Comparative Evaluation of Id Assignment Strategies in Wireless Sensor Network

Gautam
Department of Computer Science Engineering
Swami Devi Dyal Institute of Engineering & Tech. Panchkula (Haryana), India

Rubble Tayal
Department of Computer Science Engineering
Swami Devi Dyal Institute of Engineering & Tech. Panchkula (Haryana), India

Shanu Malhotra
Department of Computer Science Engineering
Institute of Science and Technolgy, Ambala (Haryana), India

Abstract

Wireless Sensor Networks (WSNs) are dense wireless networks of small, low-cost sensors, which collect and disseminate environmental data. WSNs facilitate monitoring and controlling of physical environments from remote locations with better accuracy. They have applications in a variety of fields such as environmental monitoring, military purposes and gathering sensing information in inhospitable locations. Sensor nodes have various energy and computational constraints because of their inexpensive nature and ad-hoc method of deployment. The main emphasis in this paper is to study the methods and techniques by which we can preserve more power by means of delaying ID conflict resolution until necessary in WSN. It has no requirement on apriori unique IDs of the sensor nodes, and is easy to integrate with the directed diffusion communication paradigm. In this thesis work, all the nodes in the WSN will be assigned using random ID and global ID assignment so that they will be uniquely identified in the WSN. These IDs are then treated as the network addresses of the nodes.
Keywords: WSN, MAC, IEEE, SMAC, 802.11

I. INTRODUCTION

Wireless Sensor Networks (WSNs) consists of numerous tiny sensors deployed at high density in regions requiring surveillance and monitoring. These sensors can be deployed at a cost much lower than the traditional wired sensor system. A typical sensor node consists of one or more sensing elements (motion, temperature, pressure, etc.), a battery, and low power radio trans-receiver, microprocessor and limited memory. An important aspect of such networks is that the nodes are unattended, have limited energy and the network topology is unknown. Many design challenges that arise in sensor networks are due to the limited resources they have and their deployment in hostile environments.

WSN has a great ability of obtaining data and it can work under any situation, at any time, in any place, which makes it useful in many important fields. So, the military department, industrial circle and academic circle of many countries all over the world are paying great attention to it. It also becomes a hot issue in research at home and abroad today, and it is regarded as one of the ten influencing technology in the 21st century [1].

A. Wireless Sensor Networks (WSNs):

Wireless sensor networks have emerged as one of the first real applications of ubiquitous computing. Sensor networks play a key role in bridging the gap between the physical and the computational world by providing reliable, scalable, fault tolerant and accurate monitoring of physical phenomena. A Wireless sensor network is defined as being composed of a large number of nodes, which are deployed densely in close proximity to the phenomenon to be monitored. Wireless sensor networks (WSNs) communicate via a radio interface instead of being wired to a control station.

Sensors themselves are normally not equipped with a radio interface. Therefore, a simple signal processor and a radio are packaged together with one or more sensors into what is called a wireless sensor node.

As shown in Figure 1 many sensor nodes are scattered in a sensor field and each of these nodes collects data and its purpose is to route this information back to a sink [2]. The network must possess self-organizing capabilities since the positions of individual nodes are not predetermined. Cooperation among nodes is the dominant feature of this type of network, where groups of nodes cooperate to disseminate the information gathered in their vicinity to the user [3].

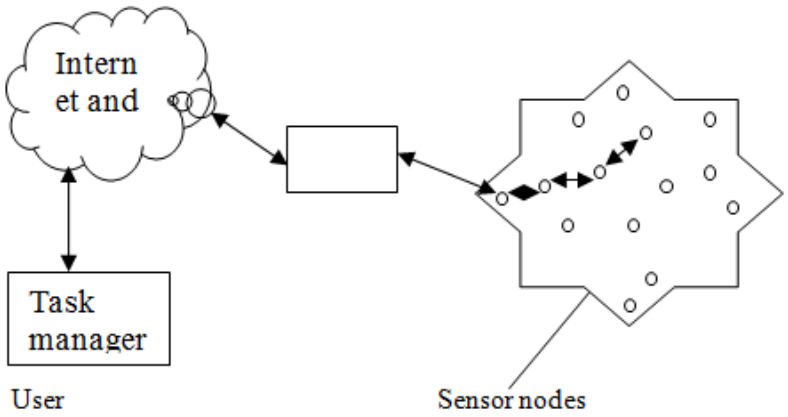

Fig. 1: Sensor Nodes Scattered In a Sensor Field

B. General Wireless Sensor Node Architecture:

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 node is, as shown in figure 1.2. In addition to regular sensor nodes, a WSN can contain one or more sink nodes (base stations). 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.The microcontroller/microprocessor performs the data processing, thereby significantly reducing the total number of data bits transmitted over the wireless medium. The radio interface comprises the radio transceiver with power control. Increased transmission power results in smaller probability of dropped packets at the receiver, but at the same time it increases the interference with other nodes in the transmission range. Therefore, intelligent polices for power adjustment at the node need to be considered.

Different types of sensors can be attached to the node through the sensor interface. Since many sensors have analog output, an additional A/D circuit may be needed to bridge the gap between the sensor and the node.These different elements of wireless sensor nodes are as follows.

1) Sensing Unit:

The Sensing unit consists of one or more sensors attached to a particular node. Each wireless sensor node is defined by the type of data it can collect, such as a temperature, humidity, thermal, seismic, visuals etc. Each wireless sensor senses one or more objects. A sensed object can either be a physical object such as a moving target, or it can be the environment of the sensor node, which might be the case when sensing temperature. When sensing a real object, meaningful data can be collected only if the sensed object is within the sensing range of the specific sensor. The wireless sensor can be in one of two states: active or inactive. The change between these two states is controlled by the application (running on the computing unit). When active, the sensor is constantly collecting data at a fixed sensing rate.

2) Communication Unit

The communication unit is in charge of relaying sensed data to the sink node and other sensor nodes when needed. The energy consumption of the communication unit depends on several factors. These include the modulation scheme, the data rate, the transmission distance and the operational mode. A communication unit can operate in several modes. The number and composition of these modes can vary from platform to platform like active, idle, and sleep. The last two modes imply constant power consumption. A constant power is also consumed during a change of operational mode. The communication energy consumption can be described in terms of transmit and receive consumptions. The transmit energy consumption depends on the transmission range and the energy consumed in the transmission circuitry. Furthermore, both transmit and receive energy consumptions depend on the message size.

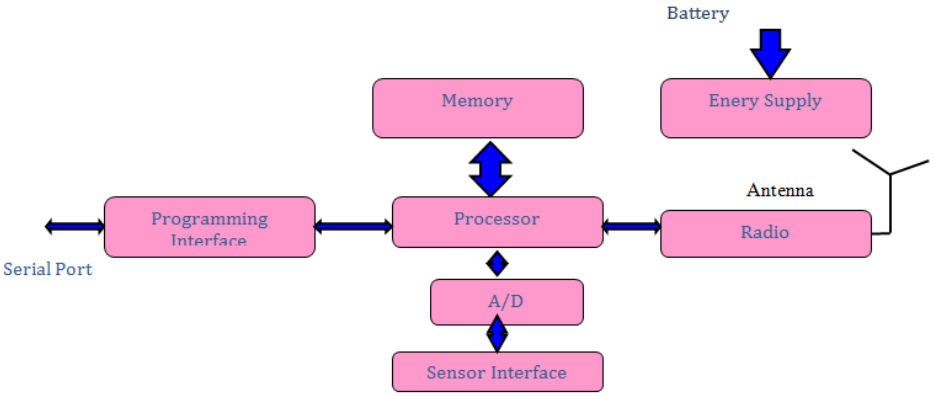

Fig. 2: General Architecture of a Wireless Sensor Node

3) Computing Unit:
The computing unit consists of a micro-controller unit, which runs the set of applications. It controls the sensing unit, performs the signal processing and executes the communication protocol. An application is attached to each sensor node. This application can request a sensor to activate or deactivate itself and can change the rate at which sensed data is collected. Another role of the application is to model any necessary processing on sensed data before sending it to other nodes in the network. It also receives and processes messages from other nodes. These messages can contain sensed data, for example when neighboring nodes aggregate their sensed data before sending a common message to the base station. Nodes can exchange other types of messages such as messages related to collaborative reconfiguration, self-initialization or cluster formation and cluster-head election.
4) Battery:
The battery is modeled as an energy reservoir initially with a fixed amount of available joules. The remaining energy of the battery is updated (reduced) every time whenever an activity that consumes energy occurs. These activities includes sensing, processing, transmitting, or receiving. Every time the remaining energy is updated, the node lifetime is also updated by adding the time since last update. The node lifetime is measured as the time since the node starts i.e. the node creation in the simulator or the node first activation.
5) Sink Node
The base station has all the components of a regular sensor node except the sensing unit and the battery. It is in charge of gathering the sensed data from sensor nodes. It also keeps track of the network lifetime. The network lifetime here is defined as the amount of time during which the network has been able to accomplish its tasks (for example collecting and relaying to the base station certain type of sensed data

II. ID 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. ID assignment solution should produce the shortest possible addresses because WSN are energy-constrained. 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 ID assignment technique 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 $l > \log_2 (4\pi dr^2)$.

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.

We can use an example to illustrate how to combine No ad hoc routing protocol with conflict resolution in ID assignment. For the small network in Figure 4, suppose that node A is the sink, node B is the source. Nodes A and B choose the same random address of a1, nodes C and D choose the same random address of a2. There are duplicate addresses among direct neighbors A and B, and among 2-hop neighbors C and D. Because all the addresses are randomly chosen and no communication has occurred yet, a node is not sure if its address is 1-hop unique, so it can use the address only temporarily. When the sink node broadcasts an interest message, the node can eliminate duplicate addresses among its direct neighbors because the receiver can choose another address randomly if it receives a packet with the same address. Once the sink node A broadcasts the interest message, node B must change its address (to a3, for example). This applies to other nodes when the interest packet is forwarded. After nodes C and D forward the message, node A will receive the same message with the same source address twice. Thus, node A will be aware that there are two direct neighbors with the same address. Node A can unicast a special control message (RESOLVE message) to notify them that there exists a 2-hop conflict. On receipt of the RESOLVE message from node A, both node C and node D need to change to another random address. If nodes C and D unfortunately choose the same address again, or choose the new address of node B (a3), there will still be a 2-hop conflict. To prevent the conflict, we require that nodes C and D broadcast an announcement of their changes (CHANGE message), which can be collected and checked by their neighbors. Because the locally unique ID is used in the construction of the path between the sink and source, a mechanism is necessary to identify the origin of the change message.

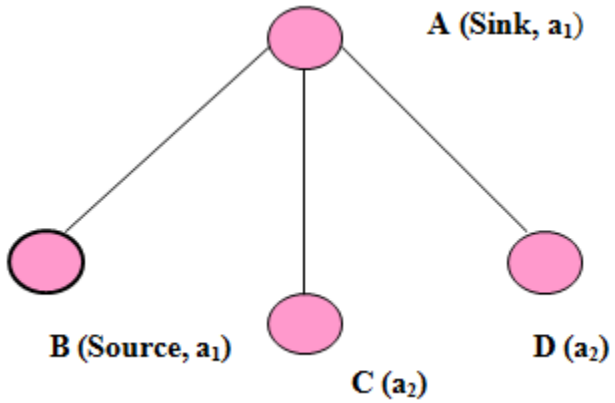

Fig. 3: A Small Sensor Network.

As illustrated in Figure 4.2, 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?

A. Procedure for ID assignment in WSN:

- In the beginning, every node chooses a random ID.
- The sink node broadcasts an INTEREST message.
- 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).
- The neighbor waits for a random delay and rebroadcasts the INTEREST message.
- 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).
- 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).
- 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).
- On receipt of a CHANGE message, a node updates its next hop back to the sink, if necessary.

B. The Impacts of Packet Loss:

Since there are only three kinds of packets utilized in ID conflict resolution, it is easy to analyze the impacts of packet loss.

1) INTEREST Message:

In case that a copy of the INTEREST message is lost, some conflicts may still exist. However, they will not prevent the transmission of reply messages, and will be resolved during the next data communication, as illustrated in Figure 4.4.

In Figure 5.4, there are a 1-hop conflict for nodes A and C, and a 2-hop conflict for node B. There are two cases for node B: it either has a separate path back towards the sink, or node A is the next hop along the path from node B to the sink. In either case, nodes A and C miss each other's
INTEREST message, and thus node C can only hear the INTEREST message from node B and \ Record node B as its upstream node. Once node C forwards the REPLY message from the source to node B, node B can send it back to the sink properly in the first case. In the second case, the REPLY message forwarded by node B will be received by both nodes A and C. Node A can send it back to the sink, node C just drops the duplicate REPLY message and waits for the next ID conflict resolution.

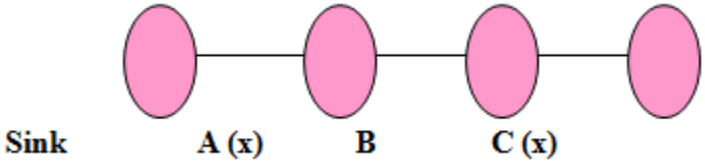

Fig. 4: An Example of 2-Hop Conflict.

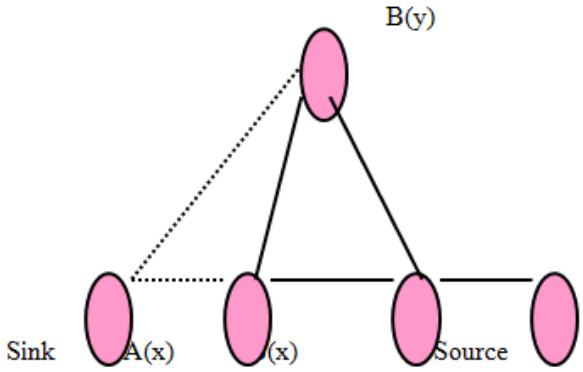

Fig. 5: An Example of Packet Loss.

2) RESOLVE Message:
In the case of the broadcast of the RESOLVE message, if one of the conflicting neighbors does not receive it, there will be no conflict. If neither/none receives it, then it is similar to the loss of INTEREST message as mentioned above.
3) CHANGE Message:
If a copy of the CHANGE message is lost, the path back towards the sink will be broken in the worst case. Thus, the changing node needs to keep its old address for some time, and notifies the sender of a reply message about the change if the reply message contains its old address. More mechanisms can be included to improve robustness of the scheme. For example, if a node finds there is a 2-hop conflict between its next hop and another neighbor, or it overhears a RESOLVE message that contains its next hop's address, it can set a timer waiting for receipt of a CHANGE message from its next hop. If the timer expires before it receives the CHANGE message, it can query the next hop for its new address.

III. RELATED WORK

In [1], 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. [2], 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 given below:

- The nodes in a sensor network are usually manufactured in batches.
- Neighbour node IDs must be stored in the memory of the sensor node during all its lifetime.
- ID Assigned field is combined as 3 parts: Group ID, Section ID, and Node ID. (For example, assigned ID, 0123 means Group ID (01), Section ID (2), and Node ID (3)).
- The number of nodes in a group should be less than 9.

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 [3], 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. [4], 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 [5], 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).

In [6], a novel scheme for a MAC address assignment is proposed. The two key features in this approach are the exploitation of spatial address reuse and an encoded representation of the addresses in data packets. To assign the addresses, they proposed a purely distributed algorithm that relies solely on local message exchanges. Other silent features of this approach are the ability to handle unidirectional links and the excellent scalability of both the assignment algorithm and address representation. In typical scenarios, the MAC overhead is reduced by a factor of three compared to existing approaches.

IV. RESULTS AND DISCUSSION

In this paper, we evaluates how to assign the ID to sensor nodes in WSN. Compared with the number of payload packets, the number of overhead packets is small, if 1-hop and 2-hop conflicts are resolved during the first broadcast, and all the nodes are stationary, there is no increase on overhead during the second broadcast. The payload packets include both INTEREST messages and REPLY messages. The overhead packets include both CHANGE and RESOLVE messages. As the address range increases, the communication overhead decreases.
The performance comparison of Two ID assignment schemes under NOAH protocol for varying sensor network size is shown with the help of graphs in terms of remaining energy consumption, distinct event delivery ratio and number of collisions.

A. Strategy:

We vary the network size from 10 sensor nodes to 30 sensor nodes for a transmission range of 150m. We calculate the remaining energy, collision counts, and distinct event delivery ratio with respect to varying network density for 150 m.

Fig. 6: Remaining Energy Consumption for Global ID and Reactive Id Assignment

From figure 6, Energy consumption for Reactive id scheme is less for higher number of nodes where as higher for lower node density. However, energy consumption for the Global id scheme is better for lower node density.

From figure 7, distinct event delivery ratio for reactive id sometime is less than global id scheme. But overall this is less in reactive id assignment.

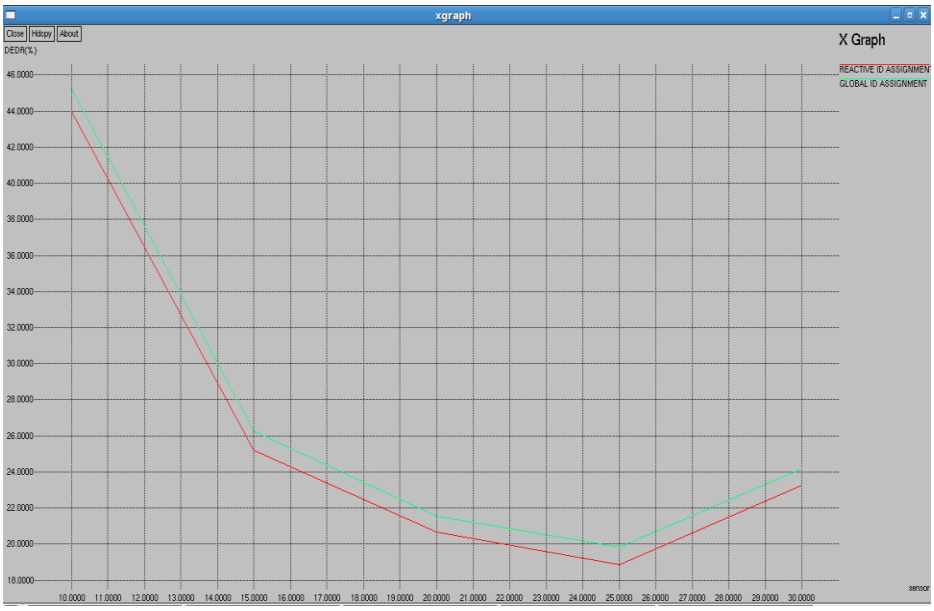

Fig. 7: Distinct-Event Delivery Ratio for Global ID and Reactive Id Assignment

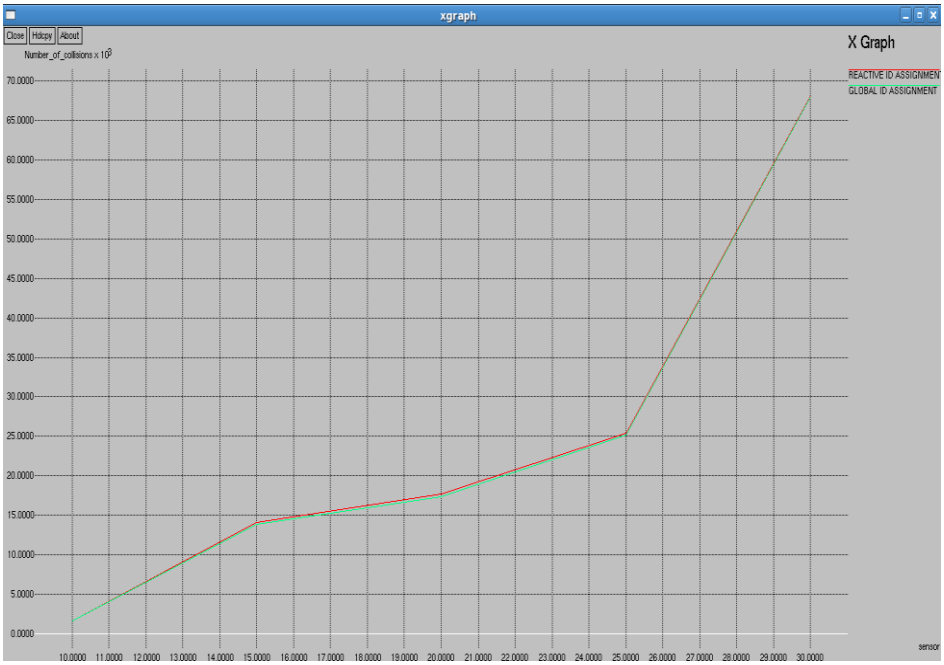

Fig. 8: Number of Collision Counts for Global ID and Reactive Id Assignment

V. CONCLUSION AND FUTURE WORK

In this paper, our main emphasis is to study the methods and techniques by which we can preserve more power by means of delaying ID conflict resolution until necessary in WSN. This thesis work assigns the random numbers as addresses to the nodes in WSN. It defers ID conflict resolution until data communications are initiated and thus saves remaining energy of the entire sensor network. The Remaining Energy is measured by the sum of energy remained for all the sensor nodes on the data transmission when IDs are assigned. As Simulation results show that the performance metrics of Global ID assignment schemes far outperforms the reactive ID assignment schemes when the network density is minimum.

Future work include the analysis of the performance of Global ID assignment in different on different parameters like total transmitting power, total receiving power and number of collision by varying packet-inter arrival period and number of hops.

REFERENCES

[1] 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.
[2] 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.
[3] 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.
[4] H. Zhou, M. W. Mutka, and L. M. Ni, "Reactive id assignment for sensor networks," In Proceedings of IEEE International Conference on Mobile Ad-Hoc and Sensor Systems, November 2005.
[5] K. Akkaya , M. Younis , "A Survey on Routing Protocols for Wireless Sensor Networks," In Elsevier, Vol. 3, pp. 329-345, May 2005.
[6] W. Qui, Q. Cheng, E. Skafidas, " A Hybrid Routing Protocol for wireless sensor networks," In International Symposium on Communications and Information Technologies , pp. 1383-1388, October 2007.
[7] 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.
[8] 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.
[9] 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.