An Energy Efficient Congestion Control Mechanism of WSN using Intelligent Agents

1H. Manikandan, 2S. Swaminathan, 2A. Srinivasan and 3H. Prabavathi
1CSE Department,
2ECE Department, Srinivasa Ramanujan Centre, SASTRA University, Kumbakonam, India
3CSE Department, AVC College of Engineering, Mayiladuthurai, India

Abstract: A Wireless Sensor Network (WSN) consists of one or more sinks and large number of sensor nodes scattered in an area. It is a collection of sensor nodes are interconnected by wireless communication channels. Wireless sensor networks will be used for such tasks as surveillance, widespread environmental sampling, security and health monitoring. With this data simple computations are carried out and communicate with other sensor nodes or controlling authorities in the network. Most of the time the sensor nodes are designed with limited energy, as a result the sensor nodes lacks recharging issues. But still wireless nodes packet-based computation is preferred since it is generally known that the computation utilizes reduced energy than the communication. In this study focus about to control the congestion and each node can achieve fair throughput whenever the congestion occurs in WSN environment. The congestion traffic is found in two streams, named downstream traffic and upstream traffic. The downstream traffic from the sink to the wireless sensor nodes is a one-to-many communication model. We present two general approaches to control congestion, network resource management and traffic control. The first approach tries to increase network resource to mitigate congestion when it occurs. The second approach tries for power control and multiple radio interfaces. It can be used to increase bandwidth and weaken congestion. When congestion occurs, the long-range radio is used as a more direct route or “siphon” to mitigate congestion.

Keywords: Congestion control, multi agents, wireless sensor networks

INTRODUCTION

Wireless sensor networks: The emerging trends in wireless accelerated the need for scalable and efficient network support. These applications include video conferencing, battle field, disaster management, etc. The traditional protocol in wired networks is extremely inefficient for such group based applications since related issues across the network to each receiver. In all these applications, communication and coordination among a given set of nodes are necessary. Wireless protocols play a vital role in mobile networks to provide this communication efficiently. Recent advances in micro-electro-mechanical systems technology, wireless communications and digital electronics have enabled the development of low-cost, low-power, multi functional sensor nodes that are small in size and communicate untethered in short distances. These tiny sensor nodes, which consist of sensing, data processing and communicating components, leverage the idea of sensor networks based on collaborative effort of a large number of nodes. With the integration of information sensing, computation and wireless communication, sensor nodes can sense the physical phenomenon, process the “raw” information, share the processed information with nearest nodes and report information to the sink. A WSN is a collection of sensors interconnected by wireless communication channels. Each sensor node is a small device that is capable of collecting data from its nearby surrounding area. With this data simple computations are carried out and communicate with other sensor nodes or controlling authorities in the network (Yuanzhu et al., 2006). Wireless communication is a major source of energy consumption in WSNs.

Routing decisions affect the number of transmissions, the distance covered per transmission and the load placed on the intermediate nodes that participate in relaying the messages. The study focused on common parameters of well-known cluster based routing protocols (Ahmed et al., 2011). Every packet transmitted in the wireless sensor networks contains useful information, which can be utilized through packet-based computation and to enhance congestion control. The wireless sensor network packet computation has small packet forwarding rate and the forwarding computation capability is limited. In this study proposes an approach to control the congestion in WSN by using intelligence agents.

Characteristics of WSN: A Wireless Sensor Network (WSN) consists of one or more sinks and large number of sensor nodes scattered in an area. With the integration of information sensing, computation and
wireless communication, sensor nodes can sense the physical phenomenon, process the “raw” information, share the processed information with nearest nodes and report information to the sink. The downstream traffic from the sink to the sensor nodes usually is a one-to-many multicast. The upstream traffic from sensor nodes to the sink is a many-to-one communication. The upstream traffic can be classified into four categories: event-based, continuous, query based and hybrid. In event-based delivery, a sensor node does event reporting if and only if target events occur. The sensor data for the event usually has very small size. Sensor nodes may need to periodically report to the sink and generate continuous data transmission in some cases. This is a continuous delivery. In query-based delivery, sensory data is stored inside network and is queried by and then transmitted to the sink on demand. At each node, an estimation of the number of downstream motes is made and the bandwidth is split up proportionally between locally generated and route-through traffic. The resulting bandwidth allocation is approximately fair. The reduction in transmission rate of route-through traffic has a backpressure effect on downstream motes, which can then reduce their generation rates (Alec and David, 2001).

There two types of congestion could occur in WSNs. The first type is node-level congestion that is common in conventional networks. It is caused by buffer overflow in the node and can result in packet loss and increased queuing delay. Packet loss in turn can lead to retransmission and therefore consumes additional energy. For WSNs where wireless channels are shared by several nodes using CSMA like (Carrier Sense Multiple Access) protocols, collisions could occur when multiple active sensor nodes try to seize the channel at the same time. This can be referred to as link-level congestion. Link-level congestion increases packet service time and decreases both link utilization and overall throughput and wastes energy at the sensor nodes. Both node level and link-level congestions have direct impact on energy efficiency and QoS (Ali and Rahmani, 2008). Therefore congestion must be efficiently controlled. Congestion control protocol efficiency depends on how much it can achieve the following objectives:

- To improve the energy-efficiency requires extending system lifetime. Therefore congestion control protocols need to avoid or reduce packet loss due to buffer overflow and remain lower control overhead that consumes less energy.
- It is also necessary to support traditional QoS metrics such as packet loss ratio
  - Node-level congestion
  - Link-level congestion, packet delay and throughput. For example, multimedia applications in WMSNs require not only packet loss guarantee but also delay guarantee
- In this study fairness needs to be guaranteed so that each node can achieve fair throughput

Most of the existing work guarantees simple fairness in that every sensor node obtains the same throughput to the sink. In fact, sensor nodes might be either outfitted with different sensors or geographically deployed in different place and therefore they may have different importance or priority and need to gain different throughput. Therefore weighted fairness is required.

The proposed method avoids overprovided resource or under-provided resource to guarantee precise and exact network resource adjustment in order. However this is a hard task in wireless environments. Unlike the approaches based on network resource management, traffic control implies to control congestion through adjusting traffic rate at source nodes or intermediates nodes. Another proposed approach is helpful to save network resource and more feasible and efficient when exact adjustment of network resource becomes difficult.

**Congestion control:** The important issues that happen in WSN is the congestion. Congestion may occur due to the many factors like buffer overflow, packet collision, concurrent transmission, etc. Due to congestion, the throughput and efficiency of the network may be reduced. Therefore congestion in the sensor network has to be controlled to obtain high efficiency, to improve fairness, to improve the QoS in terms of throughput and to reduce the packet loss ratio and the delay in the network.

**Properties of congestion control:** The congestion control schemes have number of properties. They are:

- Ability to deal with heterogeneity
- Ability to deal with ill-behaved source
- Scalability
- Stability
- Simplicity
- Fairness

**WSN congestion control mechanism:** Due to shared nature of wireless medium, all sensor nodes contend for medium access. Congestion occurs when the traffic exceeds a network capacity. When congestion occurs, packets are dropped either because of collision or buffer overflow.

There are many reasons which lead to a packet being dropped, such as, when two nodes are trying to send packets to the same node at the same time. Here a node tries to send data to another node when a third node which is out of range of the first node tries to send data to that same node. RTS/CTS implementation solves this problem but also creates another problem called exposed terminal problem. Here a node will
assume that the channel is busy by hearing a CTS packet when it can potentially send data to another node out of range of the sending node. Also another problem exists in wireless sensor network called overhearing. Here, a node receives packets which are not intended to be sent to that node (Charalambos and Vasos, 2011).

**WSN architecture:** Wireless networks deliver a lower bandwidth than wired networks; the mobility of hosts which causes topological changes of the underlying network also increases the network information. The limitation of power also leads the user to disconnect mobile unit frequently to save power (Sklar, 2001). The transport layer routing, which uses the TCP and transport connections in wireless networks are plagued by problems such as high bit rate, frequent route change and partitions (Black, 1999). While running the wireless protocol over such networks, the throughput of the connection is viewed to be poor, because this protocol takes the lost or delayed acknowledgements as congestion. The wireless transmission protocol needs more effective mitigation strategies. The effect of channel conditions on the wireless protocols performance should be overcome and there is a need to provide a robust, flexible protocol that consistently gives high performance for a variety of network environments. In this study, the performance of the wireless protocol is improved when multi agents are implemented along with the existing wireless protocol.

**Intelligent agent:** An intelligent agent is a software entity which carries out operations for the account of the user or for another program with some degree of freedom and autonomy and which exploits knowledge or representations of the desires and the objectives of the user (Gilbert et al., 1995). An intelligent agent is an autonomous entity which observes and acts upon an environment and directs its activity towards achieving goals. Intelligent agents may also learn or use knowledge to achieve their goals. This may be very simple or very complex: a reflex machine, such as a thermostat, is an intelligent agent, as is a human being, or a community of human beings working together towards a goal. Intelligent software agents have a collection of properties that make them very adequate to provide services to citizens.

Agents and Multi-Agent Systems (MASs) are more successfully deployed, even if many theoretical issues underlying them remain unexplored. The lack of rigorous formal definitions and characterizations of agent hood and the unclarity or even disagreement about what constitutes MAS; make the gap between theory and practice quite evident. The proposed system classification is meant to be theoretically comprehensive, while providing an agent designer with a practical means to choose a system that is appropriate for the task at hand. The analysis of agent systems focuses on aspects such as distribution, concurrency and security. In shifting from a comprehensive viewpoint to a narrower focus, the idea is to highlight a niche in the “agent system space” that is not currently filled by existing systems. The system classification used to restrict the possible criteria while establishing a list of features is fairly simple-differentiating between systems that facilitate the design and implementation of individual agents and those that take a more system-oriented view (i.e., concentrate on systems composed of many agents). The distinction between the Single Agent System (SAS) and MAS system implementation often displays some functional overlap; an agent system may be geared towards providing a framework in which agents interact, while also providing agent architecture or templates.

**Multi-agent model:** A multi-agent model is a dynamic federation of agents connected by the shared environments, goals or plans and which cooperate and coordinate their actions (Huhns, 1999). The capacity to communicate, to coordinate and to cooperate makes interesting the use of multi-agents in the communication environments.

An agent as “a computer system and is situated in some environment that is capable of autonomous action in this environment in order to meet its design objectives”. An agent system is shown in Fig. 1. An agent will not have complete control over its environment, in most domains of reasonable complexity. It has partial control, in that it can influence its environment. This means that from an agent’s point of view the same actions performed twice in apparently identical circumstances, might appear to have entirely different effects. A MAS is any system that contains:

- Two or more agents
- At least one autonomous agent
- At least one relationship between two agents where one satisfies the goal of the other
The typical structure of MAS consists of a number of agents that interact with one another through communication. The agents have the ability to act in an environment and have different “spheres of influence”. This means the control over or ability to influence different parts of the environment. In some cases these “spheres of influence” may overlap or coincide. This gives rise to dependency relationships between the agents. Agents will also be linked with each other by other relationships.

SYSTEM ARCHITECTURE

WSN is an autonomous, distributed, multi-hop and wireless network which performs critical tasks with nondeterministic routes over a set of possibly heterogeneous node architectures (Salim and Abdelhamid, 2011). WSN has one or more sinks and great number of wireless sensor nodes spotted in a small area. Congestion in WSN can cause missing packets, low energy efficiency and higher delay. Applications like image, video and multimedia need to transmit huge quantity of information from different wireless sensor nodes (Liqiang and Fengqi, 2009). Therefore congestion control is an important problem in the above said applications.

Upstream congestion control: Congestion is an important problem in WSN. The congestion not only wastes the scarce energy due to a large number of retransmissions and packet drops, but also hampers the event detection reliability (Fig. 2). Congestion in WSN has a direct impact on energy efficiency and application QoS (Mohammad and Donald, 2008). Congestion will cause packet loss and also leads to too much energy consumption. Hence the congestion in WSN has to be controlled in order to increase the system lifetime.

The congestion traffic in WSN can be classified into two named; downstream traffic and upstream traffic. Downstream traffic occurs in the communication network where the data is transferred from the sink node to the wireless sensor nodes. This can be considered as one-to-many multicast communication. Upstream traffic occurs in the communication network where the data is transferred from the wireless sensor nodes to the sink node. This can be considered as many-to-one communication.

The downstream traffic is diverging in nature, so the probability of congestion in this approach is less. But upstream traffic is converging in nature, so probability of getting congestion in the upstream traffic is more. Moreover, upstream network model have high bit rate than the downstream communication. Therefore the high speed upstream network model has more congestion than the downstream. Therefore congestion must be efficiently controlled. The efficiency of the

![Flow chart for congestion control](image)

Fig. 2: Flow chart for congestion control
Congestion Control with Fairness (CCF): CCF is a distributed and scalable algorithm that eliminates the congestion within a sensor network and ensures the fair delivery of packets to a sink node (Cheng and Ruzena, 2004). CCF is designed to work with any MAC protocol in the data-link layer. CCF uses packet service time to deduce the available service rate. Congestion information is implicitly reported. It controls congestion in a hop-by-hop manner and each node uses exact rate adjustment based on its available service rate and child node number. CCF guarantees simple fairness. CCF has two problems (Ren et al., 2003). The rate adjustment in CCF relies only on packet service time which could lead to low utilization when some sensor nodes do not have enough traffic or there is a significant packet error rate. Moreover, it cannot effectively allocate the remaining capacity and as it uses work conservation scheduling algorithm, it has a low throughput in the case that some nodes do not have any packet to send.

Congestion control algorithm: The CCF congestion control algorithm has the following steps to be executed at each node in every control interval:

Step 1: Measure the average rate (rout) at which the packets are sent from the node, the average aggregate input rate (rin) and the minimum number of packets in the output queue which is seen by an arriving packet in a control interval (Q).

Step 2: Based on the difference between rout and rin and Q, compute Δr. This is the total change in aggregate traffic:

\[ \Delta r = \alpha (rout - rin) - \beta (Q/\gamma) \]

Step 3: Assign Δr into individual flows to achieve fairness.

Step 4: Compare the bandwidth computed for each flow with the bandwidths. Use and propagate the smaller rate upstream.

Design architecture: The problem of single-path upstream congestion control in wireless sensor networks through the traffic control is proposed by introducing a new multi-agent system based approach to control the traffic in the upstream congestion. The traffic generated in a wireless sensor node is of two types named, source traffic and transit traffic. The source traffic is generated from each wireless sensor node and the transit traffic is generated from other wireless sensor nodes.

A Reusable Task-based System of Intelligent Networked Agents (Cooperative Distributed Problem Solving) is a cooperative multi-agent system that consists of three classes of agents: interface agents, task agents and information agents. Cooperative Distributed Problem Solving provides a domain-independent, componentized and reusable substratum to:

- Allow heterogeneous agents to coordinate in a variety of ways
- Enable a single agent to be part of a multi-agent infrastructure (Chieh-Yih et al., 2003, Chih-Kuang et al., 2011)

Cooperative Distributed Problem Solving provides facilities for reuse and a combination of different existing low-level infrastructure components and it also defines and implements higher level agent services and components that are reconfigurable and reusable.

An upstream congestion control model by using Cooperative Distributed Problem Solving Protocol (CDPSP) is proposed. CDPSP reduce the packet loss by its intelligent scheduling schemes. CDPSP consists of four components: Execution Monitor, Communicator, Planner and Scheduler.

The four modules of Cooperative Distributed Problem Solving multi-agent are implemented for the upstream congestion control as autonomous threads of control to allow concurrent planning and scheduling actions and execution in an efficient way. Furthermore, all modules are executed as separate threads and are able to execute concurrently. So almost all the packets are forwarded to the next wireless sensor node without any loses.

SIMULATIONS

All simulations are performed using Network Simulator-2 (NS-2), a network simulator that provides support for simulating wireless networks. The simulations were carried out on a wireless network environment in following three different scenarios. (A wireless environment consisting of 50, 100 and 250 wireless sensor nodes). In the wireless network environment all the wireless sensor nodes are roaming over a simulation area of 800×800 m flat space operating for 600 sec of simulation time. Each node has a radio propagation range of 200 m and channel capacity 2 Mb/s. The mobility of different levels is obtained by changing the maximum node speed with a pause time of 1 sec. The sensing node in WSN is usually stationary or moves with a walking speed of about 1 m/s. The simulation model bandwidth is normalized to 10 and in an ideal case each sensor node might receive a throughput of 0.1667 approximately.

The performance of the proposed CDPSP is evaluated and compared with the CCF protocol. CCF is
used as a distributed and scalable algorithm to eliminate congestion within a sensor network and ensures the fair delivery of packets to the sink node. CCF guarantees simple fairness and has the following two major problems (Chih-Min and Yi-Wei, 2010):

- The rate adjustment in CCF depends on packet service time that lead to low utilization when some sensor nodes do not have enough traffic.
- Also, this cannot effectively allocate the remaining capacity and uses work-conservation scheduling algorithm.

Performance evaluation: In these simulations, different wireless environment scenarios are used, with a varying scale of mobility. The following metrics are used in comparing the protocol performance:

- Throughput
- Latency
- Protocol overhead
- Jitter

Throughput: Throughput is defined as the ratio of average rate of successful message delivery over a communication channel. This ratio represents the routing effectiveness and throughput of the routing protocol in delivering data to the intended sink within the network.

Latency: Network latency is a measure of how fast a network is running. It refers to the time between the transmissions of data packets from a multicast source and the time of its reception by a multicast receiver. Latency is the delay between the initiation of a network transmission by a sender and the receipt of that transmission by a receiver. In a two way communication, it may be measured as the time from the transmission of a request for a message, to the time when the message is successfully received.

Protocol overhead: Protocol packet overhead is the ratio of the number of protocol packets originated or forwarded, related to the route creation process that are received by a node per data delivery. This metric indicates the percentage of the total protocol messages transmitted for data forwarding.

Jitter: Jitter is often used as a measure of the variability over time of the packet latency across a network. A network with constant latency has no variation (or jitter). Packet jitter is expressed as an average of the deviation from the network mean latency.

SIMULATION ANALYSIS

Throughput: From the graph, it is seen that CDPSP has better throughput than the other CFF protocol and on an average, above 92.23% of the packets have been delivered to the destination successfully in the proposed protocol. It is also seen that CDPSP is always 2-3% better than CCF during the entire simulation (Fig. 3). As said earlier, CDPSP has better throughput than the other CFF protocol and on an average, above 91.02% of the packets have been delivered to the destination successfully in the proposed protocol. The performance of the throughput degrades when the simulation time increases as more numbers of packets are communicated within the network.

Latency: Average latency is a measure of the average time between initiating a route discovery for a wireless sensor node to transmit and successfully setting up

![Fig. 3: Analysis graph for latency with 60 nodes](image-url)
route for the data transmission (Fig. 4). This refers to the time interval between the transmission of wireless sensor data packets from a wireless sensor source node and the time of its reception by a wireless sensor receiver node. From the graph, it is seen that the proposed CDPSP acquires less latency than the traditional CCF protocol. As the simulation time increases, the delay time of the packets gradually reduced. It is shown that the CDPSP manages to improve the forwarding efficiency while simulation time steps in. The average latency of the proposed CDPSP algorithm during the entire simulation is 1.56 ms, which is having an improvement of 5.12% than the existing CCF protocol.

**Protocol overhead:** The protocol packet overhead includes all the messages used in the protocol. From the graph, it is seen that CDPSP acquires an average protocol overhead of 1.63 MB which is less than the CCF protocol having an average overhead of about 2.22 MB (Fig. 5). The proposed CDPSP protocol has an improvement of 0.07% protocol overhead than the existing CCF algorithm. This is due to the fact that the data packet does not have to travel over multiple routes since the optimum route is in use. Also, in the case of the CCF, it faces frequent link breakages and data packets drop, in turn increases the routing protocol overhead.

**Jitter:** The Jitter includes all the messages used in the protocol. From the graph, it is seen that CDPSP acquires an average Jitter of 1.63 MB which is less than the CCF protocol having an average overhead of about 2.22 MB. The proposed CDPSP protocol has an improvement of 0.07% Jitter than the existing CCF algorithm. This is due to the fact that the data packet...
does not have to travel over multiple routes since the optimum route is in use. Also, in the case of the CCF, it faces frequent link breakages and data packets drop, in turn increases the routing Jitter (Fig. 5).

CONCLUSION

The performance of congestion control protocols depends on the detecting time or even correctly predicted in advance, whether the congestion degree can be accurately measured, whether the detected or predicted congestion can be notified quickly to the nodes under heavy traffic and whether these sensor nodes are able to adjust trigger correct rate adjustment. The proposed CDPSP captures the congestion degree at the intermediate sensor nodes much better than the queue-based congestion detection. But the speed with which the CDPSP detects congestion is purely dependent on how quickly the packet inter-arrival and service time can be correctly measured from the equations. The proposed CDPSP uses hop-by-hop implicit congestion notification and guarantees high link utilization and avoid congestion.

Designing a new protocol with different mobility models are suitable for future ubiquitous applications, would be our future study. Using agents to wrap incompatible systems lacking other provisions for interoperability allows the rapid construction of middleware. Simulations can also be evaluated by varying the mobility models in the simulation scenarios.

REFERENCES


