An Eradication of Malicious node Attack using a Priority Aware Frequency Domain Polling in Cyber Physical Systems

Saritha .Ibakkanavar.Guddappa[1],Dr.Rajeshwari Mahabhaleshwar Hegde [2]

[1] Asst professor , Dept. of Electronics and Telecommunication Engg , BMSreenivasaiahInstitute of Technology and Management ,Bengaluru, India

[2]Professor ,Dept of Electronics & Telecommunication Engg ,BM Sreenivasaiah College of Engineering Bengaluru, India

[1]sarithaig1224@gmail.com ,[2]rajeshwari.hegde@gmail.com

Affiliated to Visvesvaraya Technological University, Belegavi, Karnataka, India

Abstract: Cyber-Physical Systems (CPS) is a modern generation of intelligent systems with the integrated computational performance and physical capacities. The CPS is affected by the malicious attacks due to the growth of system complexity and system openness. Therefore, an efficient data transmission method is developed to improve the CPS performances. In this paper, the Orthogonal Frequency-Division Multiplexing (OFDM) based transmission device is used in the CPS to achieve the high data rate requirement of modern communications. The Priority Aware Frequency Domain Polling (PAFDP) protocol is proposed to detect the desired node from the group of nodes based on the priority value. Here, the priority is identified by using the throughput and data rate. Moreover, the malicious nodes existing in the network are identified and avoided to minimize the packet loss in the network. The performances of the PAFDP-OFDM-CPS are analysed in terms of packet delivery rate, packet loss ratio, throughput and overhead. The PAFDP-OFDM-CPS method is evaluated by using three existing methods such as Trust Aware Wireless Routing Protocol (TAWP), Trust Aware Routing Framework (TARF) and Adaptive Duty Cycle Control Based Opportunistic Routing (ADCCOR) protocol. It was found that the PDR of the PAFDP-OFDM-CPS is 99.4% for 5 malicious nodes high compared to the TAWP and TARF protocol.

Keywords: Cyber-physical systems, Malicious nodes, Orthogonal frequency-division multiplexing, Priority aware frequency domain polling protocol.

1. Introduction

Cyber-Physical System (CPS) is a real time integration of physical and the cyber world as well as it is a fundamental model of the 4th industrial revolution along with the features of the hyper-intelligence, hyper-connectivity and hyper-automation [16][23]. The fusion between the physical and cyber part is obtained based on the following four operations such as sensing the physical system state using data acquisition devices, data analysis using computation, physical objects controlling using instructions and create a closed loop to obtain automatic data flow in the network [2] [3]. The CPS uses a different type of autonomous and intelligent devices such as robots, smart meters, actuators, sensors, controllers, servers and gateways to accomplish the monitoring operations [17]. In CPS, the physical quantity is observed by using a group of sensors. The sensors of the CPS are used to monitor different physical phenomena such as humidity, temperature, rotating speed and pressure from the physical world [14]. The developed CPSs are considered as bases of modern critical infrastructures such as chemical plants, transportation, water treatment and smart grids [5] [21].

The susceptibility of the malicious attacks in the CPS are increased due to growing communication networks in the monitoring and controlling of physical systems. Subsequently, the design of resistance against the malicious attacks is difficult in the network controlled systems [7] [22]. Moreover, the CPS is affected by the malicious cyber-attacks due to the open nature of the sharedcommunication that interrupts the function of the physical part of the process [4] [10]. The conventional cyber security methods such as authentication and encryption are ineffective, when the systems are processed under the constraints of insider and physical attacks [18]. In CPS, the complex algorithms utilize for authentication verification, cryptography, integrity test and intrusion detection require huge amount of storage capacity memories [9]. The major contributions of this research paper are given as follows:

- The OFDM transmission device is used in the CPS for achieving the higher data rate requirements of the modern communications.
- In OFDM based CPS, the PAFDP protocol is used to detect the node with higher priority that leads to minimize the waiting time of the nodes.
- Moreover, the malicious nodes in the network are identified and the identified nodes are avoided from the normal nodes to secure the data transmission in the CPS.

The overall organization of the paper is as follows: The related work carried out on the recent techniques related to the secure CPS is given in section 2. The problem statement found from the existing researches along with the solution is described in the section 3. The proposed priority aware frequency domain polling protocol is described in the section 4. The results and discussion of the PAFDP-OFDM-CPS method is described in the section 5. Finally, the paper is concluded in section 6.

2.Related Work

Zhao. Z, Yang, Y., Li, Y. and Liu, R [1] presented the investigation of the security issues of CPS under undetectable attacks. The design, implementation and impact estimation of undetectable attacks were evaluated by using the geometric control. In this CPS, the feed forward-feedback structure was developed to create the undetectable attacks. The attack feedback gain of the feed forward-feedback structure was developed through the pole placement of attacked system. Here, three different attacks were considered in the realization of undetectable attack such as actuator attacks, sensorattacks, and coordinated actuator and sensor attacks. This work failed to analyze the packet delivery rate and delay while analyzing the undetectable attacks in CPS.

Xiang, X., Liu, W., Liu, A., Xiong, N.N., Zeng, Z. and Cai, Z [12] developed the ADCCOR method to obtain the lesser power consumption and higher reception rate. The important development of the ADCCOR method was mainly depends on the characteristics of the energy consumption in Wireless Sensor Network (WSN). The amount of awakened nodes was increased in the ADCCOR method, when the transmitter node required to transmit the data to the desired location. Moreover, the delay was minimized in network based on the dynamic adjustment of the duty cycle of sensor node. The delay of the ADCCOR method was increased, when transmitter node selected the relay node with higher distance from the sink. Moreover, this ADCCOR method doesn't provide any enough security to secure the data transmission.

Gifty, R, Bharathi, R. and Krishnakumar, P [6] developed the host-based probability intrusion detection by using maximum likelihood estimation and Weibull distribution method. Here, the normal nodes in the CPS were detected by using the compliance degree. This intrusion detection method was used to analyze various parameters such as failure rate and reliability in the CPS along with malicious errors. The probabilities of false positive were used to analyze the system response strength. Moreover, this probability value was used to optimize the system reliability. However, the computationof compliance degree was inaccurate because of the noise and communication errors present in the CPS. But, the compliance degree used to validate the node's state was varied based on the communication errors and noise.

Shi. D,Elliott, R.J. and Chen, T , [19] presented the stochastic modeling framework to formulate and solve the adversary attacks in CPS. The finite-state Hidden Markov Model (HMM) with the probability matrices of switching transition were used to develop the stochastic modeling framework. Here, the Markov decision process was used to control the probability matrices of switching transition. The change of probability measure was used in the finite state HMM to formulate and solve the joint state and attack estimation issue. Moreover, the marginal normalized conditional distributionswere used to estimate the attack and appropriate state.

Qureshi, N [20] presented the trust aware wireless routing protocol (TAWP) to identify and isolate the malicious attacks from WSN. This TAWP was usedfour steps such as information gathering, trust analyzing and ranking, route discovery and route selection for identifying an appropriate route among the trusted nodes. In this TAWP, trust analyzer was used to verify the trustworthiness of nodes in network. This trust information was used to identify an optimal route between the nodes. Finally, the data was transmitted and stored in the trust database. The data transmission was affected as well as the source directly stop and eliminated the route, when the misbehaving was occurred during the data transmission.

Chen. ALi, X., Ni, X. and Luo, G., [15] presented the Reliability and Timeliness Guaranteed Opportunistic Routing (RTGOR) protocol to obtain the reliable CPS data transmission. The RTGOR protocol was developed using the opportunistic routing method as well as this RTGOR protocol was integrated with quantified transmission reliability and time guarantees. In CPS, the transmission performance was increased by considering the link delay and transmission time in RTGOR protocol. However, this work doesn't consider the security against malicious attacks that caused the packet drop through the network.

3.Problem statement

The problems found from the existing research works along with the solution to overcome the identified problems using PAFDP-OFDM-CPS method are described in this section.

The communication errors and noise varied the compliance degree that affects the identification of node states over the CPS [6]. The route is discarded and data transmission is affected due to misbehaving occurred during the data transmission through CPS [20]. If the network doesn't consider any security scheme, the data transmission through the network is affected due to the malicious attacks [15]. The CPS without enough security causes the packet loss while transmitting the data packets. If the distance between the relay node and sink is high, the Adaptive Duty Cycle Control Based Opportunistic Routing (ADCCOR) method obtains higher delay over the CPS [12].

Solution:

The PAFDP method is used to select the node which has higher priority. Here, the priority of the nodes is identified by using the throughput and data rate. This polling protocol helps to minimize the transmission delay while transmitting the data from the OFDM transmitter to the receiver. Moreover, the packet drop occurred in each node is analysed to detect the malicious nodes from the network. Therefore, the malicious node is identified and avoided based on the identification of the malicious node. This malicious node identification leads to minimize the packet loss occurred in the data transmission.

4.PAFDP-OFDM-CPS method

In the PAFDP-OFDM-CPS method, a secured OFDM based CPS network is developed to satisfy the high data rate requirements of modern communications. The PAFDP protocol is developed to detect the node with higher priority.

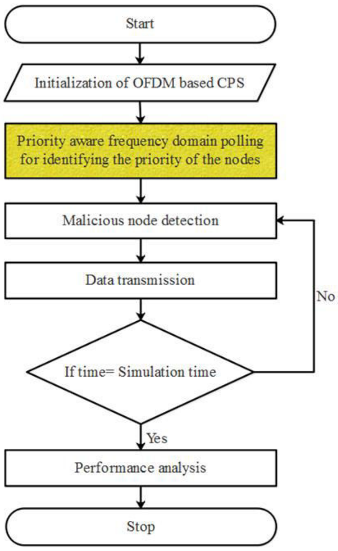
Start
Initialization of OFDM based CPS
Priority aware frequency domain polling for identifying the priority of the nodes
Malicious node detection
Data transmission
No
If time= Simulation time
Yes
Performance analysis
Stop

Figure 1. Flowchart of the PAFDP-OFDM-CPS method

The throughput and data rate are used to compute the priority of the nodes in OFDM based CPS. Additionally, the packet drop of the nodes in the CPS are identified to detect and avoid the malicious nodes. Therefore, the throughput of the PAFDP-OFDM-CPS method is increased. The flowchart of the proposed method is shown in the Figure 1.

4.1. System model

In this OFDM based CPS, the high data rate serial input is changed into a parallel lower data rate bit stream. Subsequently, the converted parallel lower data rate bit is transmitted over the signal mapper and it is given to the IFFT. The cyclic prefix is added in the input data stream to remove the inter symbol interference. The inputs given to the IFFT are converted into time domain signals and the OFDM modulated baseband signal is expressed in the equation (1). The input data is again transformed asparallel to serial data and it is transmitted through the wireless channel.

$$x(g) = \frac{1}{\sqrt{G}}\sum_{s=0}^{G-1} X_s e^{-\frac{j2\pi sg}{G}}, \quad g = 0,1, \dots ., G - 1(1)$$

Where, the gth sample of the OFDM transmitted signal at time domain is represented as $x(g)$; total amount of OFDM subcarriers are G and the modulated symbol at frequency domain in the sth subcarrier is X_s.The received signal(y) after processing through the wireless channel is specified in the equation (2).

$$y(g) = hx(g) + w(g) \qquad (2)$$

Where, the channel gain is represented as h and additive white noise is represented as w.

4.1 **Design of Priority-Aware Frequency Domain Polling in CPS**

At first, the OFDM based CPS is considered with one sink and K number of nodes. The communication channel of OFDM with bandwidth $(B)$is divided as 2S overlapping narrow band subcarriers. Next, the divided subcarrier has constant noise power density $N_0$and equal bandwidth. This OFDM only uses the even subcarriers for overcoming the severe co-channel interference. Moreover, the polling and one transmission transit gap, each frame contains a D time slots to accomplish the OFDMA transmission. The packet transmitted to the sink is obtained in the preferred deadline (T frames) or the transmitted packets are discarded during the communication. The polling of nodes and priority aware resource (i.e., frequency) allocation between the nodes are obtained by using the PAFDP that leads to achieve the reliable transmission. Moreover, the PAFDP generates the preamble phase as shown in Figure 2 in that the sink transmits the preamble to obtain the time synchronization in the OFDM network. The priorities of the nodes in the OFDM are collected based on the priority-aware polling response in frequency domain. Here, the priorities are calculated by using both the throughput and data rate of each node. From the polling results, the sink solves the uplink OFDM frequency allocation issue to achieve reliable data transmission.After the Short Inter Frame Space (SIFS) time, the aggregate acknowledgement (ACK) from the sink is used to acknowledge the transmissions occurred in the data transmission phase. Moreover, the scheduled node only sends one packer in 1 frame, however this packet occupies up to D slots.

The node priorities are categorized into various levels during data transmission. In PAFDP, the node k (k=1,2,….,K) is allocated along with T_k subcarriers (i.e.,s_(k,1),s_(k,2),…,s_(k,T_k)).
Here, the subcarriers are used along with data rate and throughput to calculate the node’s transmission priorities. The node priorities is represented as A_(k,i) and the labels in the increasing manner are specified as 1=A_(k,1)≤A_(k,2)≤A_(k,T_k)=T_k.

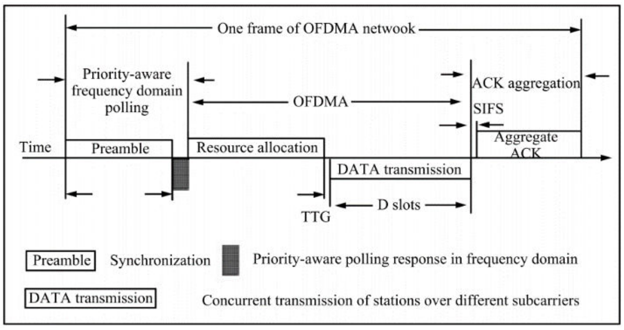
One frame of OFDMA netwook
Priority-aware frequency domain polling
OFDMA
ACK aggregation
SIFS
Aggregate ACK
Time
Preamble
Resource allocation
DATA transmission
D slots
TTG
Preamble
Synchronization
Priority-aware polling response in frequency domain
DATA transmission
Concurrent transmission of stations over different subcarriers

Figure 2. Structure of the PAFDP protocol

The priorities of the nodes are increased for next time frame, when the packets are not successfully transmitted in the current time frame. Based on the node priorities, the nodes in the OFDM transmits the data packets to the sink in each time frame.

Moreover, the reliability of the OFDM based CPS is affected, when the malicious attacks requests for high priority during the communication. In that time, the CPS considers the packet drop of the nodes (i.e., more than 50% of packet loss) to avoid the malicious attacks while transmitting the packets.

Formulation for OFDM based data transmission

The combination of OFDM based CPS with PAFDP is leads to minimize the packet loss than the traditional OFDM network. The subcarriers are used for data transmission, once the priority aware polling is completed for the nodes of OFDM. Consider G={1,2,3,..,G} is a set of available subcarriers for OFDM.

The Multiple Quadrature Amplitude Modulation (MQAM) is used by the physical layer of the OFDM network. The Bit Error Rate (BER) of OFDM based CPS with respect to the Signal to Noise Ratio (SNR) and modulation factor (M) is expressed in the equation (3).

$$P(M) = \frac{4}{\log_2 M}\left(1 - \frac{1}{\sqrt{M}}\right) Q\left(\sqrt{\frac{3\gamma}{M-1}}\right) \qquad (3)$$

where, $Q(x) = \frac{1}{\sqrt{2\pi}}\int_x^\infty \left(-\frac{t^2}{2}\right) dt$ and γ represents the SNR.

The BER for the kth node, when it is communicated with the subcarrier $s\epsilon G$ with $M_{k,s}$-QAM is shown in the equation (4).

$$P_{k,s}^{BER} = \frac{4}{\log_2 M_{k,s}}\left(1 - \frac{1}{\sqrt{M_{k,s}}}\right) Q\left(\sqrt{\frac{3\gamma_{k,s}}{M_{k,s}-1}}\right) (4)$$

Where, $\gamma_{k,s} = \frac{p_{k,s}h_{k,s}}{N_0 B}$; $\gamma_{k,s}$, $h_{k,s}$ and $p_{k,s}$represents the SNR at sink, channel gain through the sth subcarrier and kth node's transmission power respectively. Moreover, the $h_{k,s}$ is constant in each time frame, when the coherence time of channel is higher than one frame at OFDM network.

The kth node packet error rate is calculated as shown in equation (5) by considering the $L$is the packet size.

$$e_{k,s} = 1 - (1 - P_{k,s}^{BER})^L \qquad (5)$$

Where, the packet error rate is denoted as $e_{k,s}$. Next, a set of binary variables $\delta_{k,s}$ is considered equal to 1, when the subcarrier is allocated to the k th node otherwise the $\delta_{k,s}$ is specified as 0. Equation (6) expresses the probability of the kth node packets that doesn't reach to the sink at D time slots.

$$\Pr(k) = \beta_{P_k} \prod_{s=1}^{G} \prod_{t=1}^{D} \left(e_{k,s}(t)\right)^{\delta_{k,s}(t)} \quad (6)$$

Where, the timeout probability is represented as Pr; the$k$th station priority coefficient is denoted as $\beta_{P_k}(0 \leq \beta_{P_k} \leq 1)$ and this priority coefficient is used to evaluate the packet's timeout probability along with priority P_k.

In this PAFDP-OFDM-CPS method, the priority of the nodes are collected based on the PAFDP protocol. The calculation of priority values using the throughput and data rate are used to detect the desired nodes from the OFDM based CPS. Additionally, the packet drop of all nodes are analysed for detecting and eliminating the malicious nodes during the communication. This helps to minimize the packet loss in the OFDM based CPS.

5.Results and discussion

The results and discussion of the PAFDP-OFDM-CPS method is described in this section. The implementation and simulation of this proposed method with OFDM based CPS is carried out by using the Network Simulator (NS) 2.35 that is operated on a Windows 8 operating system with Intel core i3 processor and 4GB RAM. In this method, the node polling is obtained by using the PAFDP protocol. Additionally, the malicious nodes in the OFDM based CPS is identified based on the packet drop occurred at each node. Here, the OFDM based CPS is initialized with 100 nodes over the area of 500×500m^2. The specifications considered for this PAFDP-OFDM-CPS method is shown in the Table 1.

Parameter	**Value**
Number of nodes	100
Area	$500 \times 500m^2$
Channel	Wireless channel
Propagation	Two ray ground propagation
Antenna	Omni antenna
Queue	Priority queue
Length of the queue	200
MAC type	Mac/802_11

Table 1. Specification parameters

5.1. Performance analysis

The performance of the PAFDP-OFDM-CPS method is analysed in terms of Packet Delivery Ratio (PDR), Packet Loss Ratio, throughput and overhead. The performance of this method is evaluated and compared with the TAWP [20], TARF [20] and ADCCOR [12] by varying the number of malicious nodes from 1-5.

5.1.1 Packet delivery ratio

PDR is the ratio between the number of packets received at the sink and number of packets transmitted by the OFDM transmitter which is expressed in the equation (7).

$$PDR = \frac{\sum_{i=1}^{n} Y_i}{\sum_{i=1}^{n} X_i} \times 100 \qquad (7)$$

Where, the number of packets received by the sink is represented as Y; the number of packets transmitted by the source is represented as X and amount of source nodes in the OFDM based CPS is represented as i.

Number of malicious nodes	TAWP in %	TARF in %	PAFDP-OFDM-CPS in %
0	100	100	100
1	87	85	99.65
2	83	77	99.5
3	80	60	99.3
4	73	50	99.6
5	60	40	99.4

Table 2. PDR for varying malicious nodes

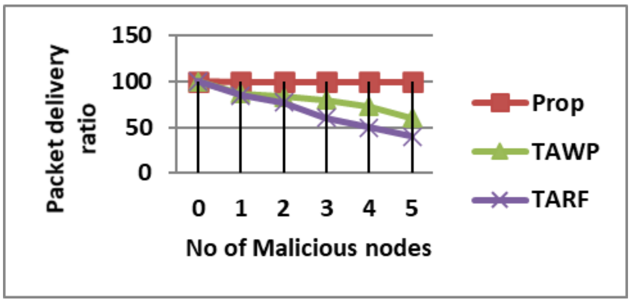

Figure 3. PDR comparison

The PDR of the PAFDP-OFDM-CPS method is increased of 99.4% based on the mitigation of malicious nodes in the OFDM based CPS comparably with TAWP [20] and TARF [20] where the PDR are 60% and 40% respectively as shown in table 2 and figure 3

5.1.2 Packet loss ratio

PLR is defined as the ratio between the amount of dropped packets and number of packets transmitted by the OFDM transmitter. Equation (8) shows the expression for the PLR.

$$PLR = \frac{\sum_{i=1}^{n} X_i - Y_i}{\sum_{i=1}^{n} X_i} \times 100\% (8)$$

Number of malicious nodes	TAWP in %	PAFDP-OFDM-CPS in %
1	11.4	0.07
2	10.55	0.1

3	**12.29**	**0.14**
4	**12.58**	**0.08**
5	**10.58**	**0.12**

Table 3. PLR for varying malicious nodes

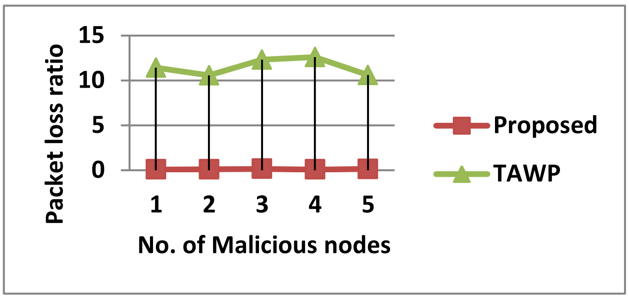

Figure 4. PLR comparison

The PLR of the proposed method is reduced of 0.12% for 5 malicious nodes when compared to the TAWP [20] which is 10.58% due tomisbehaving of the nodes in the networkas shown in table 3 and figure 4

5.1.3. Overhead

Overhead is defined as the ratio between the total amount of control packets created by the nodes in the network which is expressed in the equation (9).

$$Overhead = \sum_{j=1}^{n} R_j (9)$$

Where, the amount of nodes that created the control packets is represented as j and the control packets are denoted as R.

Number of malicious nodes	TAWP	TARF	PAFDP-OFDM-CPS
0	0	0	0
1	1	1.5	1.3
2	1.4	2	1.4
3	1.9	3	1.7
4	2	4	2.2
5	2.9	5.6	2.6

Table 4. overhead for varying malicious nodes

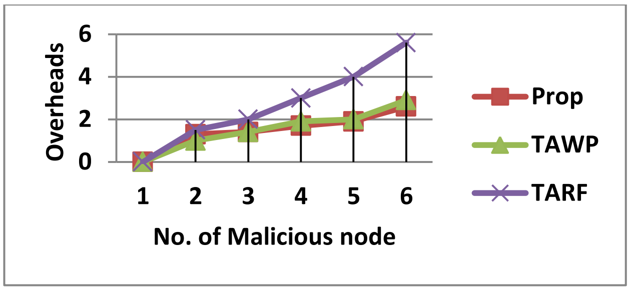

Figure 5. overhead comparison

The overhead of the proposed method is2.6 control packets for 5 malicious nodes which is less due to priority when compared to TAWP [20] and TARF [20] as shown in table 4 and figure 5

5.1.4 Throughput

Throughput is defined as the number of packets successfully received by the sink in the total time interval that is shown in equation (10).

$$Throughput = \frac{Y_i}{TI}(10)$$

Where, TI defines the time interval and $Y_i$specifies the packets received at the sink.

Number of malicious nodes	TAWP in bps	PAFDP-OFDM-CPS in bps
1	76.46	162.19
2	83.88	163.95
3	75.39	161.89
4	70.29	162.14
5	69.38	160.96

Table 5. Throughput for varying malicious nodes

The throughput of the proposed method is 160.96 for 5 malicious nodes compared to the TAWP [20] as shown in table 5 and figure 6 .

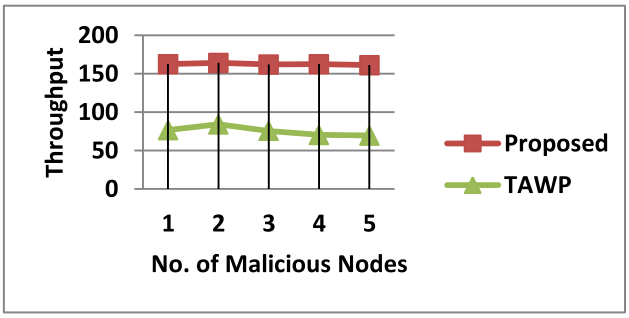

Figure 6. Throughput comparison

5.1.5 Energy consumption and Delay

The average energy consumption and average end to end delay of the proposed method is minimized compared with ADCCOR [12] protocol by varying the distance to the sinkfrom 100 m to 500 m as shown in table 6, figure 7 and figure 8.

Distance to the sink (m)	Average energy consumption (j)		Average End to End Delay (s)	
	ADCCOR [12]	PAFDP-OFDM-CPS	ADCCOR [12]	PAFDP-OFDM-CPS
100	0.0073	0.0070	12.5	10.3
200	0.00725	0.00692	30	18.6
300	0.00725	0.00693	40	32
400	0.00715	0.0069	55	43
500	0.0072	0.0070	62.5	56

Table 6. Energy consumption and Delay

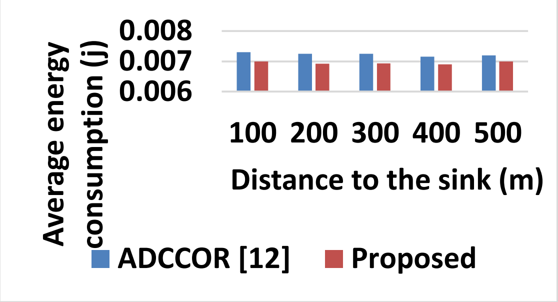

Figure 7. Average energy consumption comparison

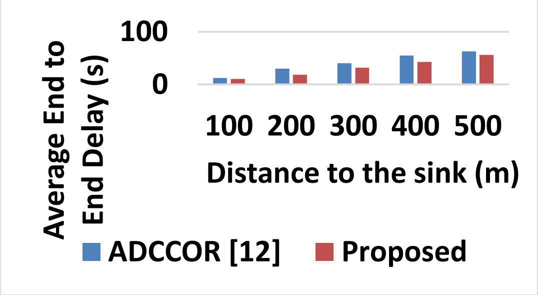

Figure 8. Average end to end delay comparison

6. Conclusion

In this paper , priority aware polling is developed using OFDM based CPS for obtaining a reliable communication and effective polling between the nodes. The priority of the nodes is identified by using the data rate and throughput. The developed PAFDP protocol is used to minimize the waiting time while transmitting the data packets and malicious nodes in the network is identified based on the packet drop occurred in each node. Therefore, the proposed PAFDP-OFDM-CPS method is used to achieve high data rate to satisfy the modern communication systems compared to the existing methods. The proposed method gives better performance in respect of the PLR, Overhead, Throughput and the PDR of is 0.12%, 2.6 control packets ,160.96 bps and 99.4% respectively for 5 malicious nodeswhen compared to TAWP, TARF and ADCCOR. In future, a frequency interleaved polling can be used to eliminate polling overflow in CPS.

Notation list:

Notation	Description
x	OFDM transmitted signal
G	Total amount of OFDM subcarriers
X_s	Modulated symbol at frequency domain in the sth subcarrier
y	Received signal
h	Channel gain
w	Additive white noise
N_0	Constant noise power density
B	Bandwidth
k	Node
$A_{k,i}$	node priorities
M	modulation factor
P	Bit error rate of OFDM based CPS
γ	SNR
$p_{k,s}$	kth node's transmission power
$e_{k,s}$	packet error rate
Pr	timeout probability
β_{P_k}	priority coefficient
R	control packets
TI	time interval

7.Conflicts of Interest:I Saritha I G , Asst Professor , Dept ETE, BMSIT&M ,declaring no conflict of interest and I am motivated to implement this proposal due to the multiple Subcarrier in OFDMA may used for CPS to reduce co channel interference.

8. **Author Contributions**: As there are two authors involved in this work , Rajeshwari M Hegde have contributed "Conceptualization, methodology, software, validation, formal analysis, investigation, resources, data curation and Myself Saritha I G contributed writing—original draft preparation, writing—review and editing, visualization, supervision, project administration, funding acquisition, etc.

9.References

[1] Zhao, Z., Yang, Y., Li, Y. and Liu, R., 2020. Security analysis for cyber-physical systems under undetectable attacks: A geometric approach. *International Journal of Robust and Nonlinear Control*, 30(11), pp.4359-4370.

[2]Lyu, X., Ding, Y. and Yang, S.H., 2020. Bayesian Network Based C2P Risk Assessment for Cyber-Physical Systems. *IEEE Access*, 8, pp.88506-88517.

[3] Yuan, Y. and Mo, Y., 2020. Security for cyber-physical systems: Secure control against known-plaintext attack. Science China Technological Sciences, pp.1-10.

[4]Ning, X. and Jiang, J., 2020. In the mind of an insider attacker on cyber-physical systems and how not being fooled. IET Cyber-Physical Systems: Theory & Applications, 5(2), pp.153-161.

[5] Zhang, Y. and Yağan, O., 2019. Robustness of interdependent cyber-physical systems against cascading failures. *IEEE Transactions on Automatic Control*, 65(2), pp.711-726.

[6]Gifty, R., Bharathi, R. and Krishnakumar, P., 2019. Privacy and security of big data in cyber physical systems using Weibull distribution-based intrusion detection. *Neural Computing and Applications*, 31(1), pp.23-34.

[7]Lima, P.M., Alves, M.V.S., Carvalho, L.K. and Moreira, M.V., 2019. Security against communication network attacks of cyber-physical systems. *Journal of Control, Automation and Electrical Systems*, 30(1), pp.125-135.

[9]Mili, S., Nguyen, N. and Chelouah, R., 2019. Transformation-Based Approach to Security Verification for Cyber-Physical Systems. *IEEE Systems Journal,* 13(4), pp.3989-4000.

[10]Kim, S., Won, Y., Park, I.H., Eun, Y. and Park
, K.J., 2019. Cyber-physical vulnerability analysis of communication-based train control. *IEEE Internet of Things Journal*, 6(4), pp.6353-6362.

[11]Sowmyashree M S, C S Mala, September 2019Development of a Novel Protocol for Improvement of Qos Inwireless Sensor Networks: P-Rpeh,*International Journal of Recent Technology and Engineering* (IJRTE) ISSN: 2277-3878, Volume-8 Issue-3

[12]Xiang, X., Liu, W., Liu, A., Xiong, N.N., Zeng, Z. and Cai, Z., 2019. Adaptive duty cycle control–based opportunistic routing scheme to reduce delay in cyber physical systems. *International Journal of Distributed Sensor Networks,* 15(4), p.1550147719841870.

[13]Fu, R., Huang, X., Xue, Y., Wu, Y., Tang, Y. and Yue, D., 2018. Security assessment for cyber physical distribution power system under intrusion attacks. *IEEE Access*, 7, pp.75615-75628.

[14]Orojloo, H. and Azgomi, M.A., 2018. A stochastic game model for evaluating the impacts of security attacks against cyber-physical systems. *Journal of Network and Systems Management*, 26(4), pp.929-965.

[15]Chen, A., Li, X., Ni, X. and Luo, G., 2018. RTGOR: Reliability and Timeliness Guaranteed Opportunistic Routing in wireless sensor networks. EURASIP *Journal on Wireless Communications and Networking,* 2018(1), p.86.

[16]Lee, B.M. and Yang, H., 2017. Massive MIMO for industrial Internet of Things in cyber-physical systems. *IEEE Transactions on Industrial Informatics,* 14(6), pp.2641-2652.

[17]Alcaraz, C. and Lopez, J., 2017. A cyber-physical systems-based checkpoint model for structural controllability. *IEEE Systems Journal,* 12(4), pp.3543-3554.

[18]Zheng, B., Deng, P., Anguluri, R., Zhu, Q. and Pasqualetti, F., 2016. Cross-layer codesign for secure cyber-physical systems. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 35(5), pp.699-711.

[19]Shi, D., Elliott, R.J. and Chen, T., 2016. On finite-state stochastic modeling and secure estimation of cyber-physical systems. *IEEE Transactions on Automatic Control*, 62(1), pp.65-80.

[20]QURESHI, N., 2015. Malicious node detection through trust aware routing in wireless sensor networks. *Journal of Theoretical and Applied Information Technology,* 74(1).

[21]Huang, S., Zhou, C.J., Yang, S.H. and Qin, Y.Q., 2015. Cyber-physical system security for networked industrial processes. *International Journal of Automation and Computing,* 12(6), pp.567-578.

[22]Hahn, A., Thomas, R.K., Lozano, I. and Cardenas, A., 2015. A multi-layered and kill-chain based security analysis framework for cyber-physical systems. *International Journal of Critical Infrastructure Protection*, 11, pp.39-50.

[23]Wan, K. and Alagar, V., 2014. Context-aware security solutions for cyber-physical systems. Mobile Networks and Applications, 19(2), pp.212-226.

AUTHORS PROFILE

Mrs.Saritha I G completed B.E (TCE), from MVIT, Bangalore, M.Tech (Digital electronics and communication) from MSRIT Bengaluru, and Pursuing Ph.D (Cyber security) from Visvesvaraya University, Belagavi. she has 12 years of teaching, 3 years of research experience. At Present, working as Asst.Professor, ETE Dept.,BMSIT, Bengaluru. Member for professional bodies, ISTE & IAPURAI. Organized and attended many Workshops, FDPs and STTPs. Guided UG Projects . Published 11 Technical papers in National \ International journals \ Conference

Dr.Rajeshwari Hegde received her Bachelor of Engineering in Electronics and Communication Engineering from National Institute of Engineering, Mysore, Master of Engineering in Electronics from BMS College of Engineering, Bangalore and PhD from Bangalore University. She is presently associated with the Department of Electronics and Telecommunication Engineering of BMS College of Engineering, Bangalore, India. Her Research interests include embedded systems and Communication. She has published 120 research papers in reputed journals and conference.