodes used in the network.

1.1 Core Features of Wireless Sensor Networks

The design of WSN is determined by the sensor nodes characteristics and by application-specific requirements. Oftentimes, the WSN has to satisfy several constraints, suggesting the need for compromise solutions that provide balance between all of the imposed constraints. The core features of WSN are listed below.

- **Energy limitations**

Energy is thus a scarce resource, and it presents a basic limiting factor for the node's lifetime. Thus, intelligent polices for the efficient utilization of the energy resources are needed. Communication in WSN is the most expensive operation in terms of energy. `

- **Local processing**

Data collected by the wireless sensor nodes that lie in proximity to each other may contain a high level of spatial and temporal redundancy. Local data processing (through data aggregation or data fusion) reduces the amount of data that have to be transmitted back to the data sink, thereby providing the application with high-level data representations that qualitatively satisfy the application's requirements.

- **Resistance to node failure**

WSN are dynamic systems. Changes in the network topology may be caused by node failure due to various factors such as depleted batteries, environmental factors (fire, flood), an intruder's attack etc. The WSN should be self-adaptable, meaning that the loss of sensor nodes should not affect the overall functionality of the WSN.

- **Scalability**

In many applications, a WSN may contain hundreds or even thousands of sensor nodes. The WSN should be scalable, meaning that the performance of these networks should be minimally affected by a change in network size. In many cases, recharging or replacing batteries is not possible, and adding new sensor nodes is the only way to prolong the lifetime of the network.

- **Deployment**

Wireless sensor nodes can be deployed in various ways, depending on the application and the environmental conditions. They can be deployed randomly over the monitoring field, they can be attached to a specific moving object that is being monitored or they can be arranged deterministically. After deployment, the sensor nodes in most applications remain static.

- **Heterogeneity**

WSN may consist of different types of nodes in terms of their sensing capabilities, computation power, memory size, radio circuitry and energy consumption. The diversity of hardware components can become a gap between these devices, raising new issues in communication and network configuration.

- **Quality of Service (QoS)**

Satisfying the application goals by meeting the QoS requirements is one of the basic principles of WSN design. Quality of service in WSN can be defined from two perspectives: Application-specific and network. The application-specific QoS refers to QoS parameters specific to the application, such as, the quality of the sensor nodes measurements, the network's coverage, the number of active sensors, delay, etc. The network's perspective of QoS refers to the problem of how the supporting network can satisfy the application's needs, while efficiently using the WSN resources such as energy or bandwidth.

II. ROUTING IN WIRELESS SENSOR NETWORK

The main goal of any type of network is to enable information exchange among peers. routing protocols establish the routing paths between the nodes. Routing in WSN is very challenging due to several characteristics that distinguish them from contemporary wireless ad-hoc networks:

- It is not possible to build a global addressing scheme for the deployment of sheer number of sensor nodes.
- In contrary to the end-to-end structure of typical communication networks, almost all applications of WSN require directing the flow of sensed data from multiple sources to a particular sink.
- Generated data traffic has significant redundancy among individual sensor nodes, since multiple sensors may generate same data within the vicinity of a phenomenon. The routing protocols should exploit such redundancy to improve energy and bandwidth utilization.
- Sensor nodes are tightly constrained in terms of transmission power, on-board energy, processing capacity and storage and thus require careful resource management.

Almost all of the routing protocols can be classified as data centric, hierarchical or location-based although there are few distinct ones based on network flow or QoS awareness [5,6].

2.1 Data-centric protocols

In many applications of WSN, it is not feasible to assign global identifiers to each node due to the sheer number of nodes deployed. Such lack of global identification along with random deployment of sensor nodes makes it hard to select a specific set of sensor nodes to be queried. Therefore, data is usually transmitted from every sensor node within the deployment region with significant redundancy. Since this is very inefficient in terms of energy consumption, routing protocols that will be able to select a set of sensor nodes and utilize data aggregation during the relaying of data have been considered. This consideration has led to data centric routing, which is different from traditional address-based routing where routes are created between addressable nodes managed in the network layer of the communication stack. In data-centric routing, the sink sends queries to certain regions and waits for data from the sensors located in the selected regions. Since data is being requested through queries, attribute based naming is necessary to specify the properties of data. Directed Diffusion aims at diffusing data through sensor nodes by using a naming scheme for the data. The main reason behind using such a scheme is to get rid of unnecessary operations of network layer routing in order to save energy. Directed diffusion suggests the use of attribute-value pairs for the data and queries the sensors in an on demand basis by using those pairs. In order to create a query, an interest is defined using a list of attribute-value pairs such as name of objects, interval, duration, geographical area, etc. The interest is broadcast by a sink through its neighbors. Each node receiving the interest can do caching for later use. The nodes also have the ability to do in-network data aggregation. The interests in the caches are then used to compare the received data with the values in the interests. The interest entry also contains several gradient fields. A gradient is a reply link to a neighbor from which the interest was received. It is characterized by the data rate, duration and expiration time derived from the received interest's fields. Hence, by utilizing interest and gradients, paths are established between sink and sources. 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 reinforces the source node on that path to send data more frequently. Figure 3.1 summarize the directed diffusion protocol. Path repairs are also possible in directed diffusion. When a path between a source and the sink fails, a new or alternative path should be identified. For this, directed diffusion basically reinitiates reinforcement by searching

among other paths, which are sending data in lower rates. Directed Diffusion differs from SPIN in terms of the on demand data querying mechanism it has..

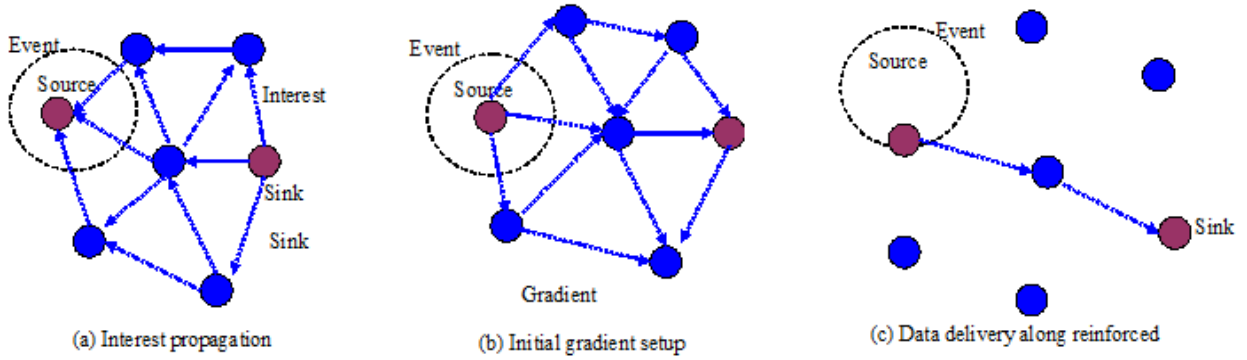

Figure 2. Directed Diffusion protocol phases

In directed diffusion the sink queries the sensor nodes if a specific data is available by flooding some tasks. In SPIN, sensors advertise the availability of data allowing interested nodes to query that data. Directed Diffusion has many advantages. Since it is data centric, all communication is neighbor-to-neighbor with no need for a node addressing mechanism. Each node can do aggregation and caching, in addition to sensing. Caching is a big advantage in terms of energy efficiency and delay. In addition, direct diffusion is highly energy efficient since it is on demand and there is no need for maintaining global network topology.However, directed diffusion cannot be applied to all sensor network applications since it is based on a query-driven data delivery model. The applications that require continuous data delivery to the sink will not work efficiently with a query-driven on demand data model. Therefore, directed diffusion is not a good choice as a routing protocol for the applications such as environmental monitoring. In addition, the naming schemes used in directed diffusion are application dependent and each time should be defined a priori. Moreover, the matching process for data and queries might require some extra overhead at the sensors.

2.2 Hierarchical protocols

Similar to other communication networks, scalability is one of the major design attributes of WSN. A single-tier network can cause the gateway to overload with the increase in sensors density. Such overload might cause latency in communication and inadequate tracking of events. In addition, the single-gateway architecture is not scalable for a larger set of sensors covering a wider area of interest since the sensors are typically not capable of long-haul communication. To allow the system to cope with additional load and to be able to cover a large area of interest without degrading the service, networking clustering has been pursued in some routing approaches. The main aim of hierarchical routing is to efficiently maintain the energy consumption of sensor nodes by involving them in multi-hop communication within a particular cluster and by performing data aggregation and fusion in order to decrease the number of transmitted messages to the sink. Cluster formation is typically based on the energy reserve of sensors and sensor's proximity to the cluster head. LEACH is one of the first hierarchical routing approaches for sensors networks [7,8]. The idea proposed in LEACH has been an inspiration for many hierarchical routing protocols, such as PEGASIS [2], TEEN [3]. The hierarchical routing paradigms can progressively prolong the network system lifetime because of its dynamic cluster operation. Also they have the advantages such as distributed property and no global network topology information is needed. However, the single hop assumption makes it not be suitable for WSN deployed in wide area. Another disadvantage is that dynamic clustering brings additional cost, such as the changing operation of cluster header.

2.3 Location-based protocols

The idea of location-based protocols is using an area instead of a node identifier as the target of a packet. Any node that is positioned within the given area will be acceptable as a destination node and can receive and process a message. In the context of WSN, such location-based routing is evidently important to request sensor data from some region. Since there is no addressing scheme for WSN like ip-addresses and they are spatially deployed in a region, location information can be utilized in routing data in an energy-efficient way. For instance, if the region to be sensed is known, using the location of sensor nodes, the query can be diffused only to that particular region which will eliminate the number of transmission significantly. Some of the protocols are designed primarily for mobile ad hoc networks and consider the mobility of nodes during the design. However, they are also well applicable to WSN where there is less or no mobility. Three main protocols of this category are SMECN, GAF and GEAR. The location-based routing protocols take into account the mobility of sensor nodes and perform very well

when the density of network increases. But, the performance is very poor when the network deployment is sparse, and there is no any data aggregation and further processing by the header node.

III. UNIQUE KEY ASSIGNMENT SCHEMES FOR WIRELESS SENSOR NETWORK

In traditional distributed systems, the name or address of a node is independent of its geographical location and is based on the network topology. However, in WSN, it has been widely proposed to use attributes external to the network topology and relevant to the application for low-level naming. The usage of the minimum number of bytes required is motivated by the need to limit the size of transmitted packets, in particular the header. For this reason, WSN are designed to limit the amount of data transmitted, for example through data aggregation. This reduces the payload of transmitted packets, which makes the header size even more significant.

In key assignment scheme, we define 1-hop uniqueness as address uniqueness among direct neighbors, and 2-hop uniqueness as address uniqueness among 2-hop neighbors. The assumption for 1-hop uniqueness is that the number of nodes in the largest complete sub-graph in the sensor network should be less than the range of the addresses (or the range of addresses minus 1, if a special address is designated as the broadcast address). The assumption for 2-hop uniqueness is that the maximum sum of the number of 1-hop neighbors and the number of 2-hop neighbors should be less than the range of the address.

With the expectant average node density (d) and transmission range (r), the designer can choose the length for the address field (l) deliberately to satisfy the assumptions.

- To satisfy 1-hop uniqueness, the address range should be greater than the number of nodes within the transmission range of one node, which means $l > \log_2 (\pi dr^2)$.
- To satisfy 2-hop uniqueness, the address range should be greater than the number of nodes within a circular area of two times the transmission range, which means $l > \log_2 (4\pi dr^2)$.

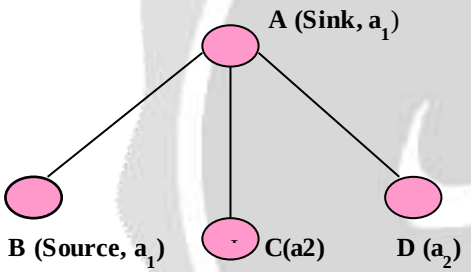

Figure 3. A small Sensor Network.

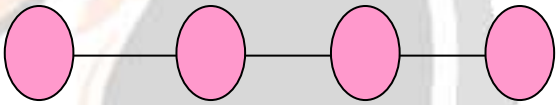

Figure 4. An example of 2-hop conflict.

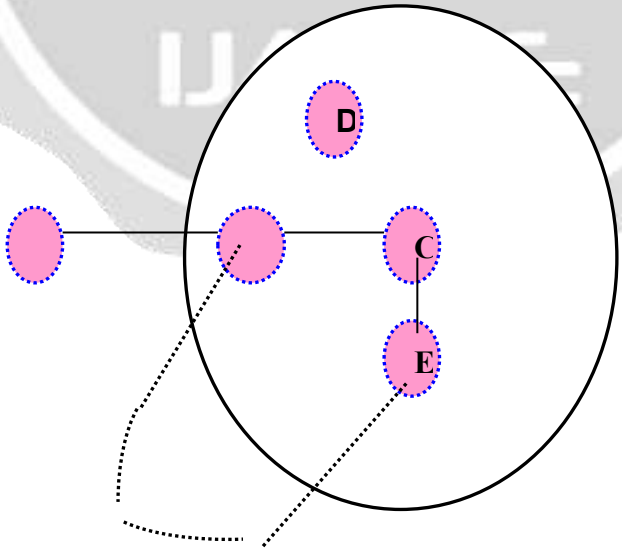

Figure 5 Path loop.

As illustrated in Figure 4, if node B records node A (with the address of x) as its next hop back to the sink and then it finds that there are two 1-hop neighbors with the same address of x, it notifies them to change. Node A may

change to the address of y, node C to z. On receipt of both change messages, which new address should be used as the next hop for node B?

There are two methods to solve this problem:

1) We can designate that every node choose a random number in addition to its random address. If the length for the random number is long enough (e.g., 16 bits), the probability that two neighboring nodes choose the same random number will be very low. If the random number is piggybacked in the broadcast of the interest message and change message, a node is differentiated among its neighbors. For a stationary sensor network, the random number is needed only once for the first broadcast/forwarding of the interest message. In case that new nodes may join the stationary network later or a node misses copies of the first interest message, a node will receive a message without the piggybacked random number as the first message. The node can just drop the message and broadcast a special control message requesting its neighbors' random number for once. Thus, the overhead caused by the random number in the interest message is trivial. However, it will bring too much communication overhead in a mobile sensor network since every interest message must include the random number.

2) The alternative for mobile sensor networks is to use a hop count field that is usually found in routing messages in a MANET. As the interest message passes a node, the hop count field is increased by 1, which is also recorded in the node. The hop count field is also included in the change announcement message. Therefore, if the hop count in the change message is equal to the receiver's hop count minus 1, then the next hop address is updated if it is the same as the old address contained in the change message. We can limit the size for the hop count field to only 4 bits, and utilize the modulo operation. As shown in Figure 5, if the hop count is 15 for node A, 0 for node B, and 1 for node C, on receipt of both change messages, node B will update its next hop address to y because $0 = (15 + 1) \bmod 16$. If the hop counts for both nodes A and C are 2, and it is 3 for node B, either one could be the next hop for node B because neither of them uses node B as the next hop. Given that node B has a hop count of i + 1, we need to calculate the probability that node C has a hop count of i with the assumptions that node C has not received any interest message yet, and that node B has not forwarded the interest message. Suppose that the transmission range is r, the average node density is d, and the packet loss rate is q. The total number of node C's neighbors is $\pi r^2 d$. If the hop counts are distributed evenly for all node C's neighbors that have received the interest message, the number of node C's neighbors whose hop counts are not i-1 is $15\pi r^2 d/16$, while the number of remaining neighbors is $\pi r^2 d/16$. The probability that node C has a hop count of i is $q^{15\pi r2d/16} * (1-q) * (\pi r^2 d/16)$, which is the probability for one neighbor of node B.

Procedure for ID assignment in WSN

I. In the beginning, every node chooses a random ID.
II. The sink node broadcasts an INTEREST message.
III. All the neighbor nodes record the sender's ID. If the sender's ID is the same as its own, it chooses another one randomly, and broadcasts a CHANGE message (this is used to solve 1-hop conflict).
IV. The neighbor waits for a random delay and rebroadcasts the INTEREST message.
V. If a node receives an INTEREST message with the same source ID more than once, it puts the ID in a RESOLVE message and broadcasts to its neighbors (this is used to solve 2-hop conflict).
VI. If a node receives a RESOLVE message containing its ID, it chooses another one randomly (because it records all the 1-hop neighbors' IDs, so it will not lead to 1-hop conflict), and broadcasts a CHANGE message (to avoid further potential 2-hop conflict).
VII. After the intended source node receives the INTEREST message, it unicasts a REPLY message back to the sink (every node records the sender's ID of the first copy of the INTEREST message as the next hop back to the sink).
VIII. On receipt of a CHANGE message, a node updates its next hop back to the sink, if necessary.

IV. RELATED WORK

H Zhou et al. [1], proposes reactive ID assignment, which is an efficient ID assignment in a WSN. Although the schemes in [2,3] recommended Huffman coded addresses for wireless sensor nodes, this paper still adhere to fixed-length IDs due to the nodes in a WSN are usually manufactured in batches. Although the average length of Huffman-coded address is less than the size of a fixed address format, it would be much easier for designers to allocate the fixed-length field for the MAC address in the physical layer in advance.Noticing that ID is not needed if there is no data communications, if we could delay ID conflict resolution until data communications are necessary, we can preserve as much power as possible. Compared with proactive schemes, a reactive ID assignment approach is proposed to accomplish the goal and preserve more power by means of delaying ID conflict resolution until necessary. It has no requirement on apriori unique IDs of the Wireless Sensor nodes, and is easy to integrate with the directed diffusion communication paradigm.

In [3], studied that, in WSN, the vast majority of wide-scale traffic consists of only a few bytes, including all network and application layer IDs. Therefore, MAC addresses, which are vital in a shared medium, present major overhead, particularly because they are traditionally chosen network-wide unique. To tackle this overhead, they propose a dynamic MAC addressing scheme based on a distributed algorithm. The assigned addresses are reused spatially and represented by variable length codewords. This scheme scales very well with the network size, rendering it well suited for sensor networks with thousands or millions of nodes. Distributed address assignment algorithm is very efficient as the network wide communication needed for a centralized algorithm is too energy costly, especially in large networks. Moreover, the network topology is not perfectly constant due to independent boot times, nodes failing or being added, etc. Since the network has to remain operational, the address assignment algorithm should quickly acquire a valid solution that tracks the topology changes. This property is called as additive convergence. A centralized algorithm would require costly global updates, therefore a distributed algorithm is a viable option.

In [4]**,** worked on a distributed algorithm that assigns globally unique IDs to sensor nodes. Initially, it assumes that all nodes are awake during the execution of the algorithm. This assumption is relaxed later in this paper to accommodate a dynamic network where nodes can join the network at any time during the execution of the algorithm or after its termination. The algorithm can be divided into three main phases. In the first phase, the objective is to assign temporary unique identifiers in the form of potentially long vectors of bytes. A tree structure rooted at the node initiating the algorithm is established during this phase. In the second phase, the temporary identifiers are used to reliably compute the size of each sub-tree and report it to the parent node. This process is done for each sub-tree from leaf nodes until the root node. At the end of this phase, the initiator knows the total size of the network. This allows the initiator to compute the minimum number of bytes required to give a unique ID to each node in the tree. The third phase consists of assigning final IDs to each node in the network going from the root to the leaf nodes.

J. H. Kang et al. [7], proposed a structure-based algorithm that assigns globally unique IDs to sensor nodes. The assumptions for implementing the Structure-based ID Assignment for WSN are the nodes in a sensor network are usually manufactured in batches and neighbour node IDs must be stored in the memory of the sensor node during all its lifetime. In order to assign globally unique IDs to each node, their algorithm divided the proposed ID assignment scheme into two parts: Parent grouping algorithm and Children grouping algorithm. They assign globally unique IDs to each node while they build groups. Firstly, Parent grouping algorithm takes roles of building core group and assigning IDs to neighbor nodes from the sink node. In order to expand children groups, these assigned IDs are working as a message forwarder. Children grouping algorithm takes roles of building expanded groups and assigning ID globally. In each group, sink node sets a header node as a sub-sink node to broadcast messages and collect information instead of the sink node. The proposed algorithm aims at assigning globally unique IDs to each node by using two grouping algorithms. Through these two grouping algorithms, it structures two levels of groups. In each group, headers take roles of sink and it assigns neighbors' IDs instead of sink node. Sink node cannot only easily assign IDs to all other nodes via header nodes but also save the energy consumption up to 25%.

In [8]**,** in their paper studied the WSN and gives comparison and classification of Routing Techniques in Wireless Ad Hoc Networks. They define the Wireless ad hoc network as a collection of mobile nodes forming a temporary network without the aid of any centralized administration or standard support services regularly available on conventional networks. It differs from the infrastructure-based network by not having base stations to rely on but the network achieves connectivity by using an adhoc routing protocol. Absence of any fixed infrastructure pose number of different problems to this area. Some of the challenges that require standard solutions include routing, bandwidth constraints, hidden terminal problem and limited battery power. This paper present a comprehensive review for routing features and techniques in wireless ad hoc networks. For more than a dozen typical existing routing protocols, they compare their properties according to different criteria, and categorize them according to their routing strategies and relationships. Their paper discussed various criteria for classifying routing protocols and provided comparisons of more than a dozen routing protocols for wireless ad hoc network. There are still many challenges facing wireless ad hoc networks. However, because of their inherent advantage wireless ad hoc networks are becoming more and more prevalent in the world

P. Jiang1 et al. [9], gives a short overview of recent routing protocols for sensor networks and presents a classification for the various approaches. The four main categories studied in their paper are data-centric, hierarchical, location-based, and network flow and QoS-aware. Then, the existing hardware research platforms are explored as well as the software platforms such as simulation and development tools. Although the performance of these protocols is promising in terms of energy efficiency, further research would be needed to address issues such as Quality of Service (QoS). Another interesting issue for routing protocols is the consideration of node mobility. New routing algorithms are needed in order to handle the overhead of mobility and topology changes in such energy

constrained environment. Since the routing requirements of each environment are different, further research is necessary for handling these instances.

In [10], summarized recent research results on data routing in WSN and classified the approaches into three main categories, namely data-centric, hierarchical and location-based. Few other protocols followed the traditional network flow and QoS modeling methodology. Their study also observed that there are some hybrid protocols that fit under more than one category. The most interesting research issues in their study related to routing protocols for WSN are how to form the clusters so that the energy consumption and contemporary communication metrics such as latency are optimized, the consideration of node mobility, and integration of WSN with wired networks (i.e. Internet).

V. CONCLUSION

The aim of this paper is to study the problem of key Assignment and their possible solution in WSNs. To ensure adequate coverage and fault tolerance in inhospitable operating conditions, researchers envision these sensor networks to be comprised of a very large number of nodes, ranging from hundreds to several thousands. This large network size not only prohibits manual setup of the network, necessitating autonomous operation, but also eliminates the option of battery replacement. Therefore, to ensure a sufficient network lifetime, all network protocols must be designed with an extreme focus on energy efficiency. This has indeed been considered as the single most important design challenge in WSN algorithms.

REFERENCE

[1] H. Zhou, M. W. Mutka, and L. M. Ni, "Reactive ID Assignment for Sensor Networks," In International Journal of Wireless Information Networks Springer Media, Vol. 13, No. 4, pp. 317-328, October 2006 .

[2] C. Schurgers, G. Kulkarni, and M. B. Srivastava, "Distributed On-demand Address Assignment in Wireless Sensor Networks," In Proceedings of IEEE Transactions on Parallel and Distributed Systems, Vol.13, pp. 1056-1064, October 2002.

[3] C. Schurgers, G. Kulkarni, and M. B. Srivastava, "Distributed Assignment of Encoded MAC Address Assignment in Wireless Sensor Networks," In Proceedings of the 2nd ACM international symposium on Mobile ad hoc networking & computing USA, pp. 295 – 298, October 2001.

[4] E. O. Ahmed, D. M. Blough, B. S. Heck and G. F. Riley, "Distributed Unique Global ID Assignment for Sensor Networks," In Proceedings of IEEE International Conference on Mobile Ad-Hoc and Sensor Systems, Vol. 7, pp. 1-23, November 2005.

[5] C. Intanagonwiwat, R. Govindan, D. Estrin, and J. Heidemann, "Directed Diffusion for Wireless Sensor Networking," In Proceedings of IEEE/ACM Transactions on Networking, Vol. 11, pp. 1-15, February 2003.

[6] J. H. Kang, M. Park, "Structure-based ID Assignment for Sensor Networks," In International Journal of Computer Science and Network Security, Vol. 6 No.7B, pp. 158-163, July 2006.

[7] D. Estrin, J. Heidemann, and S. Kumar, "Next century challenges: Scalable coordination in sensor networks," In Proceedings of the ACM/IEEE International Conference on Mobile Computing and Networking, pp. 263–270, 1999.

[8] P. Jiang, Y. Wen, J. Wang, X. Shen, and A. Xue , " A Study of Routing Protocols in Wireless Sensor Networks," In IEEE, Vol. 1, pp. 266-270, June 2006.

[9] K. Akkaya , M. Younis , "A Survey on Routing Protocols for Wireless Sensor Networks," In Elsevier, Vol. 3, pp. 329-345, May 2005.

[10] S. Dai, X. Jing, L. Li, " Research and Analysis on Routing Protocols for wireless sensor networks," In IEEE, Vol. 1, pp. 407-411, May 2005.