Received: March 9, 2021. Revised: April 22, 2021.

INASS

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Priority Aware Frequency Domain Polling Protocol in Cyber Physical Systems to Ejection of Malicious Node Attack

Saritha Ibakkanavar Guddappa[1]* **Rajeshwari Mahabhaleshwar Hegde[2]**

[1]*Department of Electronics and Telecommunication Engineering,*
BM Sreenivasaiah Institute of Technology and Management, Bengaluru, India
[2]*Department of Electronics and Telecommunication Engineering,*
B M Sreenivasaiah College of Engineering, Bengaluru, India
* Corresponding author's Email: sarithaig1224@outlook.com

Abstract: Cyber-Physical Systems (CPS) is an emerging technology of intelligent systems with the united computational performance and physical capacities. Due to the growing system complexity and system directness the CPS is affected by the malicious attacks which lead to improve the CPS performances with an efficient data transmission method. In this paper , CPS making use of the Orthogonal Frequency-Division Multiplexing (OFDM) to achieve the high data rate requirement of modern communications. The Priority Aware Frequency Domain Polling (PAFDP) protocol is proposed to detect the priority based node which identified by using the throughput and data rate from the group of nodes in the network and also the priority based nodes are identified as malicious nodes which are avoided to minimize the packet loss in the existing network. The performances of the PAFDP-OFDM-CPS are analysed in terms of various QoS parameters such as delay , energy , Packet delivery ratio , packet loss ratio , through put and overhead so that the proposed method is assessed by three existing methods such as Adaptive Duty Cycle Control Based Opportunistic Routing (ADCCOR) protocol , Trust Aware Routing Framework (TARF), Trust Aware Wireless Routing Protocol (TAWRP) and It was found that the performance of the PAFDP-OFDM-CPS is improved much compared to the above said three protocols.

Keywords: Cyber-physical systems, Trust aware routing framework, Trust aware wireless routing protocol adaptive duty cycle control based opportunistic routing protocol, Malicious nodes, Orthogonal frequency-division multiplexing, Priority aware frequency domain polling protocol.

1. Introduction

Cyber-Physical System (CPS) is a real time 4th industrial revolution along with the integration of physical and the cyber world as well as fundamental model of the hyper-intelligence, hyper-connectivity and hyper-automation with various features [1, 2]. The mixture between the cyber and physical part is obtained based on the following four major operations such as sensing the state of physical system by using data acquisition devices, computation with data analysis, controlling of physical objects using instructions and create a closed loop to obtain automatic data flow in the network [3], [4]. The CPS uses a different type of independent and smart devices such as actuators, sensors, controllers, servers and gateways to accomplish the monitoring operations [5]. In CPS, the state of physical quantity is observed by a group of sensors which are used to monitor different physical phenomena such as, temperature, humidity, pressure and rotating speed from the physical world [6]. The developed CPSs are considered as fundamentals of modern critical infrastructures such as water treatment, health monitoring, chemical plants, transportation, and smart grids [7, 8].

The vulnerability of the CPS malicious attacks is increased due to growing communication networks in controlling and monitoring of physical systems. Later, the design of eradication of malicious attacks is difficult in the Controlled network systems [9, 10].

Moreover, malicious cyber-attacks over CPS is due to the exposed nature of the shared communication that disturbs the function of the physical part of the process [7, 8]. The ineffectiveness of conventional network security methods such as authentication and encryption for inside intruder [11]. Requirement of the complex algorithms in CPS utilizes huge amount of storage capacity memories for data authentication, data integrity and intrusion detection [12]. The major contributions of this research paper are given as follows:

- Achieving high data transmission using OFDM in CPS for Modern communications.
- The OFDM based PAFDP protocol in CPS, used to detect the priority based node will leads to minimize the Packet Loss Ratio and waiting time of the nodes by improving performance of throughput and Packet Delivery Ratio.
- Moreover, achieving secured data transmission in CPS is achieved by the identifying and avoiding malicious nodes from the group of nodes in the existing network are avoided in the network.

The overall organization of the paper is as follows: The literature work carried out on the recent methods related to the CPS security is given in section 2. The statement of problem found from the existing investigations along with the solution is discussed in the section 3. The proposed protocol is described in the section 4. The results and discussion of the PAFDP-OFDM-CPS method is designated in the section 5. Finally, the paper is concluded in section 6.

2. Literature survey

Zhao, Yang, Li, and Liu [13] proposed the study of the issues of CPS security under invisible attacks. The unnoticeable attacks were estimated by using the geometric control to evaluate the design, implementation and impact. The feed forward-feedback structure was developed to create the untraceable attacks in this method so that feedback gain was improved through the pole placement of attacked system. There were three different attacks considered in the realization of undetectable attack such as sensor attacks, actuator attacks and coordinated actuator. This method failed to examine delay and the packet delivery rate.

Xiang, Liu, Liu, Xiong, Zeng, and Cai [14] 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, Bharathi, and Krishnakumar [15] investigated the host-based probability intrusion detection by using Weibull distribution and maximum likelihood estimation method where normal nodes in the system were sensed by using the compliance degree. The system response strength was analysed with the probability value which was used to enhance the system reliability. However, due to the communication errors and noise in the CPS lead to inaccurate in the computation of compliance degree which was used to validate the state of the node varied based on noise and the communication errors.

Shi, Elliott, and Chen [16] identified the stochastic modelling framework to articulate and solve the challenging attacks in CPS. The stochastic modelling were developed by finite-state Hidden Markov Model (HMM) with the probability matrices of switching transition which are controlled by the Markov decision process. The joint state and attack estimation issue was solved by the change of probability used in the finite state HMM. Moreover, the attack and appropriate state were estimated by the marginal normalized conditional distributions.

Qureshi [17] investigated the TAWRP to identify and isolate the malicious attacks from WSN. This TAWRP was used four steps such as gathering of information, trust ranking and analyzing, route discovery and route selection for identifying an appropriate route among the trusted nodes. In this method, the trustworthiness of nodes in network verified by trust analyser so that this trust information was used to identify an optimal route between the nodes. Finally, the trust database stores the transmitted data which affects the data transmission so that source stop and eliminated the route, soon after the misbehaving was occurred during the data transmission.

Chen, Li, Ni, and Luo [18] developed 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 protocol was integrated with computed time guarantees and transmission reliability. In CPS,

the transmission performance was increased by considering the transmission time and link delay using this protocol. However, this method fails to consider the CPS security due to malicious attacks which causes the packet drop through the network.

3. Problem statement

This section describes the existing research work problems along with the solution to overcome using PAFDP-OFDM-CPS method.

The Noise and communication errors varied the compliance degree that affects the identification of node in the CPS [15]. Due to the misbehaviour of the node occurred during the data transmission through CPS, the route is discarded which affects the data transmission [17]. If there are multiple selfish (or malicious) nodes, which always claim the highest priority will definitely degrade the reliability performance of the existing scheme [19]. The data transmission affects due to malicious nodes, if the network doesn't consider any security scheme [18]. Without enough CPS security causes the packet loss while transmitting the data packets. The Adaptive Duty Cycle Control Based Opportunistic Routing (ADCCOR) method attains higher delay over the CPS if the distance between the sink node and relay node is high, [14].

Solution:

To overcome above said problems, the PAFDP method is used to select the priority based node where the priority of the nodes is identified and avoided by using the data rate and throughput. This polling protocol helps to minimize the transmission delay while transmitting the data from the OFDM transmitter to the receiver. Moreover, due to the detection of malicious node the packet drop occurred in each node from the network. Therefore, malicious node identification leads to minimize the packet loss in the data transmission.

4. PAFDP-OFDM-CPS method

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

In PAFDP - OFDM based CPS, priority of the nodes is computed through data rate and throughput. 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 Fig. 1.

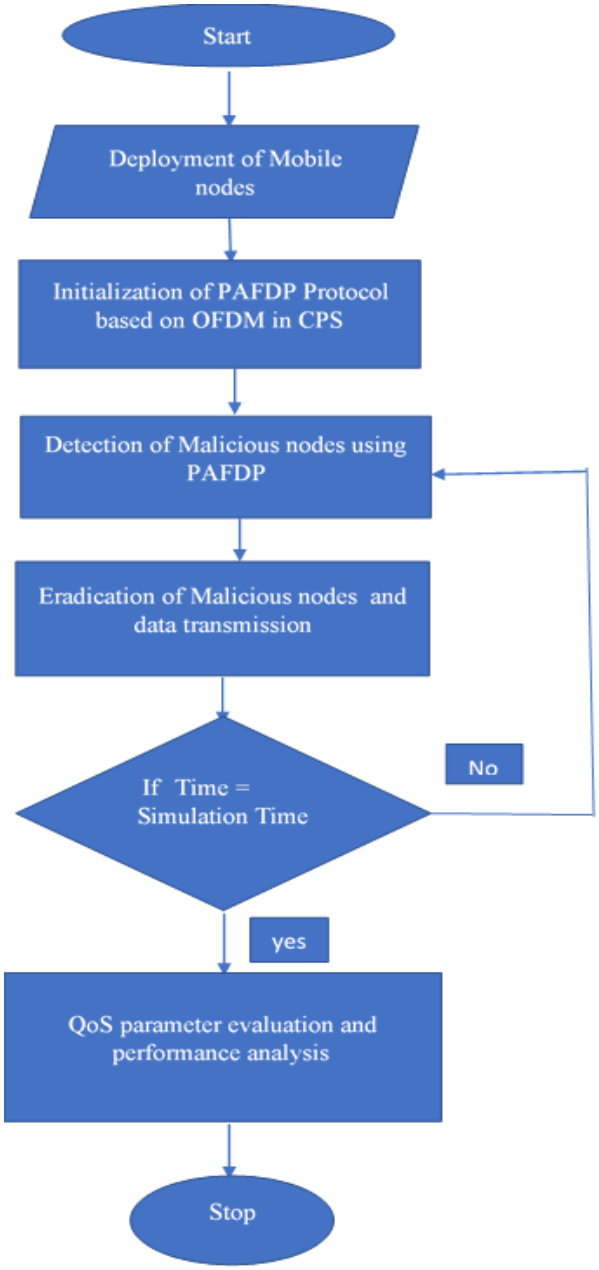

Figure. 1 Flowchart of the PAFDP-OFDM-CPS method

4.1 System model

Considering above Fig.2, The OFDM based CPS serial input data streams are changed into a parallel lower data rate bit stream which is transmitted over the IFFT along with the signal mapper. The inter symbol interference in input data streams are removed from the Cyclic prefix. IFFT is used to convert all data streams into time domain signals and the modulated OFDM baseband signal is expressed in the Eq. (1).

Later the input data is again converted back to serial data and it is transmitted over the wireless channel.

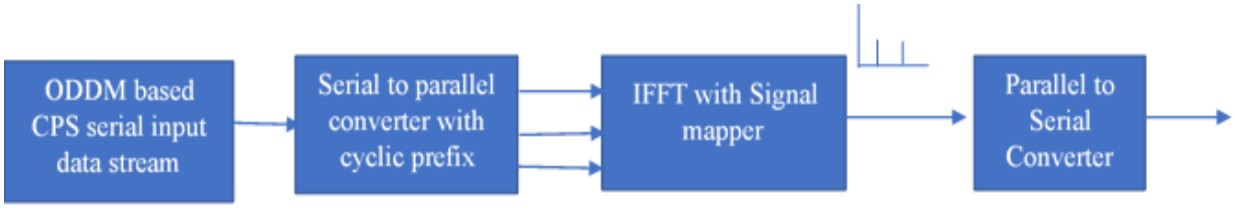

Figure. 2 OFDM based CPS system model

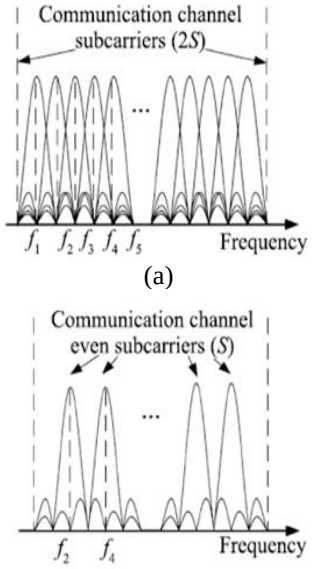

Figure. 3 OFDM Subcarriers: (a) OFDM subcarriers and (b) even OFDM subcarriers

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

where, x(g) is the g^{th} sample of the OFDM transmitted signal at time domain; G is total amount of OFDM subcarriers and X_s is the modulated symbol at frequency domain in the s^{th} subcarrier. They(g) is the output received signal after processing through the wireless channel which is specified as in the Eq (2).

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

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

4.2 Structure of PAFDP in CPS

Initially the OFDM based CPS is consisting of K number of nodes and one sink node. The OFDM communication channel with bandwidth (B) is divided as 2S overlapping narrow band subcarriers. Later the divided subcarrier has N_0 as a constant noise power density and equal bandwidth. In order to overcome the problem of severe co-channel interference this OFDM only uses the even subcarriers as in Fig 3. Moreover, each frame contains a D time slots to accomplish the OFDMA transmission along with the polling and one transmission transit gap. The packet transmitted to the sink node is obtained in the ideal deadline (T frames) or packets may be discarded during the communication. The priority and polling of nodes between the nodes are obtained by using the PAFDP that leads to achieve the reliable data transmission. Moreover, the PAFDP generates the preamble phase as shown in Fig. 4 where the sink node transmits the OFDM network.

The sink solves the uplink OFDM frequency allocation issue with the help of the polling results to achieve reliable data transmission. preamble to obtain the time synchronization in the The IFFT is used to convert input data to time domain samples. The aggregate acknowledgement (ACK) from the sink is used to acknowledge the transmissions occurred in the data transmission phase after the Short Inter Frame Space (SIFS) time. Moreover, the scheduled node only sends one packet in per frame which occupies up to D slots.

The node priorities are characterised into various levels during data transmission. In PAFDP, k $(k = 1,2, \ldots., K)$ is the node which is allocated along with T_k subcarriers $(i.e., s_{k,1}, s_{k,2}, \ldots, s_{k,T_k})$ where this subcarriers are used along with throughput and data rate to calculate priorities of the transmitted nodes which is represented as $A_{k,i}$ with the increasing manner are specified as $1 = A_{k,1} \leq A_{k,2} \leq A_{k,T_k} = T_k$.

When the packets are not successfully reached to destination in the real time frame, the priorities of the nodes are increased for next time frame so that based on the priorities of the node, the nodes in OFDM with each time frame transmits the data packets to the sink.

Moreover, when the malicious node attacks requests for high priority during the communication degrade the reliability of the OFDM based CPS. During this period, the packet drop of the nodes occurs (i.e., more than 50% of packet loss) due to malicious attacks while transmitting the packets.

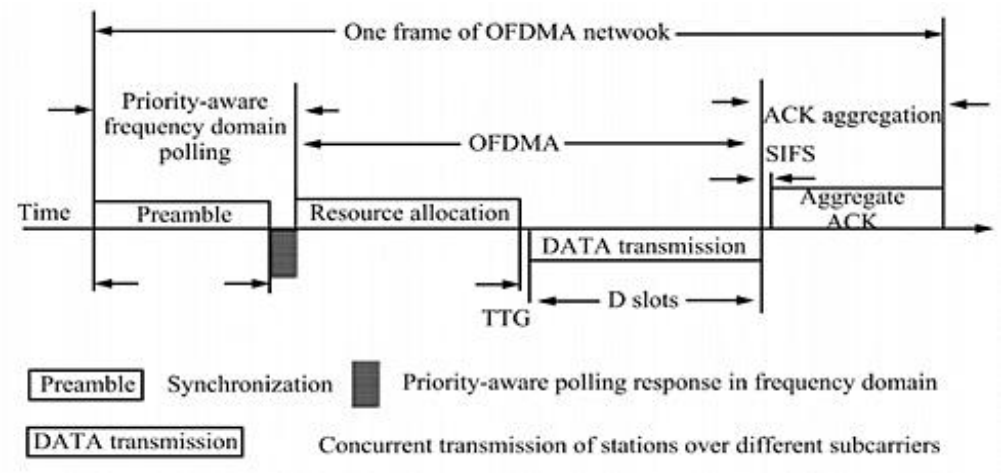

Figure. 4 Structure of the PAFDP protocol

Table 1. Specification parameters

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

5. Results and discussion

The results and discussion of the PAFDP-OFDM-CPS method is presented in this section. The simulation and implementation of this proposed method is carried out by using the MATLAB Simulator. The priorities of the nodes in the OFDM are collected based on the priority-aware polling response in frequency domain and the node polling is obtained by using the proposed protocol. Additionally, the malicious nodes in the network 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.

5.1 Performance analysis

The QOS performance of the PAFDP-OFDM-CPS method is analysed in terms of Packet Delivery Ratio (PDR), Packet Loss Ratio, throughput and overhead by evaluating and comparing with the TAWRP [17], TARF [17] and ADCCOR [14] by varying the number of malicious nodes from 1-5.

5.1.1. Packet delivery ratio

PDR is the ratio of the number of packets received at the sink to number of packets transmitted by the OFDM transmitter which is expressed in the Eq. (3).

$$PDR = \frac{\sum_{i=1}^{n} Y_i}{\sum_{i=1}^{n} X_i} \times 100 \quad (3)$$

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

Table 2. PDR for varying malicious nodes

Number of malicious nodes	TAWRP [17] in %	TARF [17] in %	ADCCOR [14] in %	PAFDP-OFDM-CPS in %
0	100	100	100	100
1	87	85	96.47	99.65
2	83	77	95.12	99.5
3	80	60	95.04	99.3
4	73	50	93.78	99.6
5	60	40	93.11	99.4

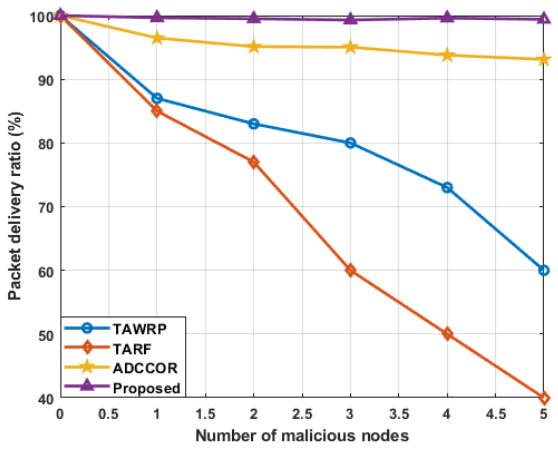

Figure. 5 PDR comparison

Table 2 and Fig. 5 shows the PDR comparison of the PAFDP-OFDM-CPS method with ADCCOR [14], TAWRP [17] and TARF [17]. which shows the PDR of the proposed method is increased with 99.4% comparably with ADCCOR[14], TAWRP [17] and TARF [17] where the PDR are 96% , 60% and 40% respectively.

5.1.2. Packet loss ratio

PLR is defined as the ratio of the amount of packets dropped to number of packets transmitted by the OFDM transmitter. Eq. (4) shows the expression for the PLR.

$$PLR = \frac{\sum_{i=1}^{n} X_i - Y_i}{\sum_{i=1}^{n} X_i} \times 100\% \quad (4)$$

The comparison of PLR for the PAFDP-OFDM-CPS method, ADCCOR [14], TAWRP [17] and TARF [17] is shown in the Table 3 and Fig. 6. From the analysis, the PLR of the PAFDP-OFDM-CPS method is reduced of 0.12 % for 5 malicious nodes when compared to the existing methods such as TAWRP [17] and TARF [17] which is 10.58% and 11.75 % respectively due to misbehaving of the nodes in the network.

Table 3. PLR for varying malicious nodes

Number of malicious nodes	TAWRP [17] in %	TARF [17] in %	ADCCOR [14] in %	PAFDP - OFDM-CPS in %
1	11.4	12.5	1.5	0.07
2	10.55	11.5	1.83	0.1
3	12.29	11	0.98	0.14
4	12.58	13	1.03	0.08
5	10.58	11.75	0.74	0.12

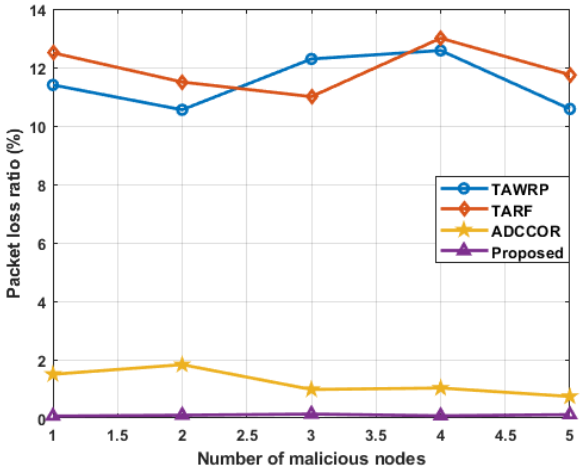

Figure. 6 PLR comparison

Table 4. Overhead for varying malicious nodes

Number of malicious nodes	TAWRP [17]	TARF [17]	ADCCOR [14]	PAFDP - OFDM-CPS
0	0	0	0	0
1	1	1.5	1.4	1.3
2	1.4	2	1.5	1.4
3	1.9	3	1.8	1.7
4	2	4	2.9	2.2
5	2.9	5.6	3.3	2.6

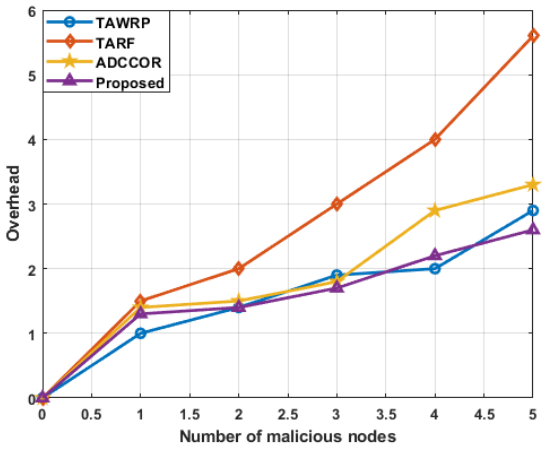

Figure. 7 Overhead comparison

5.1.3. Overhead

Overhead is defined as the total number of control packets created by the nodes in the network which is expressed in the Eq. (5).

$$Overhead = \sum_{j=1}^{n} R_j \quad (5)$$

where, j is the number of nodes that created the control packets and R. is the control packets.

Table 4 and Fig. 7 shows the overhead comparison of the PAFDP-OFDM-CPS method with ADCCOR [14], TAWRP [17] and TARF [17] where the overhead of the PAFDP method is less about 2.6 control packets for 5 malicious nodes which is less due to priority when compared to above said protocols.

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 Eq. (6).

$$Throughput = \frac{Yi}{Ti} \quad (6)$$

Table 5. Throughput for varying malicious nodes

Number of malicious nodes	TAWRP [17] in bps	TARF [17] in bps	ADCCOR [14] in bps	PAFDP-OFDM-CPS in bps
1	76.46	85.5	123.48	162.19
2	83.88	83.6	117.27	163.95
3	75.39	80.5	113.36	161.89
4	70.29	77.8	105.74	162.14
5	69.38	74.5	102.09	160.96

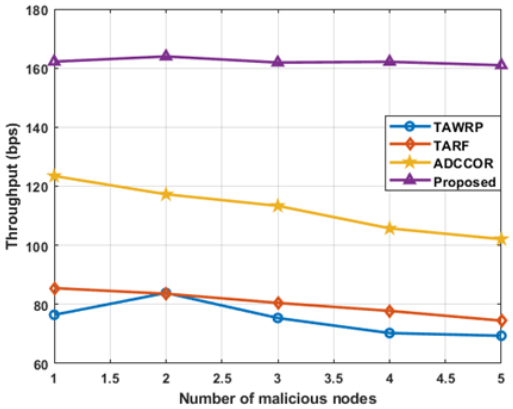

Figure. 8 Throughput comparison

where, Ti defines the time interval and Yi specifies the packets received at the sink.

Table 5 and Fig. 8 shows the throughput comparison of the PAFDP-OFDM-CPS method with ADCCOR [14], TAWRP [17] and TARF [17] where the throughput of the PAFDP method is high160.96 bps for 5 malicious nodes when compared to the above said protocols.

6. Comparative analysis

The performance of the proposed PAFDP-OFDM-CPS method is compared with ADCCOR [14], TAWRP [17] and TARF [17] to analyse the average energy efficiency of the PAFDP protocol. Subsequently, the design of avoidance of the malicious attacks is difficult in the network controlled systems.

Table 6 and 7 shows the comparison of the PAFDP-OFDM-CPS with ADCCOR [14], TAWRP [17] and TARF [17] for different sink distance i.e., from 100 m to 500 m. Moreover, Fig. 9 shows the graphical illustration for the comparison of average energy consumption which analyses the proposed method achieves better performance than the ADCCOR [14], TAWRP [17] and TARF [17]. due to its priority identification using data rate and throughput which leads to minimize the energy

Table 6. Average end to end delay consumption for varying sink.

Distance to the sink (m)	TAWRP [17]	TARF [17]	ADCCOR [14]	PAFDP-OFDM-CPS
100	14.4	15.8	12.5	10.3
200	17.8	18.4	30	18.6
300	20.1	24	40	32
400	35	43	55	43
500	52	59	62.5	56

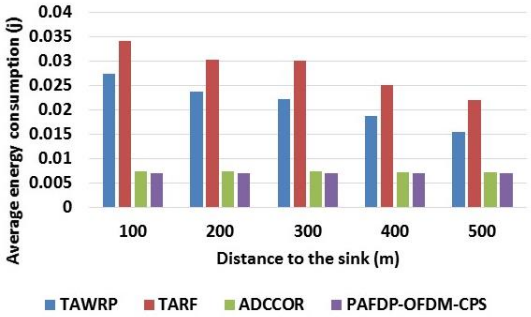

Figure. 9 Graphical illustration of average energy consumption comparison

Table 7. Energy consumption for varying sink

Distance to the sink (m)	TAWRP [17]	TARF [17]	ADCCOR [14]	PAFDP-OFDM-CPS
100	0.02734	0.03415	0.0073	0.007
200	0.02371	0.03018	0.00725	0.00692
300	0.02208	0.02993	0.00725	0.00693
400	0.01874	0.02507	0.00715	0.0069
500	0.01537	0.02201	0.0072	0.007

consumption and delay of the PAFDP protocol over the OFDM based CPS

Additionally, the PAFDP-OFDM-CPS method protects the normal node from the malicious nodes based on the packet drop based malicious node detection. This helps to improve the packet delivery ratio between the nodes.

7. Conclusion

In this paper, PAFDP- OFDM – CPS is developed for obtaining an efficient polling between the nodes and reliable communication, so that the priority of the nodes is identified by using the throughput and data rate. The proposed PAFDP protocol is used to minimize the average delay while transmitting the data packets. The malicious nodes in the network is identified based on the packet drop occurred in each

node, therefore the proposed 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 nodes when compared to TAWRP, TARF and ADCCOR. In future, the proposed method can be improvised by a frequency interleaved polling which 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

Conflicts of Interest

I Saritha I G, Asst Professor, Dept ETE, BMSIT&M, declaring no conflict of interest.

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.

References

[1] B. M. Lee and H. Yang, "Massive MIMO for industrial Internet of Things in cyber-physical systems", *IEEE Transactions on Industrial informatics*, Vol. 14, No. 6, pp. 2641-2652, 2017

[2] K. Wan and V. Alagar, "Context-aware security solutions for cyber-physical systems", *Mobile Networks and Applications*, Vol. 19, No. 2, pp. 212-226, 2014.

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

[4] Y. Yuan and Y. Mo, "Security for cyber-physical systems: Secure control against known-plaintext attack", *Science China Technological Sciences*, pp. 1-10, 2010.

[5] C. Alcaraz and J. Lopez, "A cyber-physical systems-based checkpoint model for structural controllability", *IEEE Systems Journal*, Vol. 12, No. 4, pp. 3543-3554, 2017.

[6] H. Orojloo and M. A. Azgomi, "A stochastic game model for evaluating the impacts of security attacks against cyber-physical systems", *Journal of Network and Systems Management*, Vol. 26, No. 4, pp. 929-965, 2018.

[7] Y. Zhang and O. Yağan, "Robustness of interdependent cyber-physical systems against cascading failures. *IEEE Transactions on Automatic Control*, Vol. 65, No. 2, pp. 711-726, 2019.

[8] S. Huang, C. J. Zhou, S. H. Yang, and Y. Q. Qin, "Cyber-physical system security for networked industrial processes", *International Journal of Automation and Computing*, Vol. 12, No. 6, pp. 567-578, 2015.

[9] P. M. Lima, M. V. S. Alves, L. K. Carvalho, and M. V. Moreira, "Security against communication network attacks of cyber-physical systems", *Journal of Control, Automation and Electrical Systems*, Vol. 30, No. 1, pp. 125-135, 2019.

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

[11] B. Zheng, P. Deng, R. Anguluri, Q. Zhu, and F. Pasqualetti, "Cross-layer codesign for secure cyber-physical systems", *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, Vol. 35, No. 5, pp. 699-711, 2016.

[12] S. Mili, N. Nguyen, and R. Chelouah, "Transformation-Based Approach to Security Verification for Cyber-Physical Systems", *IEEE Systems Journal*, Vol. 13, No. 4, pp. 3989-4000, 2019.

[13] Z. Zhao, Y. Yang, Y. Li, and R. Liu, "Security analysis for cyber-physical systems under undetectable attacks: A geometric approach", *International Journal of Robust and Nonlinear Control*, Vol. 30, No. 11, pp. 4359-4370, 2020.
[14] X. Xiang, W. Liu, A. Liu, N. N. Xiong, Z. Zeng, and Z. Cai, "Adaptive duty cycle control–based opportunistic routing scheme to reduce delay in cyber physical systems", *International Journal of Distributed Sensor Networks*, Vol. 15, No. 4, pp. 1550147719841870, 2019.
[15] R. Gifty, R. Bharathi, and P. Krishnakumar, "Privacy and security of big data in cyber physical systems using Weibull distribution-based intrusion detection", *Neural Computing and Applications*, Vol. 31, No. 1, pp. 23-34, 2019.
[16] D. Shi, R. J. Elliott, and T. Chen, "On finite-state stochastic modeling and secure estimation of cyber-physical systems", *IEEE Transactions on Automatic Control*, Vol. 62, No. 1, pp. 65-80, 2016.
[17] N. Qureshi, "Malicious node detection through trust aware routing in wireless sensor networks", *Journal of Theoretical and Applied Information Technology*, Vol. 74, No. 1, 2015.
[18] A. Chen, X. Li, X. Ni, and G. Luo, "RTGOR: Reliability and Timeliness Guaranteed Opportunistic Routing in wireless sensor networks", *EURASIP Journal on Wireless Communications and Networking*, Vol. 2018, No. 1, pp. 86, 2018.
[19] M. Zheng, W. Liang, J. Lin, and H. Yu, "A Priority-aware Frequency Domain Polling MAC Protocol for OFDMA-based Networks in Cyber-physical Systems", *IEEE/CAA Journal of Automatica Sinica*, Vol. 2, No. 4, 2015.
[20] X. Ning and J. Jiang, "In the mind of an insider attacker on cyber-physical systems and how not being fooled", *IET Cyber-Physical Systems: Theory & Applications*, Vol. 5, No. 2, pp. 153-161, 2020.
[21] S. Kim, Y. Won, I. H. Park, Y. Eun, and K. J. Park, "Cyber-physical vulnerability analysis of communication-based train control", *IEEE Internet of Things Journal*, Vol. 6, No. 4, pp. 6353-6362, 2017.
[22] M. S. Sowmyashree and C. S. Mala, "Development of a Novel Protocol for Improvement of Qos Inwireless Sensor Networks: P-Rpeh", *International Journal of Recent Technology and Engineering (IJRTE)*, Vol. 8, No. 3, pp. 2277-3878, 2019.
[23] R. Fu, X. Huang, Y. Xue, Y. Wu, Y. Tang, and D. Yue, "Security assessment for cyber physical distribution power system under intrusion attacks", *IEEE Access*, Vol. 7, pp. 75615-75628, 2018.