Medium Access Control CSMA/CA Binary Countdown Protocol for SCADA Application

K.U.Prateek, B. Dinesh Ballullaya, R. L. Chakrasali, S.S.Navalgund

Abstract—**This paper discusses a novel approach to access the medium using CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) protocols for SCADA (Supervisory Control and Data Acquisition) system employed in power system operation and control. This method offers superior performance over the existing practices of accessing medium using CSMA/CD (Carrier Sense Multiple Access with Collision Detection) protocols. The proposal makes use of binary countdown method with modification to suit the requirements of SCADA system such as reliability and real time operation. In this work, a program is written and the procedure is run to allocate the channel considering the priorities of the RTUs (Remote Terminal Units) and the type of data to be transmitted such as operational data and nonoperational data for operation & control. The program uses generic statement and is applicable to a system having a MTU (Master Terminal Unit) and any number of RTUs. The results obtained by running the procedure show its novelty. Further, a Moore finite state machine is designed and a VHDL model is developed for an RTU to indicate the state transition while attempting to access the channel.**

Index Terms—**SCADA, Medium access protocols, MTU,RTU, finite state machine, procedure.**

I. INTRODUCTION

SCADA is real time data management of production operations using efficient control paradigms to improve Quality, Plant & personnel safety and reduction in cost. The use of a SCADA for operating power system is supported by a distributed architecture, with number of computers, called Remote Terminal Units (RTUs). These RTUs transmit data to a control center. The data is measure of electrical parameters which depict the state of the power system. The command signals are generated by the control centre (MTU) and communicated to RTUs for equipment control. Taking into account the large number of equipment and their geographical dispersion, the communication with the control center usually uses multiplexed lines of narrowband channels [1]. In order to reduce the total number of required channels, several RTUs are usually connected to each line, sharing the channel's resources. In any broadcast network, the key driver is how to determine who gets to use the channel when there is contention for it. The protocols (a set

of rules being mutually agreed upon by the communicating parties) are in use to determine who goes next on a multi access channel and is taken care of by a sub layer of data link layer called MAC sub layer in the OSI (Open System Interconnection) reference model [2]. The procedures run to seize the physical medium for data transmission in coordinated way is called MAC (Medium Access Control) protocol.

II. SCADA SYSTEM ARCHITECTURE

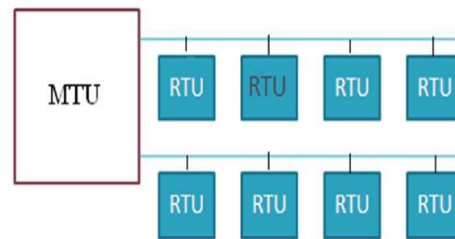A typical configuration of SCADA system architecture used in power system is shown in fig.1.

Fig.1 SCADA system architecture

It consists of a Master terminal unit (MTU) that is equivalent to a master unit in Master/slave architecture. The MTU presents data to the operator through the HMI (Human Machine Interface), gathers data from the distant sites, and transmits control signals to the remote sites. The transmission rate of data between the MTU and the remote site is relatively low and the control method is usually open loop because of possible time delays or data flow interruptions. The Remote terminal unit (RTU) functions as a slave in the master/slave architecture, sends the received control signals to the device under control, acquires data from these devices, and transmits to MTU. An RTU may be a PLC OR PC the date rate between RTU and controlled device is relatively high and the control method is usually closed loop. The data communication uses the Internet, wireless or wired networks, or switched public telephone network. The SCADA protocols have been developed for power networks keeping in view that it must be suitable for real time, reliable operation and tolerance under emergency situations because delay in communication cannot be affordable. Further, the protocols should also consider the throughput of the channel.

There is large number of protocols used in SCADA systems. These have been provided by the system manufactures or by the users. Nowadays SCADA system is migrating from customized platform to standardized PC and windows platform. The protocols are developed taking OSI model as reference, a stack of seven layers. While developing protocols for power systems, one or more of

these layers are unused/not present. In contrary, EPA model (Enhanced Protocol Architecture) specifically proposed by the IEC (International Electrotechnical Commission) [3] for the telecontrol of power systems is having three layers viz Physical layer, Data link layer and Application layer. In both approaches, the control procedures for the Medium Access Control are in the lower sub layer of the Data link layer [4-6]. The problems of the Medium Access Control encountered in IT sector LANs are very similar to those of SCADA system. Thus, one can make good use of the results and experiences from the LANs.

III. MEDIUM ACCESS CONTROL PROTOCOLS

There are many medium access control protocols to seize the physical medium and classified into three categories viz Selection (polling, token bus and token ring), Contention (ALOHA, CSMA and CSMA/CD) and Reservation.

Selection techniques are based on the transmission turn goes on in an ordered way, around a set of computers connected to the same physical medium.

In contention technique, stations contend for the physical transmission medium, producing collisions. In CSMA/CD protocol, each node willing to transmit (control centre and RTUs), has carrier sense (CS) feature. However, due to the propagation delay through the physical medium, two or more nodes could transmit at the same time, producing a collision. A node also has collision detection (CD) feature and aborts its transmission and waits for random period of time before making next attempt. Reservation techniques are based on splitting the transmission medium into different sub-channels, using physical mechanisms such as Frequency Division Multiplexing and Time Division Multiplexing and are used to establish point to point virtual connections between the stations within the networks and are rarely used in LANs.

The number of RTU's, the transmission speed, and the commuting delay are the parameters used to determine [1] the performance of protocols. In general the efficiency of the above protocols is quite low, typically between 60%-70% [7-11].

IV. COLLISION FREE PROTOCOLS

The existing protocols have the limitation of channel access delay and collision, which do not felicitate the determinism. These limitations can be overcome by employing collision free protocols such as bit map protocol, limited contention protocol, binary countdown protocol etc. to improve the situation.

In this paper, a procedure is developed using C language for Binary countdown collision free protocol which is modified to suit the requirements of SCADA system. The Program is generic that will accommodate a MTU and any number of RTUs. Further, hardware of type Moore finite state machine is designed for a RTU which makes state transition from one state to another while attempting to access the channel. The hardware is validated by developing a VHDL model.

The binary countdown Protocol: All the RTUs contending for the channel are assigned with a unique address and are assumed to be of the same length. The bits in each address position from different stations are BOOLEAN ORed together. To avoid conflicts, an arbitration rule is applied. As soon as the station sees that high order bit position i.e. 0

in its address has been over written with 1, it gives up contention [12]. This process continues and the station having address of higher number will get the channel for data transmission. It has the property that higher number stations have a higher priority than lower numbered stations. However, one must be optimistic that all the higher address stations need not have data to communicate all the time, thus, stations of lower numbered addresses will also have fair chances of sending the data. The channel efficiency of this method is very close to 100%.
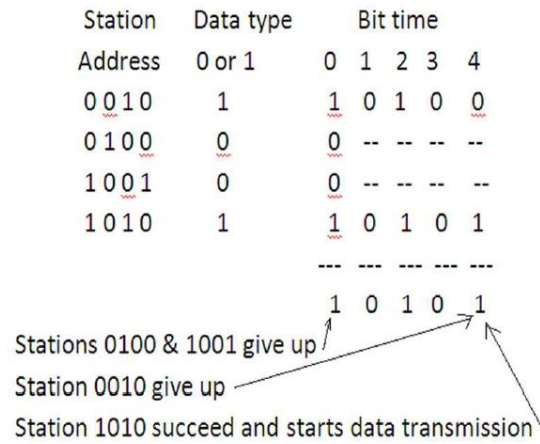
Station	Data type	Bit time				
Address	0 or 1	0	1	2	3	4
0 0 1 0	1	1	0	1	0	0
0 1 0 0	0	0	--	--	--	--
1 0 0 1	0	0	--	--	--	--
1 0 1 0	1	1	0	1	0	1
		---	---	---	---	---
		1	0	1	0	1

Stations 0100 & 1001 give up
Station 0010 give up
Station 1010 succeed and starts data transmission

Fig.2 Modified binary countdown protocol

V. THE PROPOSED METHOD

The novel proposal made here is based on the binary countdown method will little modification i.e. both the RTUs address and the type of data are attached with priority. As applied to power systems, the RTUs gather data from field devices and transmit to the MTU. The MTU will process the received data and generate accordingly the command signals and sends it back to RTUs to control the field devices. The data can be of two types in power system. The first one is the operational data such as voltage, current, frequency, real power, reactive power etc. Further, the operational data can become critical data when the values of the above parameters exceed the specified limits. On the other hand, it is the normal data as long as the above parameter values are within the permissible range. The normal data is typically for archival. The second one is nonoperational data such as status of the circuit breakers; relay contact positions etc. Which is useful in finding the power system status as well as for archival in the data warehouse. The data from the warehouse is also helpful in predicting the performance of the system offline. Whenever a RTU has critical data to transmit, it is given priority to transmit. This is necessary because, based on this data MTU will generate command signals and convey to the RTUs to implement the control action to maintain the higher qualitative degree of the system stability.

In the modified binary countdown method, both RTUs addresses and type of data are attached with priority. The RTU is permitted to transmit data on the basis of address priority, however, if another RTU having lower priority with critical data (indicated by c in the code), then the address priority is superseded and that RTU is allowed to transmit. Once the data is transmitted, then its priority becomes least in the current contention period. This is a unique feature of this work and thus, the developed procedure takes care of

the address priority and the type of data. The algorithm goes as follows:

1. All RTUs have unique address (decimal numbers used in this code) of the same length.

2. All RTUs may have both critical and normal data (indicated by c and n respectively) to transmit.

3. The critical data is having higher priority over the normal data.

4. When channel goes idle, RTUs contend for the channel by inserting the priority bits of both the data and address.

5. The RTUs having normal data to transmit, give up contention though their address priority is higher compared to other RTUs having critical data.

6. Among the RTUs having critical data, the RTU with higher address priority is permitted to transmit data. Once it completes the data transmission then its priority becomes zero (indicated in the code) thereby giving chance to other RTUs.

7. This method of channel allocation repeats and there is no possibility of collision at all.

8. Once all the channels complete the data transmission, then they wait for the next contention period and the procedure repeats.

A flow chart for the collision free binary countdown protocol is given in Fig.3.

A. Testing of the Procedure and Results

The program developed is being run on a system consisting of one MTU and 5 RTUs. The RTUs send their address bits and type of data (n for normal data and c for critical data). The procedure takes these parameters as input arguments as shown in figure 4. When the procedure is run, it will return the results as shown in figure 5. The RTU with critical data and having higher address priority is permitted to transmit. Once it relinquishes the channel then its priority becomes 0 in the current contention period and the remaining RTUs with normal data are permitted to transmit data based on their address priority.
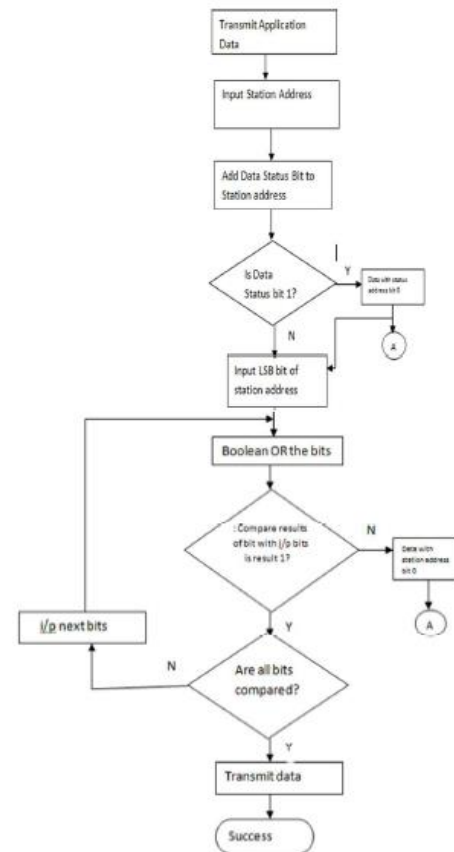

Fig.3 Flow chart for modified binary countdown protocol

Fig.4. Parameters pertaining to a system involving one MTU and 5 RTUs.

In the example shown in figure 4, there are 5 RTUs with addresses 0010,0100,1000,1010 and 1100(decimal number) and RTU 0010 is having the highest priority through RTU 1100 having least priority. Also the data is presented as critical data (c) and normal data (n). Two RTUs 1100 and 1000 have critical data. Hence, the other three RTUs though have higher address priority give up the contention. Now, only two RTUs are in race to get the channel. Of these two, the RTU having higher priority will get the channel to transmit first, and then other RTU will be allocated with the channel. Thus, RTU 1000 gets the channel first followed by 1100. These two RTUs priority becomes zero after transmission and will become quiescent till the start of the next contention slot. Then the remaining three RTUs having normal data are allocated with channel based on their address priority. The results of channel allocation are shown in figure 5.

```
Assigning the channel to RTU Number 1000
Transmitting the data 1001

Assigning the channel to RTU Number 1100
Transmitting the data 101

RTU data Display after sorting according to priority
Priority        Address Data    Type
4       10      1000    n
1       100     1010    n
0       1000    1001    c
3       1010    1100    n
0       1100    101     c
Assigning the Channel to RTUs with non-critical data
Assigning the channel to RTU Number 10
Transmitting the data 1000

Assigning the channel to RTU Number 100
Transmitting the data 1010
```

Fig.5. Results of the channel allocation

B. Design of Moore finite state machine:

A state table is developed for the channel allocation using binary countdown method and is shown in figure 6. While accessing the channel a RTU makes transition from one state to another state and finally finds itself to be in one of the states viz idle, testing the channel, contention, randomly waiting, waiting during the contention period or transmitting. The Moore finite state machine is designed and synthesized by constructing the transition table and excitation table shown in table 1 and 2 respectively. The minimal expressions are derived using K-map. Further, the machine can be simplified by state reduction. The JK flip flops are used here, as it leads to minimal external hardware. The finite state Moore machine is shown in fig. 7.
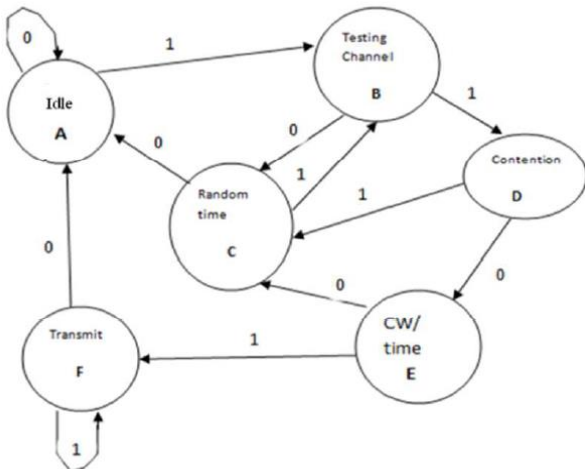

Fig.6 State diagram for binary countdown protocol

TABLE I: TRANSITION TABLE

PS			NS $Q_1^+Q_2^+Q_3^+$		Z1	Z2	Z3
	Q1	Q2	Q3	x=0	x=1			
A	0	0	0	000	001	0	0	0
B	0	0	1	010	011	0	0	1
C	0	1	0	000	001	0	1	0
D	0	1	1	100	010	0	1	1
E	1	0	0	010	101	1	0	0
F	1	0	1	000	101	1	0	1
X	1	1	0	XXX	XXX	X	X	X
X	1	1	1	XXX	XXX	X	X	X

TABLE I: EXCITATION TABLE

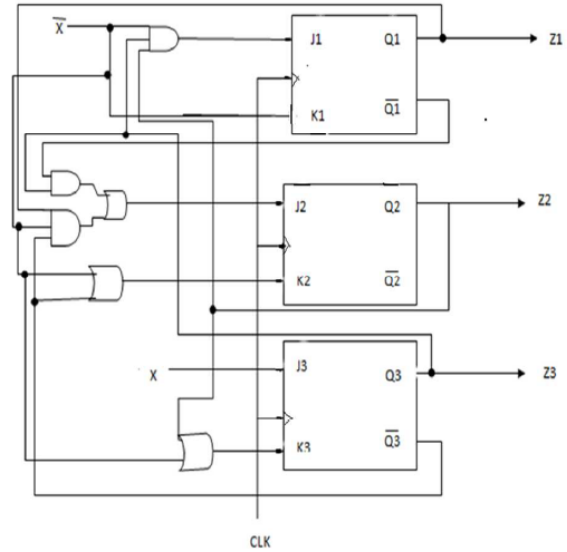| Q1	Q2	Q3	X	Q1*	Q2*	Q3*	J1	K1	J2	K2	J3	K3	Z1 Z2 Z3
0	0	0	0	0	0	0	0	X	0	X	0	X	000
0	0	0	1	0	0	1	0	X	0	X	1	X	000
0	0	1	0	0	1	0	0	X	1	X	X	1	001
0	0	1	1	0	1	1	0	X	1	X	X	0	001
0	1	0	0	0	0	0	0	X	X	1	0	X	010
0	1	0	1	0	0	1	0	X	X	1	1	X	010
0	1	1	0	1	0	0	1	X	X	1	X	1	011
0	1	1	1	0	1	0	0	X	X	0	X	1	011
1	0	0	0	0	1	0	X	1	1	X	0	X	100
1	0	0	1	1	0	1	X	0	0	X	1	X	100
1	0	1	0	0	0	0	X	1	0	X	X	1	101
1	0	1	1	0	1	0	X	0	0	X	X	0	101
1	1	0	0	X	X	X	X	X	X	X	X	X	XXX
1	1	0	1	X	X	X	X	X	X	X	X	X	XXX
1	1	1	0	X	X	X	X	X	X	X	X	X	XXX
1	1	1	1	X	X	X	X	X	X	X	X	X	XXX

Fig .7 Moore finite state machine

VHDL model for Moore finite state machine and Simulation results: The digital device i.e. a finite state machine is modeled using VHDL. The VHDL code is written using sequential style of modeling. The simulation results for two sets of states are presented in figure 8 and 9 respectively. The results clearly indicate that how a RTU is making transition from one state to another state.
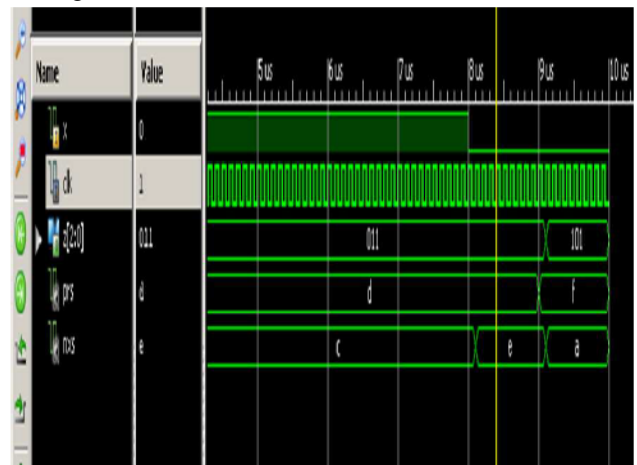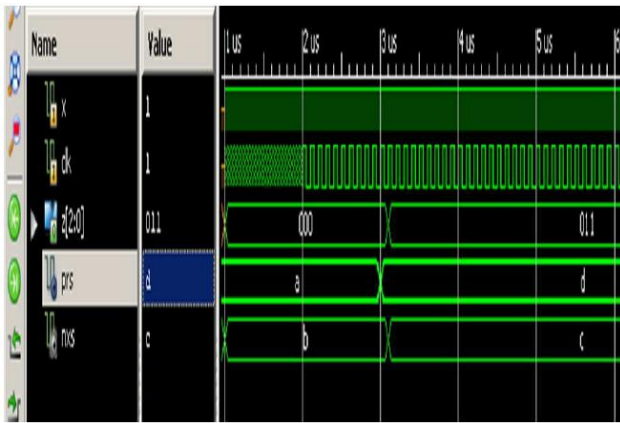

Fig.8. Simulation results of Moore VHDL model

Fig.9.Simulations results of Moore VHDL model

C. Results and Discussion

The results obtained by running the procedure are as shown in figures 4 and 5, clearly indicate that the performance of this method of channel allocation is superior to the existing CSMA/CD protocols in terms of efficiency and free from collision. Further, the requirement of critical data to reach the MTU first to augment the generation of the command signals can be achieved. This method is a promising solution for channel allocation in real time operation and control of critical infrastructures employing SCADA to achieve benefits like production efficiency, reliability, personal and plant safety. The simulation results of the VHDL model also demonstrate the state transition made by the hardware in a RTU while accessing the channel without leading to collision for smooth operation of critical infrastructures.

VI. CONCLUSION

The modified binary countdown collision free protocol for medium access control, discussed in this paper is a unique and novel approach. It overcomes the problems of collision and lower efficiency associated with the existing CSMS/CD protocols. The results of the procedure reiterate that there is no collision and efficiency is very close 100%. The need of classifying operational data into normal and critical data is emphasized in this work and algorithm demonstrate that the critical data is transmitted first followed by the normal data and subsequently giving fair chance for all RTUs to seize channel for data transmission. The generic nature of the algorithm makes it suitable for SCADA applied to control any plant/process/system. It is also demonstrated through simulation results of VHDL model that the protocol can be implemented through hardware. Hence, looking to the advantages of collision free protocol and the results obtained asserts that it can be the best MAC protocol for most of SCADA applications.

REFERENCES

[1] Joaquin Luque and Isabel Gomez "The role of Medium Access Control Protocols in SCADA systems" , by Dept of Electronic technology, University of Seville.
[2] International Organisation for Standardization: "Information processing system-Open system Interconnection- Basic Reference model ", ISO Standard 7498,1984.
[3] International Electrotechnical Commission TC% and ,"Telecontrol Equipment and systems part 5.1 Transmission frame formats " International standard, Geneva 1990.
[4] J.Luque, J.I. Escudero: "Measurement Transmission in Power Control Centres ", IEEE MELECON '91, Ljubljana, May 1991.
[5] J.Luque, J.I. Escudero, Isabel Gomez, "Differential Transmission Of Evolution Measures in SCADA Systems ", IEEE Proc.-Gener. Trans-Distrib., Vol 141,No 3. May 1994.
[6] The Institute of Electrical and Electronics Engineers, carrier sense Multiple Access with collision Detection (CSMA/CD) Access method and Physical Layer Specifications, American National Standard ANSI/IEEE std, 802.3.1985.
[7] J.Luque, J.I. Escudero, Isabel Gomez, "Determining the Channel Capacity in SCADA Systems using Polling Protocols", IEEE Power Engineering Society, Summer Meeting, July 1995.
[8] H.Tkagi, L.Kleinrock, "Throughput Analysis for Persistent CSMA Systems", IEEE Transaction on Communications, Vol. 33 No 7. July 1985.
[9] F.A.Tobagi, V.B.Hunt, "Performance Analysis of carrier sense Multiple Access with Collision Detection", Computer Networks 4,1980.
[10] S.S.Lam, "A Carrier sense Multiple Access Protocols for Local Network", Computer Networks 4,1980.
[11] H.Takagi,S.Yamada,S.Sugawara,"CSMA/CD with Deterministic contention Resolution", IEEE J. Selected Areas on Communications, Vol. SAC-1, No.5 July 1985.
[12] Andrew S.Tanenbaum and David J.Wether all text book on Computer Networks (V edition) and David J. (oct 7,2010)