International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-8 Issue-10, August 2019

Coap Based Congestion Control Mechanism For Low Power Iot Networks

Swarna M, Godhavari T

Abstract: ***Internet of Things has billions of connected devices into internet. CoAP is a Constrained Protocol used in application layer of IoT Protocol Stack. CoAP is running on top of User Datagram Protocol (UDP), which means that, there is no possibility of congestion control in it, so CoAP is responsible for Congestion control mechanism. UDP has no knowledge on congestion control. IoT has significant resource constraint, due to this there are lots of design challenges in IoT network. This paper proposes a simple change in the CoAP protocol named CoCoA (CoAP Simple Congestion Control / Advance). CoCoA introduces novel Round Trip Time (RTT), VBF (Variable Back off Factor) and aging mechanism to calculate the dynamic and controlled Retransmission Time Out (RTO) for IoT Networks. This paper compared with the existing all the congestion control mechanism and the implementation result shows that the proposed mechanism is better than the existing mechanism in terms of throughput, power consumption, memory foot print and fairness index.***

Index Terms: IoT Network, CoAP, Congestion Control, CoCoA, Low power Communication.

I. INTRODUCTION

Internet of Things and it supporting platforms are gaining lots of scope in the world market. Internet of Things (IoT), Industrial Internet of Things (IIoT), Internet of Objects and Internet of Everything (IoE) has multiple trillion dollar business every year. In order to make this things work in an efficient way, researcher are in the need of developing low power devices with low bandwidth utilization for efficient data transmission. In general, there are six building blocks of network, they are

- Packet and multiplexing,
- Naming addressing and forwarding,
- Routing,
- Security,
- Network management
- Congestion control.

In IoT network, packet size is very small compare to internet packets. But occurrence of congestion is unavoidable. In order to reduce the congestion, this paper tried all the existing congestion control mechanism and also proposed CoAP based congestion control mechanism for the IoT network. Broadly, congestion control mechanism can be classified into two category,

Manuscript published on 30 August 2019.
*Correspondence Author(s)
M. Swarna, Research Scholar, Department of ECE , Dr. M.G.R. Educational and Research Institute, Chennai, India
Dr. T. Godhavari, Professor and Head, Department of ECE, Dr. M.G.R. Educational and Research Institute (Deemed to be University), Chennai, India.

Open loop congestion control mechanism and closed loop congestion control mechanism. Open loop congestion control mechanism is straight forward approach, decision is based on the available bandwidth, there is no feedback mechanism in the case. There are several types in the open loop congestion control mechanism, they are Retransmission Policy, Window Policy, Discarding Policy, Acknowledgment Policy, Admission Policy. This policy has its implementation algorithm for congestion control mechanism like bit fair rounding, scheduled based approach, virtual clock, input buffer limit, and stop and go, all this algorithm are controlled in the source of the network. There are algorithms which controls in the destination of the network, they are Isarthmatic method, packet discarding, and selective packet discarding give better result than the source based mechanism. Even though open loop is pretty easy to implement, but it is not efficient for congestion control due to there is no information about source in the destination node or no information about destination in the source. To overcome this open loop issue, closed loop congestion control mechanism is proposed by the researcher.

In the closed loop mechanism, there is a dedicated feedback from destination to the source to provide the status of it. Based on the destination resource availability, the packet from source is sent. By this technique, congestion is almost avoided. The closed loop congestion control mechanism has implicit feedback and explicit feedback. In the implicit feedback mechanism, feedback is not sent as a separate packet, existing network packet itself will hold the congestion feedback data. In the explicit feedback mechanism, there is separate packet for the feedback from destination to source (piggybacked). Algorithm used in the closed loop congestion control mechanism is bit round faring, scheduled based approach, virtual clock and etc.

II. CONGESTION CONTROL IN IOT NETWORK

A. IoT Network

IoT is "all things", which can connect all objects at any time and any place. It is the network with the characteristics of comprehensive perception, seamless interconnection and intelligent processing. IoT is one of the promising technology which is the backbone of the smart buildings, smart cities, smart homes and etc.., IoT needs end nodes to be connected with cloud services via internet. Connected things like sensors, actuator, measuring devices and counting devices are the end nodes of IoT infrastructure.

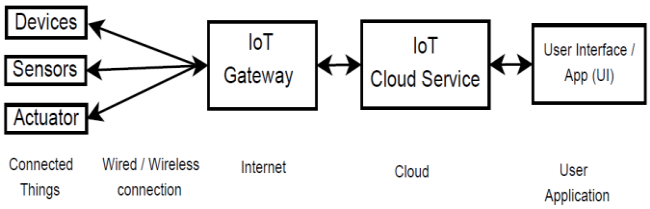

Fig. 1 – IoT Infrastructure

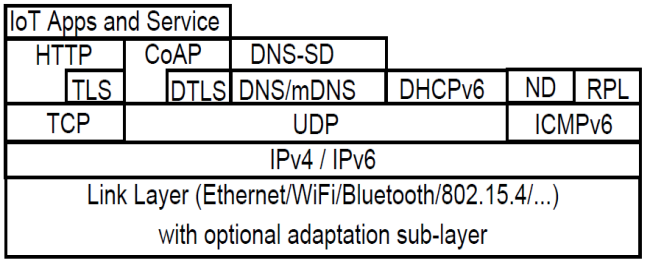

Fig. 2 – IoT Protocol Stack

Basic Infrastructure of Internet of Things (IoT) is shown in the Figure 2.1. Connected devices are running in real-time, sends the actual data to its cloud via IoT gateways. IoT gateways are communicating with nodes via light weight protocols. Gateway is connected with cloud service via actual internet connection provided by Internet Service Provider (ISP). Cloud will process the sensors data and gives the update to its user or administrator. The complete IoT infrastructure is shown Fig 1. In the entire path, packet switching plays a major role. Packet switching is implemented with layers of protocols, for every application there are dedicated protocols exist. Similarly for IoT infrastructure, dedicated protocols stack is used and it is shown in the Fig. 2.

B. Congestion Control

Flow control is the most popular in the load control paradigm in the heavy traffic network. The function of TCP protocol is to make a reliable connection for the application layer in the unreliable best effort network. In the IoT network, if we use window based flow control, it will limit the number of packets have been sent and acknowledgment has not been received. After the acknowledgment, the source will get to know that the packets has been received in the destination.

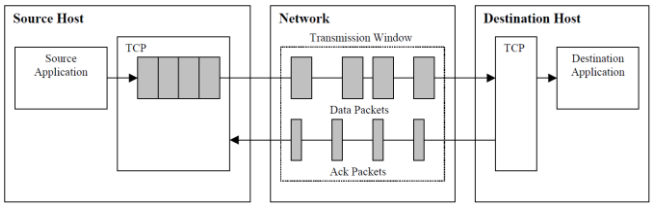

Fig. 3 . Flow control for TCP based IoT Network

Window size limits the number of packets can travel in the network from the source to destination which includes data packet, control packets and acknowledgment packets. The size of the packet is more important for flow control and the congestion control. Mostly, congestion is defined by number of packets and the maximum packet size (MPS). For a instance, if we send *W packets* at time *t*, after round trip time *(RTT)*, all the packets delivered to destination at *(t + RTT)*.the packet will be delivered and acknowledged to the source and new set of *W* packets are sent to destination. This procedure continuous until all the packets are sent. Transmission rate of the packet throughput is calculated as

$$T = W.\ MPS\ /\ (RTT) \quad bits/\ second$$

The window size is controlled by the protocol, actual window size suppose to be calculated based on minimum network capacity to transmit (cw) and receiver ability to receive the packet (aw), so the window size is defined by

$$w = min\ (cw,aw)$$

aw is not really making its role over there, *cw* is the actual decision making authority to decide the window size. In order to find the *cw*, source should know about the bandwidth delay product of the end to end connection. However, the best effort service network will not provide the clear defined available capacity of the network from source to destination. Increase the packet transmission rate will occur the packet loss. IN general, TCP has two techniques to immunize the congestion; they are *slow start and congestion avoidance*. This is the base strategy to calculate the network capacity to certain extends. Initially start with the window size of 1, increase the window size step by step until the first packet loss is detected. After the packet loss, window size increment will stop and it will fix the window size, this is called congestion avoidance mode. This is shown in the Fig 4.

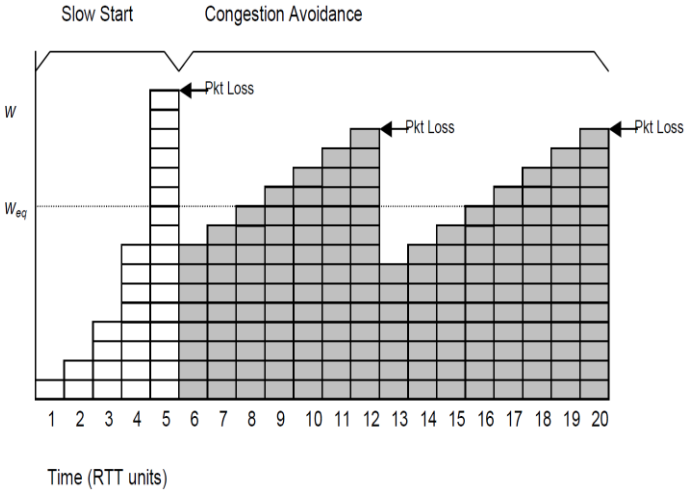

Fig 4. Congestion Control by Control of Window

Another mechanism in congestion control is catastrophic transmission failure is called Retransmission Timeout (RTO). Time out occurs only if the sent packed acknowledgement is not received in a specific time (round trip time). In order to provide QoS (Quality of Service), it is necessary to take care of all the aspects of network parameter. To increase the quality of service in IoT best effort Network, two fundamental elements need to be addressed, they are, source flow control and links Active Queue Management (AQM).TCP itself will act as a source flow control mechanism. But for the Active Queue management, it is running in a Switch or router. Its need to deployed in all the network devices like switch, router, bridge and etc. By the help of closed loop congestion control mechanism, we can attain the better efficiency of the AQM.

Retrieval Number: J91140881019/19©BEIESP
DOI: 10.35940/ijitee.J9114.0881019
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

In general, the congestion control mechanism will perform better with closed loop than open loop. Closed loop congestion control mechanism is implemented using a feedback from destination or link to source. This feedback will give information about resource availability of the link devices or destination devices. The complete description of the packet transmission with queue management is shown in the Fig. 5.

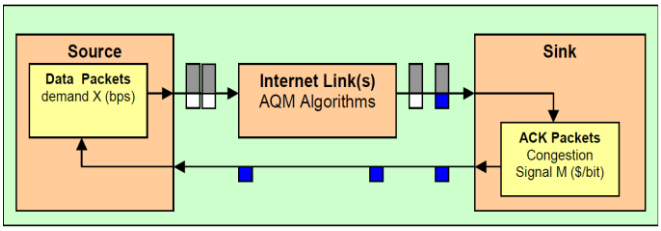

Fig 5. Physical Congestion Control Feedback loop.

The actual idea of getting better QoS means, implementing efficient packet processing engine, like better AQM service, no packet loss, no error in the packet while transmitting in the channel and so on.

C. CoAP (Constrained Application Protocol)

CoAP is a dedicated and specialized protocol internet application for IoT Devices (Constrained Devices or nodes or sensor nodes). The objective of the protocol is to work in low power application and lossy network. CoAP is a service layer protocol used for wireless sensor network. Now the advance version of WSN is IoT. IoT connects billions of devices to internet. The basic objective of the CoAP is to build a low power, less bandwidth utilization, easy to recover the data. All the objective is fulfilled with CoAP, but congestion occurrence is the major problem in the constrained devices, because many nodes will communicate to the gateway at a given time. Now it is important to add congestion control scheme in the CoAP protocol. This paper proposes a new technique to adapt congestion control in the constrained network with low power.

III. COAP SIMPLE CONGESTION CONTROL/ADVANCED (COCOA)

General form of CoAP provides basic congestion control by imposing conservative restriction on the rate of outgoing message and number of parallel message exchanged. The structure of CoAP give four types of message they are Confirmable (CON), Non-confirmable (NON), Reset (RST) and Acknowledgment (ACK) messages. For the message transmission first two types are more important, based in the reply from the destination device only the next message has to be sent, by this form, we need to develop a advance congestion control scheme with CoAP. That is called CoAP Simple Congestion Control/Advanced (CoCoA).

CoCoA is a flexible congestion control solution that has relaxed the conservative message rate restriction of the CoAP this gives better solution on congestion control in the base application. The fundamental need of designing the CoAP is on to produce a mechanism that offers a performance that is better than, or at least similar to, that of default CoAP.

CoCoA comprises three main components: adaptive RTO calculation, Variable Back off Factor (VBF) and RTO aging.

A. Adaptive RTO calculation.

Based on RFC 6298, CoCoA's RTT calculation and basic RTO calculation is calculated. RTO calculation is based on Transmission control protocol implementation. RTO is calculated by measuring an exponential weight move in average of RTT and its variation estimation. CoCoA is implementing this rule for Internet of Things. In TCP, majority of the packet loss is happened because of congestion, but IoT networks, it's due to Bit Error Rate (BER). In TCP, RTT calculation is depends on when the packet is sent, the receiver receives the packet and sends the acknowledgment to the sender, the time sender receives the packet is stamped and subtracted with the starting time of the data packet. This is round trip time of the packet. This RTT is called as Strong RTT estimator. In the IoT network using CoCoA uses weak RTT estimator, this will calculate the RTT by using measuring the time of two retransmission. This will increase the chance of considering the packet loss in the lossy network. When the weak or strong RTT is measured with that, we can find out the weak or strong RTO.

$$RTO_X = SRTT_X + K_X \,.\, RTTVAR_X$$

Where X may be weak or strong, SRTT is well known RTT in weak and variable RTT. K_X is 4 in the case of strong and 1 in the case of weak. The overall RTO is calculated based on alpha parameter.

$$RTO_{Overall} = \alpha \,.\, RTO_X + (1 - \alpha) \,.\, RTO_{Overall}$$

Where α is 0.5 for strong RTO estimator and 0.25 for weak RTO estimator. Our objective is to avoid the steep RTO increase by weak RTT estimation compare to the strong RTO estimator. There are the cases where we can reduce the weak RTO by some set of schemes, the schemes are

- Weak RTT are allowed for only two retransmission, if we have more than two retransmission, the RTO value will increase and the probability of the packet loss will increase exponentially.
- RTTVAR value is determined based on the K. For weak RTO, the value is reduced from 4 to 1.
- The weight (α) is different for strong and weak RTO, the weak estimator contributes less to RTO than the strong estimator. Strong RTO will deliver packet to the perfect location.

The RTO chosen for the IoT network is weak RTO. The values chosen here is completely depends on the stability of the network. The major concern is to build a strong and stable network with low power and low cost. Variable back off factor (VBF) is a technique used to calculate the perfect RTO in the initial time of the network. Initially the large value is given, based on the response the value will be increased or decreased. Based on the BEB and the RTO, the VBF is completely estimated. RTO aging is all about how frequently updating the RTO value or its age. RTT will keep on changes in the IoT network, its will change fast. To avoid the changes in the RTO value, CoCoA applies an aging mechanism to small and the large and small estimator.

For small and large RTO value, below one or more than two, then there will be no change in the RTT, else new measurement will be take for 16 to 4 time RTO respectively. Default CoAP will not have any restriction on sending NON message to the sender. I order to find the initial RTO time, we are in the need of CON and NON message, we will transmit and found the RTT. In order to get better understanding on hoe we estimate the RTO and RTT in CoAP and CoCoA, we should implement this proposed algorithm in the test beds.

IV. EXPERIMENTAL SETUP AND TEST CONFIGURATION

GPRS and IEEE 804.15.4 is used for evaluating the experimental results, where the nodes and the gateway is implemented in the different hardware. In the beginning stage of the M2M communication, GPRS is the hot line. IEEE 804.15.4 is used for low power communication; the common usage is on ZigBee or 6LoW-PAN. The reason behind the choosing this GPRS and the IEEE804.15.4 is they two have different bitrates and its delay characteristics. In a single hop, GPRS is implemented, but for IEEE 804.15.4 is not like that, it need multiple hops for it infrastructure, because of its low power in nature. IN order to calculate the efficiency of the congestion control mechanism, we need to compare with the existing mechanisms. The existing mechanisms are Default CoAP, PH-RTO, Linux RTO, Basic RTO, PH-RTO, CoCoA and CoCoA – S. Our objective is to compare all the existing mechanism and the proposed mechanism and to prove that the proposed is better than the existing mechanism.

In order to develop a unbiased performance analysis, we are considering different types of traffics and its responses, Continuous traffic and the Burst traffic. The analysis of the packet drops and the congestion control mechanisms are used in PH- RTO used CoAP over UDP. In IoT, cloud plays a major role, we are in the need of analyzing the Congestion control scheme in the IoT Cloud platform. The complete cloud based congestion control is implemented in ContikiMAC. In real time, congestion is depends on routing length, network unavailability, pack loss due to error in packet, we try to consider all the possible scenarios.

A. Performance Metrics.

Throughput of the continuous traffic is successfully calculated per second, but in burst traffic we tested 80% traffic should be processed by the gateway, we consider this as settling time. In order to give fairness in the calculation, we given different length, different topology. Fairness Index (FI) is used to measure the fairness of the network. FI value varies from 1 to 0. 1 means best network and 0 means worst network. Different implementations of the existing and proposed mechanism in the same platform for the evaluation. Table I shows about Comparison of the Average RTT and Initial RTO Values in Milliseconds for Different Numbers of Clients in the GPRS Setup. This paper tested even for more number of Clients in the same platform.

TABLE I: Comparison of the Average RTT and Initial RTO Values in Milliseconds for Different Numbers of Clients in the GPRS Setup

Types	10 GPRS Clients		20 GPRS Clients	
	RTT	RTO	RTT	RTO
CoAP	-	2497	-	2499
CoCoA	661	1505	1437	3379
CoCoA-S	625	1428	1275	2903
B-RTO	1025	1152	1962	2198
PH-RTO	746	1797	1835	3703
Linux	682	1235	1550	2801

In terms of fairness evaluation, different congestion control scheme is implemented and shows the probability mass function for the number of finished transaction per destination node measure during continuous traffic and the burst traffic. The CoCoA-S is not scarifies from the fairness compare to CoAP, compare with the performance improvement. CoAP is best if we define the path in specific. Memory footprint is tradeoffs between performance and memory of the algorithm. Its shown in the Fig 6.

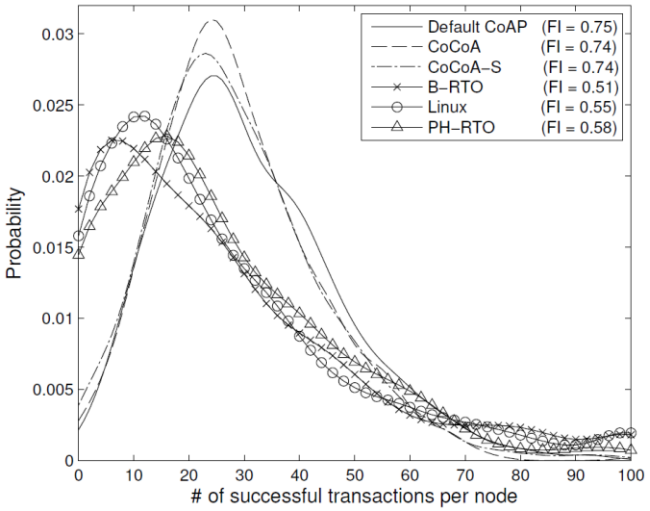

Fig 6. Probability Mass Function for the number of finished transactions per node and the Fairness Index (FI) achieved by each of the analyzed algorithms. For illustration purposes, more than 100 finished transactions per node are valuated as 100 finished transactions per node.

V. CONCLUSION

Non adaptive and conservative congestion control mechanism is given by CoAP, but advance congestion control mechanism CoCoA provides highly flexible and adaptive solution. For the calculation of adaptive RTO, using weak RTTs, VBF, and aging to optimizing the performance. Compare to CoAP, CoCoA increases the throughput and it process the burst traffic without sacrificing the fairness.

Retrieval Number: J91140881019/19©BEIESP
DOI: 10.35940/ijitee.J9114.0881019
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

In overall, the CoCoA is better than all the existing congestion control mechanism for IoT application. Hence, we recommend this CoCoA for Congestion control mechanism in IoT Application.

REFERENCES

1. A. Betzler, C. Gomez, I. Demirkol, and J. Paradells, "CoCoA+: An advanced congestion control mechanism for CoAP," Ad Hoc Networks, vol. 33, pp. 126 – 139, 2015.
2. C. Bormann, A. P. Castellani, and Z. Shelby, "CoAP: An Application Protocol for Billions of Tiny Internet Nodes," IEEE Internet Computing, vol. 16, no. 2, pp. 62–67, Mar. 2012.
3. A. Betzler, C. Gomez, and I. Demirkol, "Evaluation of Advanced Congestion Control Mechanisms for Unreliable CoAP Communications," in Proceedings of the 12th ACM Symposium on Performance Evaluation of Wireless Ad Hoc, Sensor, & Ubiquitous Networks, PE-WASUN 2015, Cancun, Mexico, November 2-6, 2015, 2015, pp. 63–70.
4. H. Ekstrom and R. Ludwig, "The peak-hopper: a new end-to-end retransmission timer for reliable unicast transport," in INFOCOM 2004. Twenty-third AnnualJoint Conference of the IEEE Computer and Communications Societies, vol. 4, March 2004, pp. 2502–2513 vol.4.
5. P. Sarolahti and A. Kuznetsov, "Congestion Control in Linux TCP," in Proceedings of the FREENIX Track: 2002 USENIX Annual Technical Conference. Berkeley, CA, USA: USENIX Association, 2002, pp. 49–62.
6. M. Kovatsch, M. Lanter, and Z. Shelby, "Californium: Scalable cloud services for the internet of things with coap," in Internet of Things (IOT), 2014 International Conference on the, Oct 2014, pp. 1–6.
7. Swarna, M., S. Ravi, and M. Anand. "Adaptive Backoff Algorithm for Congestion Control in IoT." (2016): 205-214.
8. Swarna, M., S. Ravi, and M. Anand. "Leaky bucket algorithm for congestion control." *International Journal of Applied Engineering Research* 11.5 (2016): 3155-3159.
9. R. Lim, F. Ferrari, M. Zimmerling, C. Walser, P. Sommer, and J. Beutel, "Flocklab: A testbed for distributed, synchronized tracing and profiling of wireless embedded systems," in Information Processing in Sensor Networks (IPSN), 2013 ACM/IEEE International Conference on, April 2013, pp. 153–165.
10. Kumar, Shanmuga, and Noor Mahammad Sk. "High precision and high speed handheld scientific calculator design using hardware based CORDIC algorithm." *Procedia Engineering* 64 (2013): 56-64.

AUTHORS PROFILE

M.Swarna, Research Scholar, ECE Department, Dr. M.G.R. Educational and Research Institute, Chennai, India. Email: swarnavinil@gmail.com.

Dr. T. GODHAVARI is currently working as Professor and Head ECE Department in Dr. M.G.R. Educational and Research Institute (Deemed to be University), Chennai. She obtained her Ph.D. from Sathyabama University, Master's degree with honors in Communication System from Dr. M.G.R. Educational and Research Institute (University), Chennai and Bachelor's degree in Electronics and Communication Engineering from IRT Tech, Erode, affiliated to Bharathiar University, Coimbatore. She has published 20 papers in International and National Journals and Conferences. Her areas of interest include Neural networks, Cryptography, Quantum computing and Computer Networks. She has 20 years of teaching experience. She has attended and organized Seminar and workshops related to her area of research. She is a Life Member in ISTE and CRSI (Cryptology Research Society of India), and Member in IET.