EAI Endorsed Transactions
on Energy Web
Research Article EAI.EU

An Energy Efficient Node Scheduling based Congestion Control Scheme for WSN Multicasting

G. Raja Vikram[1,*], K. Shahu Chatrapati[2] and A.V.N. Krishna[3]

[1] Asst. Professor, Department of CSE, Vignan Institute of Technology & Science, Hyderabad, Telangana, India.
[2] Professor, Department of CSE, J.N.T.U.H College of Engineering, Manthani, Telangana, India.
[3] Professor, Department of CSE, CHRIST (Deemed to be University), Bangalore, Karnataka, India.

Abstract

Wireless Sensor Network (WSN) is the most preferred technology for communication in resource constrained environments. They offer high-quality data propagation with limited delay. Sensor Network can be established with the help of self-configurable nodes to monitor various physical phenomenon. Multicasting in WSN results in low communication control overhead but may lead to congestion, which results in data loss, redundant transmissions, poor throughput and reduced network lifetime. In this paper, we propose a protocol to estimate the Degree of Congestion (CD) at each node to ensure load balance and avoid further congestion within the network. It is demonstrated that the proposed scheme is better compared with existing congestion control schemes in terms of end-to-end delay and energy efficiency.

Keywords: Wireless Sensor Network, Congestion Control, WSN Multicast, Energy Efficiency, Node Scheduling.

Received on 18 March 2020, accepted on 23 April 2020, published on 29 April 2020

doi: 10.4108/eai.13-7-2018.164178

*Corresponding Author. Email: grajavikram@gmail.com

1. Introduction

Wireless Sensor networks have found their way into applications like disaster relief, war-field surveillance, monitoring big constructions and emergency rescue. They come with advantages like ease of deployment, less configuration effort. The Prime issues to focus in WSN are: energy limitation, limited set of computations, security, and congestion. The Nodes in WSN won't have an unlimited power supply due to remote deployment. The limited energy available must be used in an optimal way to extend node lifetime, in turn the network lifetime. Typical operations that are executed in regular networks cannot be applied in WSN due to limited energy resources. Hence, the algorithms that provide robust security cannot be implemented on these networks.

In WSN, nodes are freely deployed in known or unknown terrain to sense physical phenomenon. Hence, these nodes are susceptible to security attacks like node compromising, masquerading. A Light-weight and robust security algorithm is the need of the hour to strengthen the network security.

Typical applications like Video Conferencing and battlefield surveillance, needs to establish communication between a single source and multiple destination systems. To perform this task efficiently, Multicast Communication is preferred over unicasting. For Group communication, unicast will forward individual data packets to each node separately, whereas in multicasting, a single message can be used to reach group of nodes. This will result in significant saving of energy and extends overall network lifetime. Multicasting can be implemented through IP Multicast or routing algorithms at various levels of protocol stack.

Congestion is observed, when the overall network traffic or individual link traffic goes beyond its threshold capacity. Congestion control is a time critical mechanism as it needs to deal with dynamic network traffic and buffer capacity changes. In Resource critical WSN environment, congestion control should be enforced properly, else it results in poor network lifetime.

In this paper, we propose a node scheduling-based congestion control scheme for WSN multicasting. To extend network lifetime and thus to provide seamless communication, we devise a Node Scheduling based Secured Multicast (NSSM) scheme. The Major contributions of this paper are given below.

1.An Optimized Binary tree is constructed. An ECC based Group key is generated and securely distributed among all the members.
2. A Novel algorithm for congestion control is proposed, based on congestion degree calculation.
3. Simulations are carried out by adjusting active node time to ensure improved throughput.

The Structure of the paper is as follows: Section 2 elaborates on existing approaches for congestion techniques for secured multicast communication. Section 3 outlines the proposed solution and Section 4 focus on result analysis. Conclusion is given in Section 5.

2. Related works

Reliable Multicast Research Group (RGMP) has established transport protocols for secured and robust multicasting in wired networks. WSN networks are highly sensitive with respect to the data load and congestion, hence the design issues considered for wired networks may not be suitable for these resource constrained environments.

Congestion in WSN may happen at two levels: Node level and Link level. When the buffer at the node overflows, node level congestion is observed. This leads to data loss, increase in delay and additional overhead for retransmission. Link level congestion is observed when multiple nodes tries to access channel simultaneously and due to collision packet gets lost. This leads to high service time and poor link utilization.

[1-4] illustrated a comprehensive review on existing WSN congestion control schemes. These papers have presented a comparative study of existing congestion control schemes along with graphical illustrations. WSN Congestion control schemes can be classified into two categories namely, Centralized and Decentralized.

In Centralized schemes, the base station will take measures to alleviate or control congestion in the network. Member nodes of the network simply follow the instructions issued by the base station. They simply act as dumb terminals in the congestion control. In this approach, the base station periodically gathers data from the network members. Whenever, it senses a congestion occurrence, it instructs the nearby nodes to limit the traffic flow to avoid congestion.

In Decentralized schemes, the task of congestion control is distributed across the network. Each node will contribute in congestion control as stated in [5]. As sensor node are sparsely deployed, the congestion control task is also divided into various subroutines across the network.

[6] propose Local Cross Layer Congestion Control (LCLCC) approach based on buffer occupancy. In this method, a sensor node takes two roles. In Source duty role, it senses the environment and generates packets for transmission. Hence it controls the packet generation rate in this mode. In Router duty mode, it receives packets from its neighbors and forwards towards the base station. In router mode, congestion in regulated based on the link load.

In [7], an Adaptive Duty Cycle based Congestion Control (ADCC) was proposed for congestion control based on congestion degree. In this method, a parent node will calculate packet service time based on the packets received from its child nodes. When the congestion degree goes beyond the threshold, parent will notify its child nodes to adjust their transmission rates.

Receiver Assisted Congestion Control (RACC) scheme was proposed in [8]. According to this approach, receiver maintains two timers to track packet round-trip time and inter-arrival time. When the packet sent by sender doesn’t arrive before the timer expires, receiver acknowledges the sender immediately. Sender will use the information given by receiver to adjust its congestion window.

An Intelligent automaton-based congestion control technique named as Learning Automaton based Congestion Avoidance Scheme (LACAS) was proposed by [9]. At each node, an autonomous learning machine will reside. It learns from the past data and takes decision on data flow to avoid congestion.

A Comprehensive comparative analysis on latest WSN congestion control schemes is presented in [10-15].

3. Proposed work

Solutions to WSN congestion problems can be classified into two approaches namely traffic control and resource control. In Traffic control approach, congestion is restricted by reducing the transmission demand. Upon detecting congestion, the sender is notified to adjust the traffic according to the available buffer capacity. The main criteria for this approach are: resource utilization and fairness. Fig. 1(a) shows the traffic control approach. In Resource control method, congestion is mitigated by increasing the buffer capacity to receive more packets as shown in Fig.1(b). Our proposed approach uses a combination of traffic control and resource control schemes.

3.1. Communication model

To achieve energy efficient secured multicasting, we propose to use an ECC based Multicast model. This approach comprises of following issues:

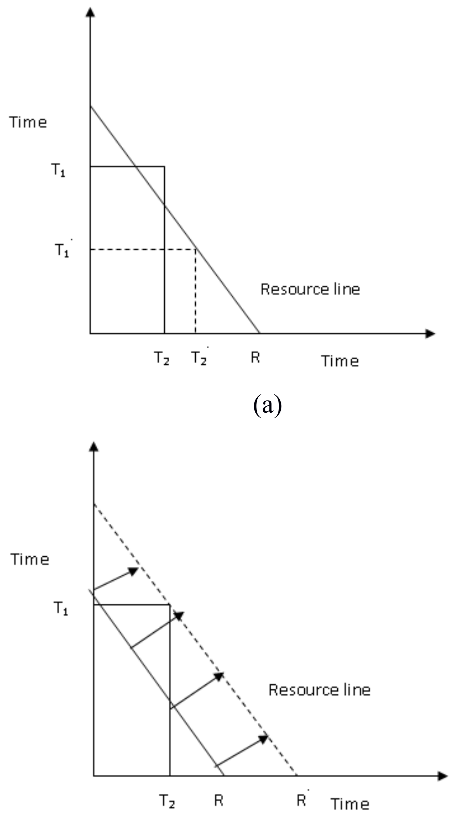
- Node Deployment
- Node Scheduling based Secured Multicast model

- Congestion control

Node Deployment

Sensor nodes are deployed randomly over the coverage area. They are self-configurable and operates with a limited energy source. For example, to monitor battle-field, group of sensors can be thrown from a low-flying airplane. These nodes will configure themselves to form a communication network.

In this approach, nodes are formed into clusters of unequal length. A Cluster Head (CH) will lead each group. The Clusters nearby the base station will have less competition radius compared with faraway ones. Generally, CHs near base station needs to handle data coming from its cluster members as well as from other clusters to en route to the base station. With unequal clustering, as the cluster length is less, the CH near the base station will handle less intra cluster traffic avoiding quick drain out of energy. Hence hot-spot problem is eliminated.



(a)

(b)

Figure 1. (a) Traffic Control Method
(b) Resource Control Method

Node Scheduling based Secured Multicast model (NSSM)

In a clustered environment, each sensor node will sense data continuously and forwards it to the CH. CH will optimize data by aggregating sensed data and sends it to the base station through intermediate CH nodes. To save energy, the proposed NSSM scheme works in duty-cycle mode where each node operates in two modes: active and sleep modes. Firstly, the number of nodes sufficient to cover the given cluster area are selected and kept in active mode. The remaining nodes will be in sleep mode.

The Duty-cycle based approaches can be synchronous or asynchronous. In Synchronous mode, nodes will be in active or sleep mode based on the negotiation made with in a frame. Example synchronous protocols were explained in [16-18]. In asynchronous mode, preamble sampling techniques are used to periodically wake-up nodes for a short duration as explained in [19-20].

In Proposed approach, a Tree-based multicast model is used. To ensure secured communication, the Group key is generated using light-weight Elliptic Curve Cryptography (ECC) based algorithm. ECC is best suited for resource constrained environments. It is stated that, for 128-bit message security, ECC needs 256-bit key compared with 3072 bits key in RSA.

A Binary tree is built for every cluster, rooted from cluster head. A Tree Vector (TV) is constructed storing the level-wise path from root to leaf nodes. during this approach, a secured cluster key's generated in a very conducive fashion and distributed among all the members. The cluster Key generation method is explained below in Figure 2.

ECC based Group Key Generation Algorithm

a. For all the leaf nodes private and public keys are calculated as
Private Key Pr_i^h = Secret random value known only to the node
Public Key $Pb_i^h = Pr_i^h \cdot G$

b. For all the intermediate nodes private and public keys are calculated as
Private Key $Pr_i^h = Pr_i^{2i} \cdot Pb_i^{2i+1}$
Public Key $Pb_i^h = Pr_i^h \cdot G$

c. For root node private key is calculated as
Private Key $Pr_i^h = Pr_i^{2i} \cdot Pb_i^{2i+1}$
Group Key $G_k^h = Pr_i^h$

where Pr_i^h, Pb_i^h are the private and public keys of a node i at a height h in the binary tree,
Pr_i^{2i} is the private key of left child of i^th^ node in the tree and
Pb_i^{2i+1} is the public key of right child of i^th^ node in the tree

Figure 2. Algorithm for Group Key Generation

As explained above, the cluster key is created from leaf nodes to the root node (CH) in a very cooperative fashion. After key distribution part, every node can hold cluster key. This key will be used to guarantee secure cluster communication. The cluster key is going to be updated, whenever a new member joins or existing member leaves the cluster.

Once a source node has to communicate a message to cluster of members in a given region, it'll forward a multicast message to the corresponding CH. Upon receiving message, The CH can cipher the message using cluster key and forwards to its children within the logical tree created during network construction. These intermediate nodes can decode the message as well as forwards to their children till all the nodes within the cluster receives it. Periodically, The CH can sense the existence of all cluster members by sending hello packets to any or all the members. The Members can respond by ACK packets to announce their convenience. once a cluster member desires to go away the cluster it'll intimate its parent by sending remove packet. This packet will be forwarded until it reaches the CH. The CH can then generate new key and propagates back to reach all the members. This method can guarantee forward and backward secrecy.

After the group-key is established among all the members, the source will forward the multicast message to destination CH. This message will be encrypted by the key shared by all the CHs. Upon receiving the message, the CH will decrypt it and forwards it to all the group members using the secured group key.

Congestion Control

In Traditional networks, based on buffer occupancy of a node or load on a link congestion is detected. When congestion is observed, techniques like priority-based packet dropping or reducing packet rate at source will be used to control it. As WSN has limited resources, the congestion control mechanisms should be simple and energy aware.

In NSSM, the congestion at a node is calculated by deriving congestion degree. Node Congestion degree is derived from its required service time and duty-cycle active state duration. The Service time of a node N (S_N) is calculated as shown in equation (1).

$$S_N = D_N / \Sigma(P_i) \qquad (1)$$

where, S_N – Required Service time of a node N

D_N – Duty cycle duration of N

$\Sigma(P_i)$ – Packet inter-arrival times of child nodes

The Congestion degree of a node Φ_N is calculated as shown in equation (2)

$$\Phi_N = AD_N - S_N \qquad (2)$$

where, AD_N is the active duty-cycle duration of N

If $\Phi_N = 0$, congestion is not observed and node continues with same active duty cycle period and service time.

If $\Phi_N < 0$, node will follow resource control approach to control congestion by adjusting its active duty cycle period. NSSM Congestion control algorithm is presented in fig.3.

Algorithm for Congestion Control

```
Step 1: For each intermediate node
            Calculate Service time $S_N = D_N / \Sigma(P_i)$
            End For
Step 2: Calculate Congestion Degree
            $\Phi_N = AD_N - S_N$
Step 3: if $\Phi_N$==0, Then the active duty cycle time is
            exactly equals to the time required to
            handle in incoming packet load. Hence
            network will be in congestion free state.
            Goto Step 7.
Step 4: if $\Phi_N$ >0, Then the active duty cycle is
            more than the time required to handle the
            incoming packets. Congestion is not
            observed.
            Goto Step 7.
Step 5: if $\Phi_N < 0$ , then congestion is detected and
            resource control approach is used to adjust
            the active duty-cycle time.
            Goto step 6
Step 6: if $S_N > MAX\text{-}AD_N$
            then New-$AD_N$ = MAX-$AD_N$
            else if $S_N < MIN\text{-}AD_N$
            then New-$AD_N$ = MIN-$AD_N$
            else New-$AD_N$ = $S_N$
Step 7: End
```

Figure 3. Congestion Control Algorithm

As observed in the above algorithm, when service time is within the threshold values new active time is set to service time, hence resource control is enforced.

Once the congestion is detected, an intimation needs to be propagated to all the other nodes contributed in congestion. When the service time (calculated as per equation (1)) exceeds MAX-AD_N , child nodes transmission rate must be revised accordingly.

4. Simulation and Results

We have used Java based simulation environment to demonstrate the efficiency of NSSM congestion control scheme. For Simulation, we have considered the network topology shown in fig.4.

In this simulation, the Duty-cycle (D_N) period of each node is assumed to be same and set to 100ms. The Active period is set to 20ms (20 percent of the total D_N) and 10ms, 30ms are taken as minimum and maximum active period thresholds. The Simulation parameters are taken as shown in table 1.

The Variation in ADN of Node A can be observed in Fig. 5. When the traffic on a specific link is low, the node active time should be minimized to save energy. However, the receiving node's active time will rise if the network traffic is high.

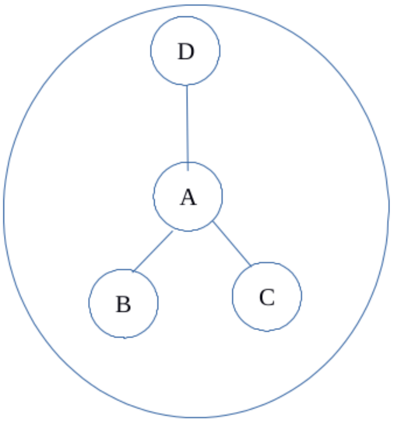


Figure 4. The Network Topology

When node B and C transmits the data simultaneously to A, the network becomes congested. Hence, the rate of packet receiving will reduce. Compared with schemes without congestion control, in NSSM the packet reception rate will be high.

Table 1. Simulation Parameters

Parameter	Value
Area	100m x 100m
Number of Nodes	5
D_N	100ms
AD_N	20%
MIN-AD_N	10%
MAX-AD_N	30%

In NSSM, source node attempts traffic control, when the link traffic is higher than MAX-AD_N as shown in fig. 6.

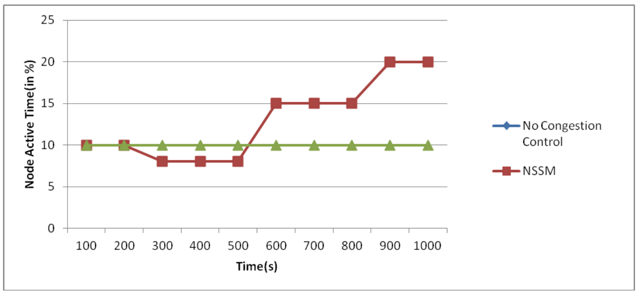


Figure 5. Change in Active time for node A

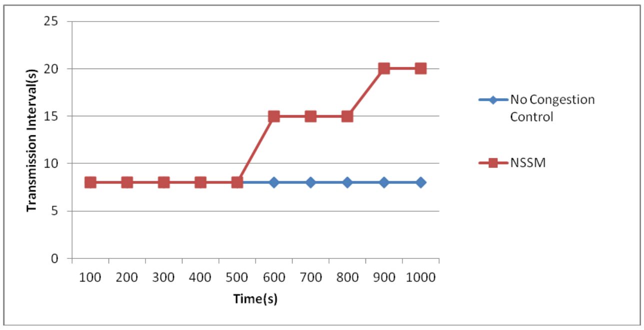


Figure 6. Traffic Control at node A

When node B and C transmits the data simultaneously to A, the network becomes congested. Hence, the rate of packet receiving will reduce. Compared with schemes without congestion control, in NSSM the packet reception rate will be high.

In NSSM, source node attempts traffic control, when the link traffic is higher than MAX-AD_N as shown in fig. 6.

5. Conclusion

Multicast communication in Wireless Sensor Networks has practical relevance in Internet of Things (IOT) and other latest technologies. Applications like Home automation, Habitat monitoring require a group of nodes deployed in a given region to sense and forward optimized aggregated data to the base station through intermediate CHs. WSN Multicasting will address these concerns efficiently. However, when the network traffic is heavy, congestion control schemes must be employed to maintain communication smoothly.

In this paper, a Node Scheduling based Secured Multicast (NSSM) approach is proposed to ensure congestion free WSN multicasting. The NSSM scheme determines the node congestion degree and accordingly updates the active duty-cycle time of the sender to ensure traffic control. Simulation results have demonstrated that, NSSM significantly improves the overall throughput of the network with less control overhead. We anticipate the further development of applying node scheduling and other energy conservation techniques like unequal clustering to extend the network lifetime and provide secured, scalable and congestion free multicast communication.

References

[1] Rekha, Gomathy, C., Sebastian, S.K., Pushparaj, K. and Mon, V.B., (2010). A Survey on congestion control in wireless sensor networks. International Journal of Computer Science & Communication, 1(1), pp.161-164.

[2] Kaur, J., Grewal, R., & Saini, K. S. (2015, June). A survey on recent congestion control schemes in wireless sensor network. In 2015 IEEE International Advance Computing Conference (IACC)(pp. 387-392). IEEE.

[3] Flora, D. J., Kavitha, V., & Muthuselvi, M. (2011, March). A survey on congestion control techniques in wireless sensor networks. In 2011 International Conference on Emerging Trends in Electrical and Computer Technology (pp. 1146-1149). IEEE.

[4] Rathod, H. M., & Buddhadev, B. V. (2011, December). Comparative study of congestion control techniques for wireless sensor network. In 2011 Nirma University International Conference on Engineering (pp. 1-5). IEEE.

[5] He, T., Ren, F., Lin, C., & Das, S. (2008, June). Alleviating congestion using traffic-aware dynamic routing in wireless sensor networks. In 2008 5th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (pp. 233-241). IEEE.

[6] Vuran, M. C., & Akyildiz, I. F. (2010). XLP: A cross-layer protocol for efficient communication in wireless sensor networks. IEEE transactions on mobile computing, 9(11), 1578-1591.

[7] Lee, D., & Chung, K. (2010). Adaptive duty-cycle based congestion control for home automation networks.IEEE Transactions on Consumer Electronics, 56(1), 42-47.

[8] Shi, K., Shu, Y., Yang, O., & Luo, J. (2010). Receiver-assisted congestion control to achieve high throughput in lossy wireless networks. IEEE Transactions on nuclear science, 57(2), 491-496.

[9] Misra, S., Tiwari, V., & Obaidat, M. S. (2009). LACAS: learning automata-based congestion avoidance scheme for healthcare wireless sensor networks. IEEE Journal on Selected Areas in Communications, 27(4), 466-479.

[10] Kaur, M., Verma, V., & Malik, A. (2018, January). A Comparative Analysis of Various Congestion Control Schemes in Wireless Sensor Networks. In 2018 8th International Conference on Cloud Computing, Data Science & Engineering (Confluence) (pp. 14-15). IEEE.

[11] Jan, M. A., Jan, S. R. U., Alam, M., Akhunzada, A., & Rahman, I. U. (2018). A comprehensive analysis of congestion control protocols in wireless sensor networks. Mobile networks and applications,23(3), 456-468.

[12] Srivastava, V., Tripathi, S., & Singh, K. (2020). Energy efficient optimized rate based congestion control routing in wireless sensor network. Journal of Ambient Intelligence and Humanized Computing, 11(3), 1325-1338.

[13] Chai, Y., Du, H., Ye, Q., Liu, C., Xu, W., & Zhang, C. (2018, December). An Energy-Efficient Multicasting Algorithm for Duty-Cycled WSNs. In 2018 IEEE Global Communications Conference (GLOBECOM) (pp. 1-6). IEEE.

[14] Gong, H., Fu, L., Fu, X., Zhao, L., Wang, K., & Wang, X. (2016). Distributed multicast tree construction in wireless sensor networks. IEEE Transactions on Information Theory, 63(1), 280-296.

[15] Carlier, M., Algora, C. M. G., Braeken, A., & Steenhaut, K. (2018). Analysis of Internet Protocol Based Multicast on Duty-Cycled Wireless Sensor Networks. IEEE Sensors Journal,18(10), 4317-4327.

[16] Ye, W., Heidemann, J., & Estrin, D. (2004). Medium access control with coordinated adaptive sleeping for wireless sensor networks. IEEE/ACM Transactions on Networking (ToN), 12(3), 493-506.

[17] Van Dam, T., & Langendoen, K. (2003, November). An adaptive energy-efficient MAC protocol for wireless sensor networks. In Proceedings of the 1st international conference on Embedded networked sensor systems (pp. 171-180). ACM.

[18] Lu, G., Krishnamachari, B., & Raghavendra, C. S. (2004, April). An adaptive energy-efficient and low-latency MAC for data gathering in wireless sensor networks. In 18th International Parallel and Distributed Processing Symposium, 2004. Proceedings. (p. 224). IEEE.

[19] Polastre, J., Hill, J., & Culler, D. (2004). Versatile low power media access for wireless sensor networks. In Proceedings of the 2nd international conference on Embedded networked sensor systems (pp. 95-107). ACM.

[20] El-Hoiydi, A., & Decotignie, J. D. (2004, June). WiseMAC: an ultra low power MAC protocol for the downlink of infrastructure wireless sensor networks. In Proceedings. ISCC 2004. Ninth International Symposium on Computers And Communications (IEEE Cat. No. 04TH8769) (Vol. 1, pp. 244-251). IEEE.