A NEW SENSOR NETWORK PROTOCOL STACK ARCHITECTURE FOR CONGESTION CONTROL

Dr. Jasmine K.S., Babitha Naidu
Dept. of MCA, RVCE, Bangalore, India

ABSTRACT: A wireless sensor network is new technological advancement in wireless communication. Sensor networks are made up of hundreds or thousands of sensor nodes which are densely deployed in a remote environment with the capabilities of sensing, wireless communications and computations. Many different routing, power management and data dissemination protocols have been designed for wireless sensor networks. In this paper a study on layered protocol stack architecture for communication in sensor networks along with the various congestion control algorithms is discussed.
KEYWORDS: Protocol stack, Sensornet protocol layer, Congestion control, Flow control, Reliability.

1. INTRODUCTION

With the advent of new technologies in fast pace nowadays; becomes possible to significantly develop tiny and small size, low power, and low cost multifunctional sensor nodes. These nodes are capable of wireless communications, sensing and computation. Wireless sensor network is a combination of sensor techniques, embedded techniques, distributed information processing, and communication mechanisms.
Many applications are developed using sensor networks, most of these applications are custom made with no standardization in the protocols and a basic architecture that can be used for communication.
Since there is no basic architecture this enforces each developer to build each component in their application from scratch. If there is a common framework of integral components to be used, it would help save greatly in development and testing time since not everything has to be built from scratch every time.
To build a standard protocol architecture for communication in sensor networks:
Any protocol framework must be resource-aware. Thus the two main requirements of protocol architecture are:
(a) It should have a compostable framework
(b) It should be resource aware [A+02]
The basic architecture must be able to support multiple types of application needs of the user. Since sensor nodes run on battery, which cannot be replenished resources is a constraint, although it is very efficient, in terms of sensing, computation and communication.
Sensor networks lack in the communication activities of transmitting and receiving which take up most of the energy. So resource awareness should be inbuilt in the protocol architecture for efficient communication.
In the proposed architecture, we make a distinction between data and control packets in sensor networks.
We propose that in addition to having a protocol layering like the TCP/IP stack and a common layer like SP, segmenting the communication protocol architecture into a data and control plane is very essential to make best available use of resources in sensor networks. We make this distinction from the fact that there are huge differences in the requirements of control and data messages in sensor network communication. The basic difference is that data packets do not require as much of a reliability guarantee as control packets. Control packets on the other hand require a hard guarantee of reliable delivery [A+02].
We also observe that even for control packets sent by the one node of a sensornet, complete reliability in terms of that packet reaching all nodes in the network is not always necessary. For example, the sink node may just want to query the network and make sure that *at least* a required portion of the network is up. It Would be a waste of the network's resources if the query propagates the entire network, all the nodes which are up respond to the sink, and then the sink calculates whether the required number of nodes is up. In this regard, we introduce the concept of *semi-reliability* in sensor networks, wherein a node can choose to send a control message to only a part of the sensor network, and not to all nodes. This will be very useful in network management, where the sink can query parts of the network at a time to check if that part of the network is congested or not.

2. THE ARCHITECTURE OF THE PROTOCOL STACK FOR WIRELESS SENSOR NETWORKS

The architecture of protocol stack used by the sink (sensor base station) and sensor nodes. This protocol stack integrates power and routing awareness, integrates data with networking protocols communicates power efficiently through the wireless medium, and promotes cooperative efforts of sensor

nodes. Figure 1 depicts the layers of the architecture. This protocol stack is made up of physical layer, data link layer, network layer, transport layer, application layer, and power management plane, mobility management plane, and task management plane.

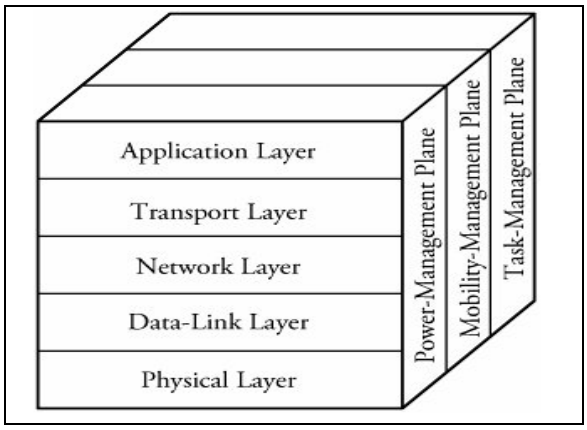

Fig. 1. Sensor networks protocol stack architecture

Functionalities of each layer in the architecture

Protocol stack: physical layer

- Frequency selection
- Carrier frequency generation
- Signal detection
- Modulation
- Encryption

Protocol stack data link layer

- Multiplexing of data streams
- Data frame detection
- Medium access
- Error control

Protocol stack: Network layer

- Power efficiency
- Data-centric nodes
- Data aggregation is not always desirable
- Attribute-based addressing and location awareness

Protocol stack: transport layer

- End-to-end reliability
- Multi-hop retransmission
- Congestion
- End-to-end security
- Like SSl: authentication, encryption, data integrity

Protocol stack: application layer

- Sensor network management
- Database queries
- Time synchronization/calibration

Power management plane

Manages how a sensor node uses its power and manages its power consumption among the three operations (sensing, computation, and wireless communications). For e.g., to avoid duplicated messages, a sensor node may turn off its receiver after receiving a message from one of its neighbors. Also, a sensor node broadcasts to its neighbors that it is low in power and cannot take part in routing messages. The remaining power is reserved for sensing and detecting tasks.

Mobility management plane

Detects and registers the movement/mobility of sensor nodes as a network control primitive. Hence a route back to the user is always kept, and sensor nodes can keep track of who their neighbors are. Therefore, the nodes can balance their power and task usage by knowing this situation [A+02].

Task management plane

Balances and schedules the events' sensing and detecting tasks from a specific area. Hence; not all of the sensor nodes in that specific area are required to carry out the sensing tasks at the same time. Depending on their power level, some nodes perform the sensing task more than others [A+02].

3. SENSOR NETWORKS PROTOCOL STACK ARCHITECTURE WITH SENSORNET PROTOCOL LAYER

Sensornet Protocol is a single hop broadcast protocol which is situated between the network and the link layer in the protocol stack [Ram**].

As any sensor network application is closely tied to the network layer routing protocols, the common layer of SP cannot be at the network layer. And similarly there are numerous link layer protocols and each Sensor-net application developer might prefer to be able to choose a protocol which will be best suited for the application. And the functionalities offered by the various link layers are widely varying in nature. SP is basically an interface between the network and the link layer abstracting the functionalities of the link layer and offering them as services to the network layer talks about how SP should be able to provide the network layer functionalities.

Figure 2 shows the network architecture with an SP layer.

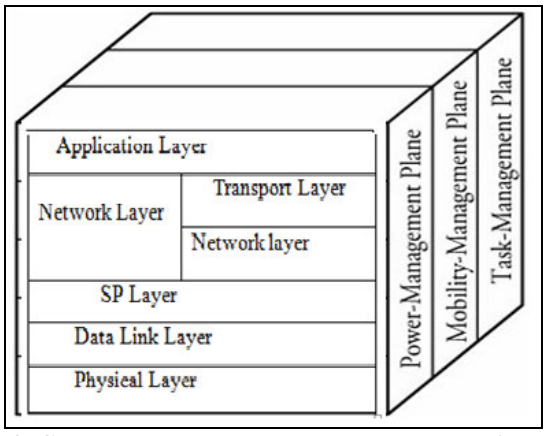

Fig. 2. Sensor networks protocol stack architecture with SP

In sensor networks there are two types of communications based on the messages carried.
The two types of messages are *data messages* and *control messages*.
Data messages are those messages which involve transfer of sensor data within the sensor network, data messages are used in all the applications.
Control messages are used to transfer configuration, topology detection, Neighbor discovery, route discovery, time synchronization, reprogramming, reliability and network management (such as congestion and flow estimation and recovery),control messages doesn't transfer sensor data.
When both data messages and control messages are compared control messages are important because loss of a control message by the sink (sensor base station) is expensive when compared to loss of sensor data. In general, more care should be taken in the reliable delivery of control messages. With regard to Reliability, reliable range of semantics must be present to take care of the control messages delivery.
Since sensor networks work on batteries inclusion of reliability to data messages is not feasible.
Control messages have a higher priority than data messages, so that even in a congested input queue in a node, control messages are given higher priority so that they are not dropped due to congestion or flow control.
Figure 2 shows the architecture of sensor networks after including the control / data plane abstraction. The data plane is the same as the architecture of figure 1. But the control plane has the network layer further divided into two sub layers namely network layer and transport layer, transport layer is added to take care of reliable data transmission of control messages, congestion control, and flow control. TCP was designed for wired networks since sensor networks are wireless networks lot of issues which are necessary for wireless networks are not included in TCP.

4. MAJOR ISSUES IN SENSOR NETWORK PROTOCOL STACK ARCHITECTURE

Congestion
The most predominant issue in Wireless Sensor Network is Congestion**.** There are many sources for congestion. They are buffer overflow, concurrent transmission, and packet collision. Congestion causes packet loss, which in turn reduces throughput and energy efficiency. Therefore congestion in WSN's needs to be controlled for high energy-efficiency, to prolong system lifetime, improve fairness, and improve quality of service (Qos) in terms of throughput (or link utilization) and packet loss ratio along with the packet delay. A WSN consists of one or more sinks and perhaps tens or thousands of sensor nodes scattered in an area.
Congestion restraint generally follows two steps:
Congestion detection and *congestion control.* In this paper we have stated various congestion control algorithms for wireless sensor networks.

4.1 Congestion Control for Wireless Sensor Network

The Congestion control algorithms prevent the network from entering Congestive Collapse. Congestive Collapse is a situation where, although the network links are being heavily utilized, very little useful work is being done.
These kinds of cases are being handled effectively by large number of algorithms.

1. *HMAC*

It gives proportional access, i.e. a node Carrying higher amount of traffic gets more access to the medium than others. Therefore, downstream nodes obtain higher access to the medium than the upstream nodes. This access pattern is controlled with local values and is made load adaptive to cope up with various application scenarios. The congestion process can be normalized when there is synchronization between upstream node and downstream node. To implement this we have to check whether sufficient buffer space is available at the downstream node [OMC06].

2. *Weighted Round Robin Forwarding (WRRF).*

This method avoids the packet to drop due to Congestion by not allowing upstream nodes to transmit if buffer full. This is been achieved by giving priority. The downstream node allows all the packets to be transmitted by the upstream nodes but all are not transmitted at the same time. For the first round some packets will be transmitted and likewise the process continues until the entire packet is been sent. This provides efficient method for controlling congestion [OMC06].

3. *In priority Based Rate Adjustment technique (PRA)*, when a notification for congestion is been made the rate is been limited accordingly. (i.e.) when congestion happens congestion notification bit which is used in AIMD gets information about how much decrease or increase in the rate for transmitting the packet has to be given so as to overcome the congestion [EB04].

4. *Short Term Congestion Control*

Is a method in which node experiences congestion, its immediate child node split the real time traffic on to its alternate parent (route) in a proportion to their

weight factor. This weight factor is solely depends on the end-to-end path delay from the alternative parent (route) node to the sink. This approach will eventually carry the newly created real time data flows at a slower rate along the primary route, allowing the congested node to be relieved and thus alleviate congestion.

5. *Long Term Congestion Control*
When a back pressure message reaches the source node it initiates Long-term congestion control. Source node sends Proportionate real time traffic as the similar way of short-term congestion control along its alternate routes (parents) based on their weight factor Moreover; source node dynamically adjusts to the changing conditions and selects the best node (parent) as its primary route to send further packets. As a result subsequently both the real time and non-real time data flows will follow the changed or updated primary route.

6. *Priority based Congestion Control node*
Priority index is introduced to reflect the importance of each node. It uses inter arrival time along with packet service time for detecting Congestion Degree and uses hop-by-hop control technique. It consists of key components such as intelligence control detection, implicit congestion notification and priority based rate adjustment technique [EB04]. Once a packet is sent it calculates the degree of congestion using the Congestion Degree formula [C+10] [WCK02]. This algorithm makes a notification about the occurrence of congestion. Thus occurrence of congestion will be announced to nearby nodes. By getting the notification each nodes will adjust rate of transmission so as to control congestion.

7. *Pump Slowly Fetch Quickly, PSFQ*
It takes a different approach and supports a simple, robust and scalable transport that is customizable to meet the needs of different reliable data applications. It is used to distribute data from a source node by pacing data at a relatively slow speed ("pump slowly"), but allowing nodes that experience data loss to fetch (i.e., recover) any missing segments from immediate neighbors very aggressively (local recovery, "fetch quickly"). In this case there is a possibility of getting packet to be lost. This can be made out by using a Negative ACK towards the source. Thus how the protocol provides control for congestion [ZNT07].

8. *Topology Aware Resource Adaptation (TARA)*
The capacity of a given topology is defined by the Maximum throughput (i.e. packet delivery rate) that can be observed by the sink(s). If there are no interferences between links, the capacity of a topology would be the same as the maximum throughput achievable by unlimited unidirectional transmissions in a one-hop topology. The interference between links makes the overall throughput much smaller than the one-hop capacity [HJB04].

9. *Light weight buffer management*
This is an effective approach that prevents data packets from overflowing the buffer space of the intermediate sensors. This approach automatically adapts the sensors' forwarding rates to nearly optimal without causing congestion. It gives how to implement buffer-based congestion control with different MAC protocols. In particular, for CSMA with implicit ACK [C+10].

4.2 Flow Control

Flow Control in sensor networks is not that much of a problem because of the scale of data which is being transmitted in it. In sensor networks the scale of data is usually very less compared to a wired network, since all the nodes have to transmit is the data they sense at regular intervals and control information occasionally.
Flow control also usually manifests as a congestion problem in the area surrounding the receiver, and it back propagates up to the sender, which can then reduce its reduce its transmission rate[Ram**].

4.3 Reliability

The problem of achieving reliable transmission between remote nodes over multiple hops despite Channel errors, collisions or congestion has at least the following dimensions:

i. Single packet vs. block of packets vs. stream of packets:

Transmitting a single packet or an infinite number of packets play an important role on the architecture. Reliable delivery of single packets can be important for example for highly aggregated data, reliable delivery of blocks is required for applications like disseminating new code or new queries into the network [HJB04] Transfer of data report in intervals is one of the examples of stream of packets.

ii. Guaranteed vs. stochastic delivery:

Applications that require guaranteed delivery. Examples are:
(i) Reporting of very important events from sensors to a sink node, (ii) the distribution of new code or queries from the sink node to sensors [ZNT07] or (iii) handing over the target state in a tracking application

between nodes close to the target trajectory [WCK02].

iii. Sensors-to-sink vs. sink-to-sensors vs. local sensor-to-sensor:

Communication in sensor networks does not take place between arbitrary nodes, but is either from
Sensor nodes to a single or a few sink nodes, from a sink to (groups of) sensors or locally between (groups of) sensors when these run collaborative signal processing algorithms.
There is no single protocol covering all the points in this design space (TCP is not doing this either), but several solutions have been developed for single points or small point sets.

5. CONCLUSIONS

In the sensor networks communication, there is a need to consider message data and control data, loss of control data is more critical than message data. Losing a control data will be more expensive, so control messages are given higher priority so that they are not dropped due to congestion or flow control. In the proposed architecture, the control plane has the network layer further divided into two sub layers namely network layer and transport layer, transport layer is added to take care of reliable data transmission of control messages, congestion control, and flow control. The paper also discusses various flow control mechanism which provides reliability in a multi-hop communication.

REFERENCES

[A+02] **I. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci** - *A survey on Sensor Networks,* in IEEE Communications Magazine, vol. 40, Issue: 8, pp. 102-114, August 2002.

[C+10] **Rekha Chakravarthi, C. Gomathy, Suraj K. Sebastian, Pushparaj K, Vinu Binto Mon** - *A Survey on Congestion Control in Wireless Sensor Networks*, in International Journal of Computer Science & Communication, Vol. 1, No. 1, January-June 2010, pp. 161-164

[EB04] **C.T. Ee, R. Bajcsy** - *Congestion Control and Fairness for Many-to-one Routing in Sensor Networks*, in Proc. ACM Sensys, Nov. 2004.

[Han04] **Rick Han** - *CSCI 7143 Secure Sensor Networks Fall,* in survey2_sensor Net overview.ppt, 2004

[HJB04] **B. Hull, K. Jamieson, H. Balakrishnan** - *Mitigating Congestion in Wireless Sensor Networks,* in Proc. ACM Sensys, Nov. 2004.

[OMC06] **Md. Obaidur Rahman, Muhammad Mostafa Monowar, Choong Seon Hong** - *A Qos Adaptive Congestion Control in Wireless Sensor Network,* in IITA, Nov. 2006.

[Ram**] **Siddharth Ramesh** - *A Protocol Architecture for Wireless Sensor Networks*, School of Computing, University of Utah, Salt Lake City, UT 841

[WCK02] **C.-Y. Wan, A. T. Campbell, L. Krishnamurthy** - Psfq: *A Reliable Transport Protocol for Wireless Sensor Networks. In Proc. of First ACM International Workshop on Wireless Sensor Networks and Applications,* (WSNA 2002), pages 1–11. Atlanta, September 2002.

[ZNT07] **Kang J. Zhang, Y. Nath, B. Tara** - *Topology Aware Resource Adaptation to Alleviate Congestion in Sensor Networks,* in IEEE Transaction on Parallel and Distributed Systems 18(7), 919–931 (2007).