Cluster QoS Framework Based On Time Control And Synchronized Access Scheduling Mechanism In Wireless Sensor Network

P.Vijayalakshmi and B.G.Geetha

Background: Clustering in distributed sensor network have emerged as powerful computing of recent advances in high-speed networking technology and increasing processor speeds. Such sensor node clustering is becoming increasingly popular for providing cost-effective and affordable computing environments for day-to-day computational needs of a wide-range of applications. Objective: Emerging applications targeted for clusters in wireless sensor network are inherently interactive and collaborative in nature. These applications demand end-to-end Quality of Service (QoS) in addition to performance result. Location privacy in wireless sensor network takes time for the remarks to reach analysis and reaction part of adversary. Results: To reduce the time taken for the reaction and broadcast the packet without overload, introduced a QoS framework that provides bandwidth guarantees for communication in a WSN. The framework consists of a cluster node with Network Crossing Point based on Time Control and Synchronized Access Scheduling mechanism. A crossing point is developed so that an application using the general Message Transitory Crossing point (MTC) standard specifies bandwidth requirements of their flows to the underlying wireless sensor network. Conclusion: The framework is developed and evaluated on a KEGG Metabolic Relation and Reaction Network and SMS Spam Collection Data Set. Performance of QoS framework is measured in terms of node mobility rate and packet broadcast efficiency outperforms by 28.43 %. The proposed framework is quite unique and sustains next generation interactive and mutual applications on clusters in WSN.

INTRODUCTION

Traditionally, applications embattled for clustering distributed sensor network have primarily included compute-intensive jobs such as scientific and engineering simulations. However, with the growth of modern networking and the Web technologies, a new generation of applications is being targeted for clusters in wireless sensor networks. These clustering applications are used in large databases, data mining, imaging, shared interactions, effective reality, multimedia responder, web responder, distributed revelation, collaborative computing, and telemedicine.

The above modern WSN applications are primarily 'interactive' and 'collaborative' in nature. Thus, in addition to demanding 'high performance with lesser time', demand an 'end-to-end QoS' from the underlying system. For example, an image application incorporated with amount rendering on each node of a cluster might need to have some enthusiastic bandwidth from each node to a front-end node in the cluster so that the rendered data can be composed at the front-end node with a preferred frames and sent to the client over the WSN network. Similarly, for a cluster-based file server, a telemedicine application involving medical video transmission might require guarantee on bandwidth allocation from a back-end node to the front-end node so that it can be sent to the client over WSN at a certain rate.

To provide such end-to-end QoS in WSN, one needs to have QoS associated with both computation and communication inside the cluster and support 'predictable' execution time for the application. Many of these applications also demonstrate 'packet broadcast' property so that they can adapt depending on the available resources and desired QoS level for the applications.

Kiran Mehta, et al., 2012 initially formalizes the location privacy issues in sensor networks under this strong adversary model and computes a lower bound on the communication overhead wanted for achieving a known stage of location privacy. It proposes techniques to present location privacy to monitored objects. Chi
Lin et al., 2012 proposes a DAACA which consists of a three phases namely initialization, packets transmissions and operations on pheromones.

Current generation of clusters in WSN using the popular interconnects but do not provide any QoS support. Clusters normally use uneven topologies and connected deadlock-free routing schemes. Thus, dislocate separation of nodes in a cluster for different jobs do not unavoidably lead to disjoint paths for inter-processor communication and node Input/output jobs. Even though a space-partitioned node allotment scheme in WSN is used for mapping different jobs to the nodes of a cluster, some communication links may still be used in a time-shared manner. This is a serious obstruction for harnessing the computational power of clusters for next generation applications in distributed sensor nodes.

QoS Framework Network Crossing Point based on Time Control and Synchronized Access Scheduling mechanism provides bandwidth guarantees for communication within a cluster. The time control mechanism operations are done by controlling the speed at which packets are injected at the source into the network. Such a NCP-based development scheme provides advantages of finer granularity and reducing the overload occurrence in distributed sensor nodes. The NIC-TCSAS scheme uses combination with the identify access control and scheduling unit which maintains global knowledge of cluster traffic patterns to offer bandwidth allocation to competing flows and that monitors incoming requests for allocation and reallocation.

Here provide an overview of Network Crossing Point (NCP) based on Time Control and Synchronized Access Scheduling mechanism. The rest of this paper is arranged as follows: Section 2 describes the survey of papers. Section 3 introduces architecture diagram of the NIC-TCSAS scheme with different phases. Section 3.1, 3.2 describes about proposed method and algorithm. Section 4 shows the evolution and experimental evaluation; Section 5 evaluated the results and discuss about it. Section 6 describes conclusion.

Literature Review:

Zhen Yu., and Yong Guan., 2010 propose a dynamic en-route filtering scheme that addresses both false report injection and DoS attacks in wireless sensor networks. In our scheme, each node has a hash chain of authentication keys used to endorse reports; mean while, a legitimate report should be authenticated by a certain number of nodes. First, each node disseminates its key to forwarding nodes. Then, after sending reports, the sending nodes disclose their keys, allowing the forwarding nodes to authenticate their reports.

Abhishek Agarwal., and Aditya K. Jagannatham., 2012 framework employs adaptive modulation for transmission of the best number of packets towards fulfilling the Quality of Service (QoS) constraints. This framework is formulated as a Markov Decision Process (MDP) which minimizes the long term packet drop rate.

Ozlem Durmaz Incel., et al., 2012 first believe time scheduling on a single frequency channel with the aim of minimizing the integer of time slots essential to absolute a converge cast. It combines scheduling with transmission power control to improve the belongings of interference.

Jiguo Yua., et al., 2012., a cluster-based routing protocol for wireless sensor networks with non uniform node distribution is proposed, which includes an energy-aware clustering algorithm EADC and a cluster-based routing algorithm. Gholam Hossein Ekbatanifard., et al., 2012 focuses on adaptive quorum-based MAC protocol, Queen-MAC. This protocol separately and adaptively schedules nodes wake-up times, decreases idle listening and collisions, increases network throughput, and extends network lifetime. Queen-MAC is highly suitable for data collection applications.

Ungjin Jang., et al., 2012. addresses the problem of scheduling the sleep–wake cycles of nodes in a data gathering tree under deadline constraints. After officially modeling the problem being addressed, an optimal wake-up frequency assignment (OWFA) algorithm, which takes into account the data rate at each node and the total allowable delay. Yuan He., and Mo Li.,2012 propose COSE, a query-centric framework of collaborative heterogeneous sensor networks, where sensor networks collaborate with each other for effective and efficient processing of queries. Tarek Bejaoui., and Nidal Nasser., 2011 evaluate the performance of an hybrid and adaptive call admission control protocol for UMTS cellular networks with underlying tunnel-WSN.

Satayajayant Misra., et al., 2010, of the relay node placement problem, where relay nodes can only be placed at a set of candidate locations. In the connected relay node placement problem, we want to rest a minimum number of relay nodes to ensure that each sensor node is connected with a base station through a bidirectional path. The base station only retrieves the aggregated result, not individual data, which causes two problems. First, the usage of aggregation functions is constrained by Chien-Ming Chen., et al., 2012. Second, the base station cannot corroborate data integrity and authenticity via attaching message digests or signatures to each sensing sample.

Yu-Kai Huang., et al., 2012 present an adoptive-parent-based framework for a ZigBee cluster-tree network to increase bandwidth utilization without generating any extra message exchange. To optimize the throughput in the framework, model the process as a vertex-constraint maximum flow problem, and expand a distributed algorithm that is fully well-matched with the ZigBee standard.

To broadcast the packet within the time limit, a new technique named Network Crossing Point (NCP) based on Time Control and Synchronized Access Scheduling mechanism is presented.
**Proposed Network Crossing Point Based On Time Control And Synchronized Access Scheduling Mechanism:**

Network Crossing Point based on Time Control and Synchronized Access Scheduling mechanism is shown in Fig 3.1.

![Diagram of Network Crossing Point based on Time Control and Synchronized Access Scheduling mechanism](image)

Fig. 3.1: Network Crossing Point based on Time Control and Synchronized Access (NCP-TCSA) Scheduling mechanism

The above Fig 3.1 describes the Time Control and Synchronized Access Scheduling mechanism on wireless sensor network. The wireless sensor network senses the distributed nodes and uses the QoS framework. The proposed QoS framework is implemented with a time-control mechanism at the NCP level together with a Synchronized Access Scheduling (SAS) Manager. Communication flows are synchronized by calculating the rate at which data is transferred into the Network Crossing Point and sent into the network.

Time-control (TC) scheme implemented at the host, but a NCP-based scheme in WSN is preferred since it allows a finer granularity of control, as the NCP deals with frames whereas the host will deal with messages. Since the QoS mechanism is implemented by the firmware on the NCP in distributed sensor nodes. The solution is particularly attractive in that it requires no additional components, or changes in commodity components.

An SAS manager approves reservation requests of every application before they can be granted. The SAS keeps information about the bandwidth available on every link in the wireless sensor network. When a request comes in, either for a new bandwidth allocation or for a change of stipulation, the SAS uses the stored data to verify that granting the request will not over-allocate the links to be traversed by the flow in the network.

In case, if it grants the request and updates the information maintained in its data structures, the responsibility of the SAS manager is therefore to make sure that no link in the cluster is being over-allocated and to inform the time control agent in the NCP of changes in bandwidth stipulations arising from allocations and reallocations. The next section gives the actual mechanism at the NCP that performs rate-control on packet injection into the wireless sensor network.
Every NCP connecting to the network has the QoS features that are executing at the hosts and reserve certain amounts of network resources in terms of network bandwidth, and be guaranteed that the reserved bandwidth be available only to them. NCP scenario is similar to the case in which every executing application has its own independent virtual network that is unaffected by interference due to the communication flows of other processes on the cluster. An example of the Time-control (TC) mechanism is shown in Time Control Agent.

Fig. 4: Time Control mechanism

As shown in the figure, even though the flows of two separate applications in WSN share links between the switches, there will not be any interference between them if a certain amount of bandwidth is reserved by each communication flow, and the rate of injection of each flow into the network is controlled. But the proposed time control mechanism is only a local scheme, and every NCP can be expected to know only information about flows coming out and going into that host distributed sensor node. Stipulation of network links requires a more global knowledge of the traffic patterns in the cluster. A trusted manager called the Synchronized Access Scheduling (SAS) Manager maintains such information.

3.1 NCP based Time Control Mechanism:

Every message flow has a well-defined basis and a well-defined sink in distributed sensor node. The endpoints of the flow are logical and there are several communication endpoints on the same physical wireless network node. The flows are then multiplexed over the physical link of NCP. When requesting bandwidth guarantees, an application is required to make QoS stipulations for each of the communication flow originating from it. Time-control algorithm in NCP assumes the bandwidth requested by the application is the maximum amount that it requires.

The SAS agent running on that node make sure that the request satisfaction, maps the bandwidth value to a parameter known as the Inter-Transmit Time (ITT) and passes value to the time-control agent at the NCP in WSN. Therefore, ITT value associated with every flow are defined as the minimum interval that elapses between the successive injections of the packets from that flow into the network crossing point.

At any given time point, let $c_1, c_2, ..., c_n$ be ‘n’ communication flows sourced at a particular distributed sensor node. Let their corresponding ITT values be $\{\text{ITT}_1, \text{ITT}_2, ..., \text{ITT}_n\}$. The actual time control algorithm uses another set of parameters called Subsequent Transmit Time (STT).

$$\text{STT} = \text{STT}_1, \text{STT}_2, ..., \text{STT}_n$$

Specifies the absolute time before which a packet from a given flow should not be dispatched in NCP. The STT value of a flow is initialized to the current time when a message send is posted for that flow in WSN. The below describes the algorithm flow of time control mechanism...


Begin

Step 1: At any time t,
Step 2: Let ‘k’ be the communication flow
Step 3: STTk = min (STT1, STT2, STT3…STTn).
Step 4: If STTk <= t
Step 5: Transmit packet from flow ‘k’
Step 6: Update STTk to STTk + ITTk

End

The described algorithm maintains ITT and STT information at the NCP and these values decides the next packet to be transferred into the wireless sensor network. To reduce the overhead of the QoS mechanism in NCP-TCSAS, the next smallest STT value is searched in parallel with the current packet being sent. This ensures search for the minimum STT value among all the message flows of requested QoS does not fall in the critical path of sends, and that the flow with the least STT value is known at the time of servicing the subsequently send. If no flow is “prepared to be sent” at the current time in time control mechanism, then data from finest effort flows is transferred into the wireless sensor network.

3.2 Synchronized Access Scheduling (SAS) Implementation:

The SAS is the policing individual at the cluster-level that handles requests for wireless sensor network allocation and reallocation. The criteria for admitting a new message flow with a given bandwidth requirement in NCP-SAS is as follows:

- If the message flow is admitted, then the increasing bandwidth requirement for all flows at the source distributed sensor network node of the new flow should not exceed its max out capability.
- If the message flow is admitted, then the increasing bandwidth requirement for all flows using the switch output ports traversed by the new flow should not exceed the corresponding outgoing link capacity in NCP.
- If the message flow is admitted, then the increasing bandwidth requirement for all flows at the destination distributed sensor network node of the new flow should not exceed its max out capability.

If the addition of a stipulation request satisfies all of the above conditions then the request is permitted in SAS mechanism. Now, it is the duty of the SAS to convert this stipulation in terms of ITT values and inform the time-control agent at the NCP level of the new premium stipulation. The ITT value is defined as follows:

\[\text{ITT} = \text{Time} \times \left(\frac{B_{\text{max out}}}{B_{\text{con}}}\right)\]

Where, Bcon is the bandwidth condition of the new message flow in wireless sensor network. The implementation of the SAS is designed in such a way that a copy of the SAS should run on every wireless sensor node in the cluster. These restricted copies of the SAS are slave SAS from the master. An application on a wireless sensor node send its stipulation request to the restricted slave SAS running on that node. One of these SAS is also designated as master SAS, which maintains information about all live requests currently operating on all the links in the cluster.

To regulate a request, each slave SAS sends it to the master SAS then uses the information it maintains to study if the three conditions specified above are satisfied if the new request is to be allowed. Once a result is taken, the master informs the slave, who then either makes the stipulation is possible. If it’s not possible it informs the requester that the stipulation cannot be satisfied in NCP-SAS. All the SAS accept requests are taken when a QoS request.

Since the slave SAS makes the stipulation on behalf of the user which cannot misuse the bandwidth feature by assigning any desired bandwidth value to itself. The SAS also maintains information about all finest-effort flows in the NCP-SAS system. These message flows that are not requested any specific bandwidth value but are prepared to use whatever bandwidth is enduring after allocations have been done in NCP. As premium requests are allocated and reallocated as requested by the applications the SAS also calculates the amount of bandwidth remaining for finest-effort traffic and updates the applications about the changed values in minimal time.

Experimental Evaluation:

An experimental evaluation of Network Crossing Point based on Time Control and Synchronized Access (NCP-TCSAS) Scheduling mechanism is implemented in NS2 simulator. In order to test the diverse clustering algorithm techniques in WSN, KEGG Metabolic Reaction Network (Undirected) Data Set and SMS Spam Collection Data Set.

KEGG Metabolic pathways can be realized into wireless sensor network. Two kinds of network / graph can be formed. These include Reaction Network and Relation Network. In the Reaction network, Substrate or
Product compound are considered as Node and genes are treated as edge. While in the relation network, the Substrate and Product compounds are measured as Edges and enzyme and genes are placed as nodes. We tool large number of metabolic pathways from KEGG XML. They were modeled into the graph as described above. With the help of Cytoscape tool, varieties of network features were computed.

The SMS Spam Collection is a public set of SMS labeled messages that have been composed for mobile phone spam research. A collection of 425 SMS spam messages was physically extracted from the Grumble text Web site. This is a UK forum in which cell phone users make public claims about SMS spam messages, most of them without coverage the very spam message received. The identification of the text of spam messages in the claims is a very hard and time-consuming task, and it concerned suspiciously scanning hundreds of web pages. The performance of the proposed Network Crossing Point based on Time Control and Synchronized Access (NCP-TCSAS) Scheduling mechanism is measured in terms of

i). Bandwidth in Mbps
ii).Sensor Node Mobility rate
iii).QoS Packet broadcasting Efficiency

RESULTS AND DISCUSSION

In this work it shows the broadcasting of packets in an efficient way with a minimal time using the Time Control and Synchronized Access Scheduling mechanism. The performance of Network Crossing Point based on Time Control and Synchronized Access (NCP-TCSAS) Scheduling mechanism is compared with the Protecting Location Privacy (PLP) in Sensor Networks.

Bandwidth:

Bandwidth is defined as the amount of data that can be carried from one point to another in a given time period (usually a second). This kind of bandwidth is usually expressed in mega bits (mega of data) per second (bps).

The above table (table 5.1) describes the bandwidth efficiency (i.e) the data transfer rate from the source to destination node in the wireless sensor node. The above table 5.1 describes the Network Crossing Point based on Time Control and Synchronized Access (NCP-TCSAS) Scheduling mechanism with the Protecting Location Privacy (PLP) in Sensor Networks for bandwidth in Mega bits per second (Mbps).

**Table 5.1: Time in seconds vs. Bandwidth in MBps**

<table>
<thead>
<tr>
<th>Time in seconds</th>
<th>Bandwidth in Mbps</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Proposed NCP-TCSAS Mechanism</td>
</tr>
<tr>
<td>15</td>
<td>20</td>
</tr>
<tr>
<td>30</td>
<td>17</td>
</tr>
<tr>
<td>45</td>
<td>13</td>
</tr>
<tr>
<td>60</td>
<td>12</td>
</tr>
<tr>
<td>75</td>
<td>12</td>
</tr>
<tr>
<td>90</td>
<td>10</td>
</tr>
<tr>
<td>105</td>
<td>9</td>
</tr>
</tbody>
</table>

Bandwidth = Bmax out / Bcon
Where, Bmax out – Bandwidth maximum value
Bcon – Bandwidth condition value

The above table (table 5.1) describes the bandwidth efficiency (i.e) the data transfer rate from the source to destination node in the wireless sensor node. The above table 5.1 describes the Network Crossing Point based on Time Control and Synchronized Access (NCP-TCSAS) Scheduling mechanism with the Protecting Location Privacy (PLP) in Sensor Networks for bandwidth in Mega bits per second (Mbps).

**Fig. 5.1:** Time in seconds vs. Bandwidth in MBps
Fig 5.1 describes the bandwidth with the time in seconds. The time is used in terms of seconds to calculate the reaction of the master to the slaves. The time control mechanism is used broadly to calculate the relation and reaction time using the KEGG Metabolic Reaction Network Data Set. The time control mechanism in Network Crossing Point (NCP-TC) produce the better result in proposed system with 7.86 % increased in data transfer rate (i.e. bandwidth) when compared with the Protecting Location Privacy (PLP) in Wireless Sensor Networks.

**Sensor Node Mobility Rate:**

Sensor Node Mobility Rate is of anxiety with higher mobility tends to correlate with lower achievement of nodes in network crossing point.

**Table 5.2:** No. of sensor nodes vs. Sensor Node Mobility Rate

<table>
<thead>
<tr>
<th>No. of sensor nodes</th>
<th>Sensor Node Mobility Rate</th>
<th>Proposed NCP-TCSAS Mechanism</th>
<th>Existing PLP in WSN</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>95</td>
<td>75</td>
<td>74</td>
</tr>
<tr>
<td>20</td>
<td>96</td>
<td>74</td>
<td></td>
</tr>
<tr>
<td>30</td>
<td>94</td>
<td>75</td>
<td></td>
</tr>
<tr>
<td>40</td>
<td>93</td>
<td>76</td>
<td></td>
</tr>
<tr>
<td>50</td>
<td>93</td>
<td>77</td>
<td></td>
</tr>
<tr>
<td>60</td>
<td>92</td>
<td>74</td>
<td></td>
</tr>
<tr>
<td>70</td>
<td>90</td>
<td>73</td>
<td></td>
</tr>
</tbody>
</table>

Mobility Rate (MR) = \( \frac{100 \times (MN_1 + MN_2 + \ldots + MN_n)}{100} \)

Where, \( MN \) = Mobility Node in distributed sensor network

The above table (table 5.2) describes the sensor node mobility rate based on the nodes in wireless sensor network. The table 5.2 describes the sensor node mobility rate on Network Crossing Point based on Time Control and Synchronized Access (NCP-TCSAS) Scheduling mechanism and Protecting Location Privacy (PLP) in Wireless Sensor Networks.

**Fig. 5.2:** No. of sensor nodes vs. Sensor Node Mobility Rate

Fig 5.2 describes the sensor node mobility rate on NCP-TCSAS mechanism. The mobility rate of the nodes increased drastically due to the introduction of the similar node clustering using the network crossing point. The SMS Spam Collection Data Set describes the result using multiple times evaluation of nodes ranging from 10 – 70. The dataset finds the mobility rate in higher ratio using Network Crossing Point based on Time Control and Synchronized Access (NCP-TCSAS) Scheduling mechanism. The mobility rate is increased by 18.43% when compared with mobility rate values of Protecting Location Privacy (PLP) system.

**QoS Packet Broadcasting Efficiency:**

It is defined as the QoS amount of information transfer in the form of packets in wireless sensor network. The efficiency is measured in terms of percentage.

**Table 5.3:** Cluster Size vs. QoS Packet broadcasting Efficiency

<table>
<thead>
<tr>
<th>Cluster Size (Kbps)</th>
<th>QoS Packet broadcasting Efficiency (%)</th>
<th>Proposed NCP-TCSAS Mechanism</th>
<th>Existing PLP in WSN</th>
</tr>
</thead>
<tbody>
<tr>
<td>1000</td>
<td>92</td>
<td>62</td>
<td></td>
</tr>
<tr>
<td>1500</td>
<td>91</td>
<td>65</td>
<td></td>
</tr>
<tr>
<td>2000</td>
<td>93</td>
<td>64</td>
<td></td>
</tr>
<tr>
<td>2500</td>
<td>94</td>
<td>64</td>
<td></td>
</tr>
<tr>
<td>3000</td>
<td>95</td>
<td>68</td>
<td></td>
</tr>
<tr>
<td>3500</td>
<td>95</td>
<td>67</td>
<td></td>
</tr>
<tr>
<td>4000</td>
<td>95</td>
<td>66</td>
<td></td>
</tr>
</tbody>
</table>

QoS PBE = \( \frac{\text{No. of packets transferred}}{\text{Total no. of packets in WSN}} \times 100 \)
The above table (table 5.3) describes the packet broadcasting efficiency based on cluster size. The packet broadcast efficiency is analyzed using the KEGG Metabolic Relation Network dataset. The QoS framework is maintained in NCP system and efficiency measured in percentage (%).

![Fig. 5.3: Cluster Size vs. QoS Packet broadcasting Efficiency](image)

Fig. 5.3 describes the QoS Packet broadcasting Efficiency on KEGG Metabolic Relation Network dataset. The Synchronized Access Scheduling mechanism effectively uses the master and slave concept to transfer the source data to the destination with the minimal time. Compared to the Protecting Location Privacy (PLP) wireless sensor network system, Network Crossing Point based on Time Control and Synchronized Access (NCP-TCSAS) Scheduling mechanism 28.43% outperforms well in packet broadcasting.

Finally, the cluster node with Network Crossing Point based on Time Control and Synchronized Access Scheduling mechanism develops an application. A crossing point is developed so that an application using the general Message Transitory Crossing point (MTC) standard specifies bandwidth requirements of their message flows to the underlying wireless sensor network. The framework developed and evaluated on a KEGG Metabolic Relation and Reaction Network and SMS Spam Collection Data Set.

Conclusion:

Network Crossing Point based on Time Control and Synchronized Access Scheduling mechanism with QoS framework supports wireless sensor network applications. It uses the Time Control mechanism and Synchronized Access Scheduling method in a reliable way to reduce the time taken for reaction and broadcast the packet without overload. It also handles interference between applications and provides a scheme for partitioning clusters without any significant overhead or modifications. Experimental results have shown that the framework can be used to execute applications in a reserve-flexible manner. Applications running on clusters therefore execute independently, without interference from other applications using the cluster, at the same time providing good resource utilization in minimal time. NCP-TCSAS monitors the behavior of packets belonging to individual flows, to study if the bandwidth allocated to an application is suitable for the data that has been over allocated. Experiments are conducted in the KEGG Metabolic Relation and Reaction Network and SMS Spam Collection Data Set to evaluate the time taken to broadcast the packets. Accuracy of the NCP-TCSAS broadcasting of packets outperforms 28.43 % better when compared with the Location privacy in wireless sensor network.

REFERENCES


