Hindawi
Wireless Communications and Mobile Computing
Volume 2021, Article ID 2803335, 10 pages
https://doi.org/10.1155/2021/2803335

Review Article

Channel Access-Based Joint Optimization of AoI and SINR under Attack: Game Theory and Distributed Approach

Yaoqi Yang,[1] Xianglin Wei,[2] Renhui Xu,[1] Laixian Peng,[1] Shuai Cheng,[1] and Lin Ge[1]

[1]*College of Communications Engineering, Army Engineering University of PLA, Nanjing 210000, China*
[2]*The 63rd Research Institute, National University of Defense Technology, Nanjing 210007, China*

Correspondence should be addressed to Xianglin Wei; wei_xianglin@163.com and Laixian Peng; lxpeng@hotmail.com

Received 28 May 2021; Revised 22 June 2021; Accepted 2 July 2021; Published 20 July 2021

Academic Editor: Dr. Muhammad Shafiq

Copyright © 2021 Yaoqi Yang et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

This paper focuses on the joint optimization of the Age of Information (AoI) and Signal to Interference plus Noise Ratio- (SINR-) oriented channel access problem under attack in the Wireless Sensor Networks (WSNs). Firstly, to overcome the uncertain, dynamic, and incomplete information constrains, an active probability model and a controlling channel model are proposed for the sensors and the receiving end, respectively. Secondly, to ensure the AoI and SINR of the data generated by the sensors when transmitted under attack, one utility function based on average AoI and SINR is defined. Then, considering the distributed feature of the channel access process, the joint optimization problem is formulated under the game theory structure. Then, a distributed learning algorithm is proposed to reach the Nash Equilibrium (NE) of the game. Finally, simulation results have verified the correctness and effectiveness of the proposed method.

1. Introduction

1.1. Background. AoI (Age of Information) refers to the time interval between data's generations to its receiving end, and it is significantly different from the traditional concept of per-packet delay. Therefore, due to the capacity of representing the freshness of the data, lots of efforts have been made on AoI, which is significantly different from the traditional concept of delay. Up to now, plenty of researchers have devoted themselves to AoI's research from different aspects. To be specific, the queueing model's effect on the average AoI has been investigated in [1, 2]; the scenario about multihop transmission is considered in [3, 4]; the packet with losing situation is revealed in the calculation of AoI in [5]. In addition, more and more works concentrate on the goal that minimizes the average AoI, and the typical given approach is to adopt the strategy with weighted-sum average AoI.

Owing to a series of advantages of AoI, it can bring the unexpected benefit when used in some traditional cases. The scenario contains internet of things (IoT) and cyber physics systems (CPS) with edge-enabled storage or caching [6], where the transmitted data is time critical and requires high timeliness at the receiving end. Driven by the timeliness, AoI is utilized to measure the performance of the wireless transmission. For example, in mission-ciritcal industrial Wireless Sensor Networks (WSNs), data freshness is very critical to ensure a high-quality product manufacturing. In addition, SINR (Signal to Interference plus Noise Ratio) is also an important indicator for evaluating the performance of the network [7]. Therefore, to comprehensively optimize the effectiveness and reliability of the network, we consider a scenario where the sensors are undergoing the wireless channel access attack [8–14], and we focus on how to select the available channel to transmit the data generated by sensors while keeping the freshness of the data and maximizing the SINR as much as possible.

The wireless channels could be allocated in centralized or distributed manner. For the first one, though we can solve the

above problem by setting a central controller to allocate the channel resources based on the each sensor's average AoI payoff, two factors limit the proposal's practicality. On the one hand, the calculation capacity requirement for the central controller is high, especially when the number of the sensors is large. On the other hand, the efficiency of the controller may not meet the need of the sensors when the scale of the network is very large; for example, the attack has influenced the available channel set, but the channel access strategy has not been sent to some sensors in time. Compared with the centralized decision-making (DM) manner, the distributed proposal has the following advantages. Firstly, the implementation cost is low, because there is no need to set a central controller. Secondly, each sensor could make the channel access decision by itself, promoting the efficiency of the channel selection. Thirdly, the decision-making process can adapt to the change of the attack quickly in dynamic scenarios.

However, it is a nontrivial task to solve the problem in a distributed manner. The following aspects hinder us from directly using of the referred method. Firstly, taking the practical application of the sensors into consideration, a sensor would not access the channel when there is no data to transmit. Therefore, how to capture this dynamic attribution of the sensor will be a challenge. Secondly, the attack progress is unpredictable and the available channel set for each sensor is unknown; how to perform the DM matching with the changing environment is also a problem. Thirdly, there is no information exchange for each sensor in the distributed manner, so the sensor does not know the chosen channel and the current state (accessing the channel or not) of other sensors. Therefore, the information attribution constraints, which are uncertain, dynamic, and incomplete, let the goal to solve the channel access under dynamic attack problem more challenging.

To tackle this tricky problem, game theory is a suitable framework to coordinate the behavior between different sensors [15]. To be specific, we formulate a game which is based on average AoI and SINR indicator under attacks in the WSNs, and a distributed learning algorithm is proposed to obtain the solutions.

1.2. Related Work. It is convenient to use game theory to model and analyze the routing and resource allocation problems in a competitive environment and especially in the security issues of the wireless network. To be specific, when some users want to access limited channel resource, how to select the channel to transmit is the key point for users. It should be noted that all users want to maximize their profits. Therefore, the relationship between users needs to be accurately described to calculate their revenue separately. Besides, game theory can model the complex relationships in a dynamic and iterative viewpoint, which would give the better assignment scheme by deriving the NE solution.

As shown in Table 1, the efforts in the channel access with game theory are classified by their optimization goals, solution or method, and the attack consideration. It can be seen that mean throughput is the main optimization indicator in the literature [7, 16–18], and transmission with errors or collision situations are discussed in [19, 20]. Besides, the whole network's utilities are optimized in [21–24]. It is obvious that the joint optimization of AoI and SINR has not been paid enough attention under attack, and the proposed solution or method should be in the distributed manner. In order to make up the above research gap, the joint optimization issue under attack is researched in this paper.

1.3. Main Work and Contributions. In this paper, our main contributions are threefold:

(i) The AoI and SINR-oriented channel access model under attack is formulated as an optimization problem, in which the transmission and controlling channels and the unknown nature of attacks are included to formulate the average AoI and SINR. Then, a game-based framework is established to curve the uncertain, dynamic, and incomplete information constrains

(ii) A distributed learning algorithm is proposed to derive the NE of the game, in which the channel access algorithm based on stochastic learning automata is put forward

(iii) To evaluate the performance of the proposed algorithm, simulation experiments are conducted to verify the correctness and effectiveness of the proposed algorithm

The remainder of this paper is organized as follows. In Section 2, we describe the system model and formulate the problem. Our proposed algorithm is then introduced in Section 3. Simulations about the performance of the proposed algorithm are detailed in Section 4, and Section 5 concludes the paper.

2. System Model

2.1. Network Model. In the WSN, N sensor nodes are deployed, and they can be represented by the set $\mathcal{S} = \{S_1, S_2, \cdots, S_N\}$. In addition, the active probabilities of the sensor nodes are also considered here. To be specific, $S_n = 1$ means the n-th node is active; otherwise, $S_n = 0$ represents the inactive status of the n-th node.Denote the set $\mathcal{B} = \{n \in N : S_n = 1\}$ as an arbitrary nonempty active sensor node set, and Γ as the set for all the active sensor nodes. At this time, the active probability of the WSN is $\mu(\mathcal{S})$, and it can be expressed as

$$\mu(\mathcal{S}) = \mu(S_1, S_2, \cdots, S_N) = \prod_{n=1}^{N} p_n,$$
$$p_n = \begin{cases} \beta_n, & S_n = 1, \\ 1 - \beta_n, & S_n = 0. \end{cases} \tag{1}$$

Table 1: A comparison of channel access efforts based on game theory model.

Reference	Optimization goal	Solution/method	Attack consideration
[7]	Mean throughput	A distributed learning algorithm	×
[19]	Collision slots	The Lagrangian extreme value approach	×
[16]	Mean throughput	A distributed and online algorithm	×
[17]	Mean throughput	An EGT algorithm	×
[21]	Quality of service	The stochastic game theory tool set	×
[20]	Transmission and blocking probabilities	A CA algorithm	×
[22]	Channel access and resource allocation	Convex optimization	×
[18]	Mean throughput	A closed-form solution for SG	×
[23]	Network utility	A distributed algorithm	×
[24]	Spectral efficiency	An expectation maximization algorithm	×
This work	Average AoI	Reinforcement learning-based distributed scheme	

Meanwhile, the active probability for $\mathscr{B}$, which represents an arbitrary nonempty active sensor node set, is

$$\sum_{\mathscr{B}\in\Gamma} \mu(\mathscr{B}) = 1 - \mu(\mathscr{B}_0), \tag{2}$$

where $\mu(\mathscr{B}_0)$ is the probability when all sensor nodes are inactive, and it can be calculated as

$$\mu(\mathscr{B}_0) = \prod_{n=1}^{N} (1 - \beta_n). \tag{3}$$

2.2. Channel Model. In the WSN, owing to the dynamic and complexity transmission environment, the active probability of the sensor nodes and stability of the wireless channel are always changing. Moreover, the attacker can also deteriorate the availability of the wireless channels. In order to ensure the essential information exchange among the sensor nodes, two kinds of wireless channels models are adopted here, i.e. TC (transmission channel) and CC (controlling channel) [25]. To be specific, the TC is used to transmit ordinary data, and CC is responsible for exchanging some control information, such as channel-selection status, and node active probabilities. For ease of narration, denote $\mathscr{A}_n = \{a_1, a_2, \cdots, a_M\}$ as the available TC set for the n-th sensor node, where M is the number of the available TCs. When all the active sensor nodes finished the sensing process and transmitted the sensed data through the wireless channels, the channel access strategy of the n-th sensor node is $a_n \in A_n$, which means the channel a_n is selected by the n-th node to transmit the data.

2.3. Attack Model. An attacker can damage the performance of the WSN, such as QoS (quality of service). To be specific, at one certain attacking time slot, some available channels may become unavailable; at this time, the channel's stability and the reliability decreased. Then, due to the unavailable channels, the AoI and SINR performances of the sensed data in the WSN are influenced. However, given the limited attacking capacity of the attacker, which is consistent with [25], there is at least one available TC in the data transmission process; i.e., it is impossible for the attacker to make all the TCs unavailable at one attacking time slot, and CC is always reliable and available.

2.4. AoI Model. Here, we firstly consider the average AoI model for single node when there is no attack. Then, in the proposed scenario, where the average AoI for multisensor nodes under attack needs to be derived, the average AoI expression with a closed form is derived.

2.4.1. AoI for Single Node without Channel Attack. In order to determine the average AoI of the sensed data, the model based on queue theory is detailed here. The serving rule is FCFS (first come first serve), and the queue model is $M/M/1$. According to [26], the average AoI of the sensed data can be determined by

$$AoI_T = \lim_{T\longrightarrow\infty} A_T = \lambda\left(E[XT] + \frac{E[X^2]}{2}\right), \tag{4}$$

where λ denotes the incoming rate of the sensed data, i.e., data generating rate; $E[\cdot]$ is the operation for calculating expectation value; and X and T represent the stochastic variables for the sensed data's arrival time and system time, respectively.

Under the $M/M/1-\text{FCFS}$ queue model, where the sensed data's generating rate subjects to the Poisson distribution, the serving rate, i.e., the sensed data transmission rate in the wireless channels, obeys the negative exponential distribution with parameter μ. Based on [26] the serving rate ρ can be calculated as

$$\rho = \frac{\lambda}{\mu}. \tag{5}$$

At this time, the average AoI of $M/M/1-\text{FCFS}$ queue model is [26]

$$\text{AoI} = \frac{1}{\mu}\left(1 + \frac{1}{\rho} + \frac{\rho^2}{1-\rho}\right). \tag{6}$$

2.4.2. AoI for Multinodes with Channel Attack. Given the fact that multiple sensor nodes can access one wireless channel at the same time, the distribution of arrival time X and system time T will change. To be specific, when τ sensor nodes select the same wireless channel to transmit the sensed data at the same time, the data generating rate of the n-th sensor node should be calculated as

$$\lambda_i = \frac{\lambda i}{\sum_{j=1}^{\tau} \lambda j}, \tag{7}$$

where λi is the data generating rate by the i-th sensor node and the channel serving rate μ is unchanged. Therefore, take (7) into (6), the average AoI of sensed data generated by the i -th sensor node is

$$\begin{aligned}\text{AoI}_i &= \frac{1}{\mu}\left(1 + \frac{\mu}{\lambda_i} + \frac{(\lambda_i/\mu)^2}{1-(\lambda_i/\mu)}\right)\\ &= \frac{1}{\mu}\left(1 + \frac{\mu}{\lambda i/\left(\sum_{j=1}^{\tau}\lambda j\right)} + \frac{\left(\lambda i/\left(\sum_{j=1}^{\tau}\lambda j\right)/\mu\right)^2}{1-\left(\lambda i/\left(\sum_{j=1}^{\tau}\lambda j\right)/\mu\right)}\right).\end{aligned} \tag{8}$$

Furthermore, when the WSN is under attack, the average AoI will change at the same time. In order to accurately curve the dynamic channel access relationships among the sensor nodes, the channel selection status, sensor node category, and time slots need to be jointly considered. To be specific, let $C(e,t)$ be the sensor node set which accesses the e-th channel at the t-th time slot. Since the $C(e,t)$ is related with the accessed channel and time slot, it would change with the launching of the attack at one particular attacking time slot. At this time, the average AoI of data, which is generated by the i-th sensor node, can be calculated as

$$\begin{aligned}\text{AoI}_i &= \frac{1}{\mu}\left(1 + \frac{\mu}{\lambda_i} + \frac{(\lambda_i/\mu)^2}{1-(\lambda_i/\mu)}\right)\\ &= \frac{1}{\mu}\left(1 + \frac{\mu}{\lambda i/\left(\sum_{j\in C(e,t)}\lambda j\right)} + \frac{\left(\lambda i/\left(\sum_{j\in C(e,t)}\lambda j\right)/\mu\right)^2}{1-\left(\lambda i/\left(\sum_{j\in C(e,t)}\lambda j\right)/\mu\right)}\right).\end{aligned} \tag{9}$$

2.5. SINR Model. When the i-th active sensor node selects the channel $a_i \in \mathscr{A}_i$ to transmit the sensed data, the SINR of the i-th active sensor node, which is from the arbitrary active node set $\mathscr{B}$, under the channel access strategy (a_i, a_{-i}), can be calculated as

$$\text{SINR}_i(\mathscr{B}, a_i, a_{-i}) = \frac{p_i d_i^{-\alpha}}{\sum_{j\in\mathscr{B}\setminus\{i\}:\, a_j=a_i} p_j d_{ij}^{-\alpha} + \sigma}, \tag{10}$$

where p_i is the transmitting power of the i-th sensor node, d_i is the distance between the i-th sensor node and its corresponding receiver, α is the path loss efficient, d_{ij} is the distance between the i-th and j-th sensor nodes, and σ means the environment noise. Therefore, the molecular represents the transmitting power of the sensed data; the denominator is the sum of the interference of other sensor nodes choosing the channel a_i and the environment noise.

2.6. Problem Formulation. The problem that needs to be solved is how to make each sensor node's own channel access strategy to jointly minimize the AoI and maximize the SINR when the WSN is under attack, i.e.,

$$\begin{aligned}&\min\ \{a \times AoI_i - b \times \text{SINR}_i\}\\ &\text{s.t.}\begin{cases} j \in C(e,t)\\ 0 \le t \le T\\ a_i \in \mathscr{A}_i\\ 1 \le e \le M\\ 1 \le i \le N\\ \mathscr{B} \in \Gamma,\end{cases}\end{aligned} \tag{11}$$

where a and b are the weighting factors to make AoI and SINR optimize in the same dimension. Note that it is difficult to directly use the typical method to solve the formulated problem (11), e.g., convex optimization, because the relationships of the channel selection results are relevant to time. Therefore, in order to make the nontrivial problem solvable, the problem in (11) needs to be reformulated with the game theory perspective, which is shown in (12).

Moreover, the payoff $R_i(\mathscr{B}, a_i, a_{-i})$ needs to be defined based on the optimization goal in (11) at first, i.e.,

$$R_i(\mathscr{B}, a_i, a_{-i}) = a \cdot \frac{1/(L(\mathscr{B})-1)\sum_{j\in B\setminus\{i\}:\, a_j=a_i}\text{AoI}_j}{\text{AoI}_i} + b \cdot \text{SINR}_i, \tag{12}$$

where the number of channels in set $\mathscr{B}$ is represented by $L(\mathscr{B})$. The numerator of the first item in R_i represents the channel competition effect on the average AoI among the sensor nodes which select channel a_i; and the denominator

Input: $K = \{1, 2, \cdots k_{\max}\}$: the iteration times set; $\mathscr{A}(n)$: the available channel set for the active sensor node; $q_{nd}(i) = 1/|\mathscr{A}_n|$: initial mixed strategy of each sensor node ($\forall n \in N, \forall d \in \mathscr{A}_n$); $\mathscr{B}(i)$: the active sensor node set in the current slot; b: the learning step size.
Output: $q_{nd}(k)$: the final mixed strategy of the active sensor node ($k \geq 1, \forall n \in N, \forall d \in A_n$); the AoI utility AoI_i; the SINR utility $SINR_i$.

1: **For** the iteration time $i = 1 : k_{\max}$ **do**
2: **If** the sensor node is inactive
3: Do nothing, i.e. :
$q_{nd}(i+1) = q_{nd}(i)$
4: **Else**
5: Perform the SLA algorithm, i.e.
6: Derive the normalized payoff $r_n(i) = R_n(i)/R_n^{\max}$ by (12)
7: **If** $d = a_n(i.)$
8:
$q_{nd}(i+1) = q_{nd}(i) + br_n(i)(1 - q_{nd}(i))$
9: **Else**
10:
$q_{nd}(i+1) = q_{nd}(i) - br_n(i)q_{nd}(i)$
11: **End**
12: **End**
13: Record AoI_i based on (9)
14: Record $SINR_i$ according to (10)
15: **End**

Algorithm 1. Channel access strategy for the sensor node under attack

of first item is the average AoI of the data generated by the i-th sensor node, and the second item means the weighted SINR value. At this time, as for $R_i(\mathscr{B}, a_i, a_{-i})$, the larger its value is, the smaller of the AoI value is and the larger of the SINR value is, where the sensed data is fresher and more reliable.

Note that all the sensor nodes prefer to minimize the average AoI and maximize the SINR of the data to be transmitted; their relationships are contended and noncooperated. At this time, we aim at maximizing the expectation value of the defined payoff, so (11) is equally transformed into (13), where the AoI and SINR are jointly optimized for the varying active sensor node set:

$$P_1 : \max_{a_i} E_{\mathscr{B}}[R_i(\mathscr{B}, a_i, a_{-i})] = \max_{a_i} \sum_{\mathscr{B} \in \Gamma} \mu(\mathscr{B}) R_i(\mathscr{B}, a_i, a_{-i}). \tag{13}$$

3. Game-Based Joint Optimization of AoI and SINR

3.1. Basic Idea. To jointly optimize the AoI and SINR performance, the minimizing problem is formulated in (11), while it is not applicable to the typical convex optimization approach. Then, the problem is equivalently transformed in the perspective of game theory, which aims at reaching the NE of the games in (13). Finally, based on the stochastic learning automata, one distributed algorithm is proposed to reach the NE by determining each sensor node's channel access strategy under attack.

3.2. Stochastic Learning Automata. To derive the NE of the reformulated problem in (13), one distributed-learning algorithm is adopted at first, which is mainly based on the stochastic learning automata [27, 28]. Then, combining the established models in Section 2 with the stochastic learning automata, the contents of the stochastic learning automata algorithm include the following steps:

(Step 1) All the inactive sensor nodes keep the current state and do nothing;

(Step 2) In the current time slot, the whole active nodes determine their channel access strategy based on the current payoff;

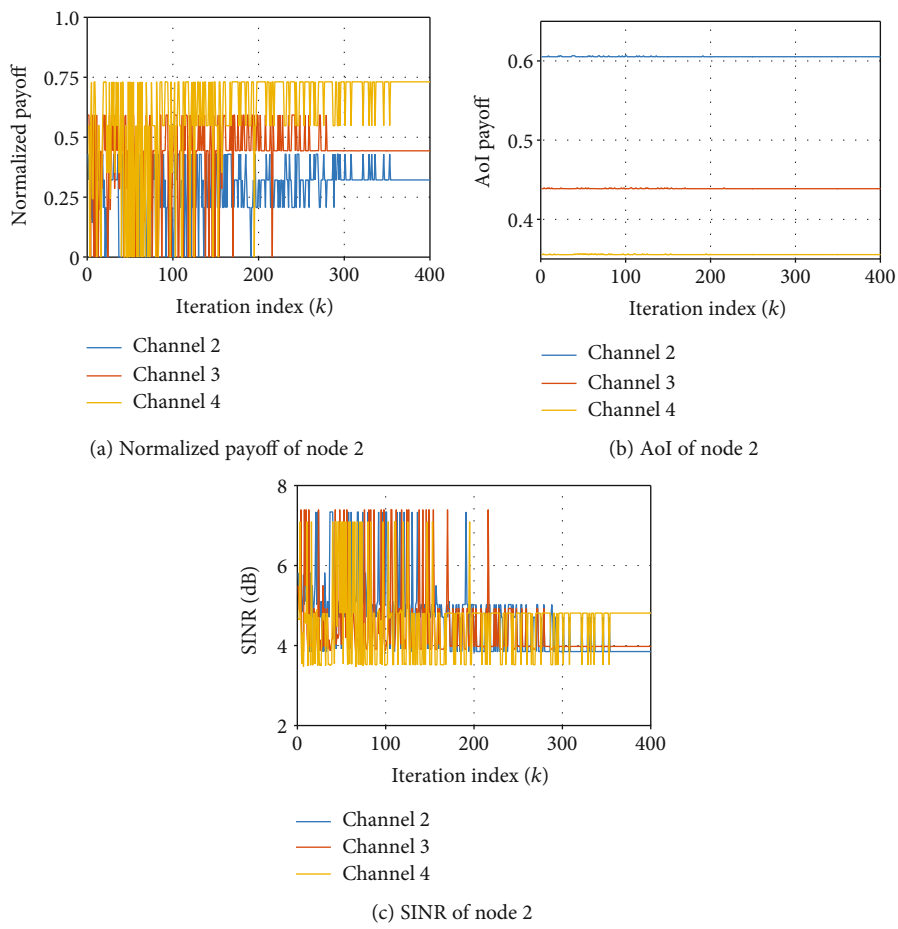
(Step 3) The channel access strategies are updated by the received payoff of the active sensor nodes at the next time slot.

3.3. Joint Optimization Algorithm. Note that TC can be used to transmit the sensed data, and the interactive information among the sensor nodes can be achieved by CC. Therefore, the sensor nodes can get their payoff instantaneously, which can be used to make the channel access strategy by itself in a distributed manner.

Based on the above analysis, the solution of the NE is detailed in Algorithm 1. To be specific, Steps 1–3 determine the channel access strategy for the active node; Steps 4–6 calculate the payoff of each sensor node; the channel access probability is included in Steps 7–8, where the payoff increased by choosing the current channel; Steps 9–12 decrease the channel access probability due to the decreased payoff; in Steps 13–15, the AoI and SINR utilities are determined finally.

Table 2: Parameter settings of the sensor nodes.

Node ID	Transmitting power	Generating rate	Available channel	Horizontal position	Vertical position
1	240	2	1, 2, 3, 4	53.78	20.39
2	630	3	2, 3, 4	49.11	226.60
3	255	4	1, 3, 4	544.70	328.04
4	175	5	3, 4	387.50	453.89
5	385	6	2, 3, 4	238.76	30.65
6	500	7	1, 2, 4	108.33	213.20
7	550	8	1, 2, 3, 4	318.55	411.87
8	300	9	1, 2, 4	371.37	361.69



(a) Normalized payoff of node 2

(b) AoI of node 2

(c) SINR of node 2

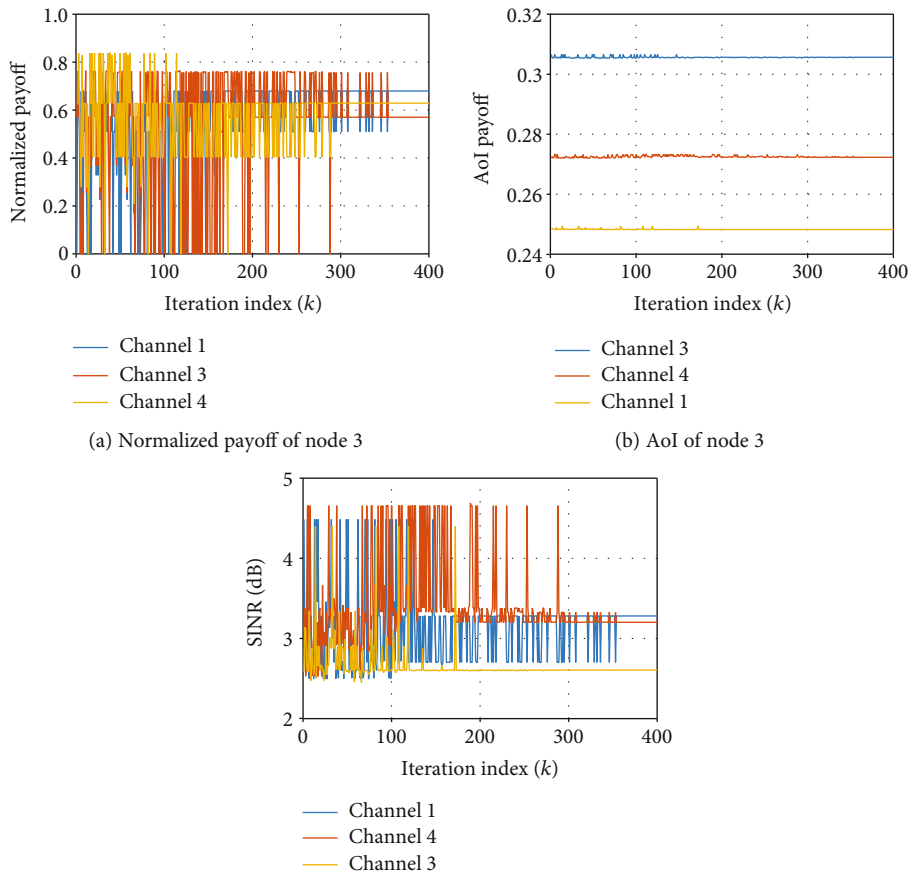
Figure 1: The performance of sensor node 2.

4. Simulation Results and Analysis

4.1. Parameter Settings. The simulation settings are listed in Table 2, where different sensor nodes have different transmitting powers, data generating rates, available channels, and positions. Besides, the serving rate of the wireless channel is set as 9.5, the active probability of the sensor nodes is 0.8, and the coefficients a and b are 5 and 1, respectively.

4.2. Compared Baselines. In order to evaluate the performance of the proposals, three algorithms are introduced as the baselines compared with the proposed algorithm.

(i) Optimal: the optimal algorithm is to find the best solution in a centric manner, which could can get the best performance by the exhausting searching approach.



(a) Normalized payoff of node 3

(b) AoI of node 3

(c) SINR of node 3

Figure 2: The performance of sensor node 3.

(ii) Best response: the best response algorithm could determine the best NE and worst NE of the game theory, which can be the upper and lower bounds of the solution in the game [29].

(iii) Random selection: the random selection algorithm means the sensor node select the channel to access, which has no relation with the defined payoff.

4.3. Correctness Verification. For ease of presentation, sensor nodes 2, 3, and 4 are selected as the example to show the correctness of the proposals.

4.3.1. Performance of the Sensor Node. Figure 1 is the normalized payoff, AoI, and SINR performance of the sensor node 2. As can be seen from Figure 1(a), with the iteration times increasing, the max payoff is obtained by selecting channel 4, the reason is that when node 2 selects channel 4, the AoI and SINR performance are the best, which are revealed in Figures 1(b) and 1(c). For ease of narration, sensor nodes 3 and 4 select channel 1 and channel 3 to transmit the sensed data, respectively, which are shown in Figures 2 and 3.

4.3.2. Channel Selection Probability. Figure 4 is the channel access probabilities of sensor node 2, sensor node 3, and sensor node 4. In Figure 4, on the one hand, when the iteration times increase, sensor node 2 would select channel 4, and so do channels 1 and 3 for nodes 3 and 4, respectively. On the other hand, in Figures 1, 2, and 3, the performance can reach best in the same channel selection results, so the correctness of the proposals is verified.

4.4. Effectiveness Verification. To evaluate the effectiveness of the proposed algorithm, 4 scenarios with heterogeneous active probabilities of the sensor nodes are considered here, where the active probabilities of the sensor nodes are set as follows:

(Case 1) $\{0.1,0.2,0.3,0.5,0.7,0.9,0.8,0.9\}$

(Case 2) $\{0.2,0.3,0.4,0.6,0.8,0.9,0.9,0.9\}$

(Case 3) $\{0.3,0.5,0.6,0.8,0.9,0.9,0.9,0.9\}$

(Case 4) $\{0.6,0.6,0.8,0.9,0.9,0.9,0.9,0.9\}$

Figure 5 is the effectiveness performance verification under 4 scenarios with heterogeneous active probabilities. As shown in Figure 5, on the one hand, when the active

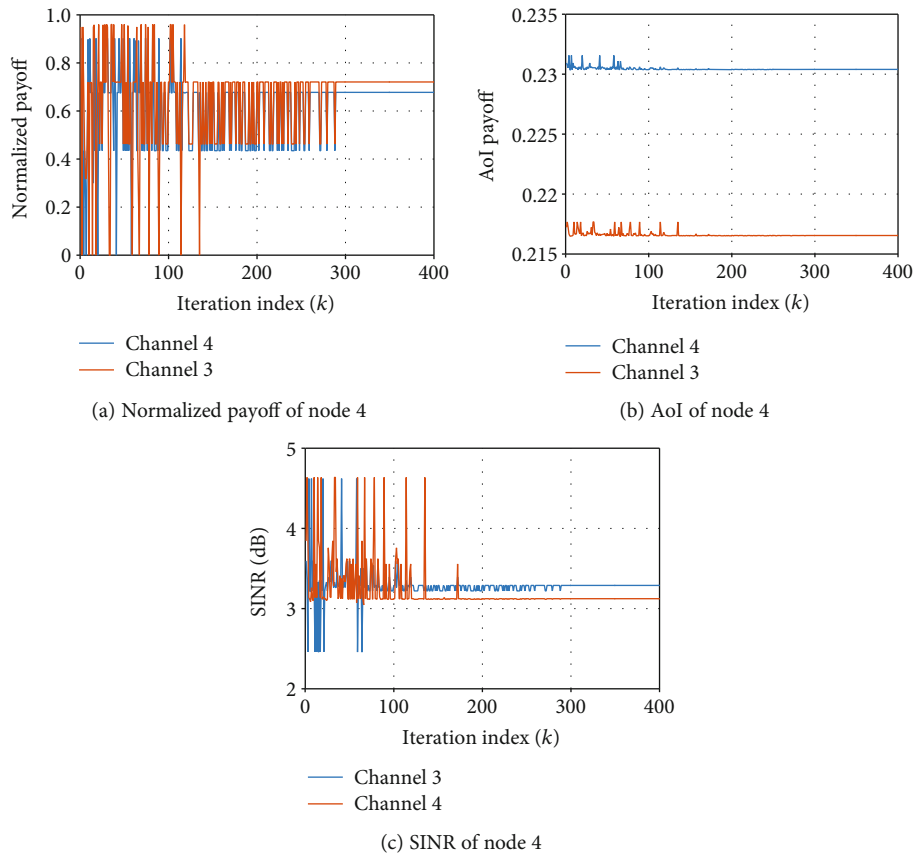


Figure 3: The performance of sensor node 4.

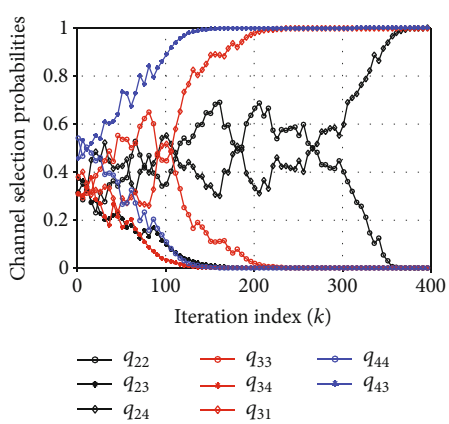


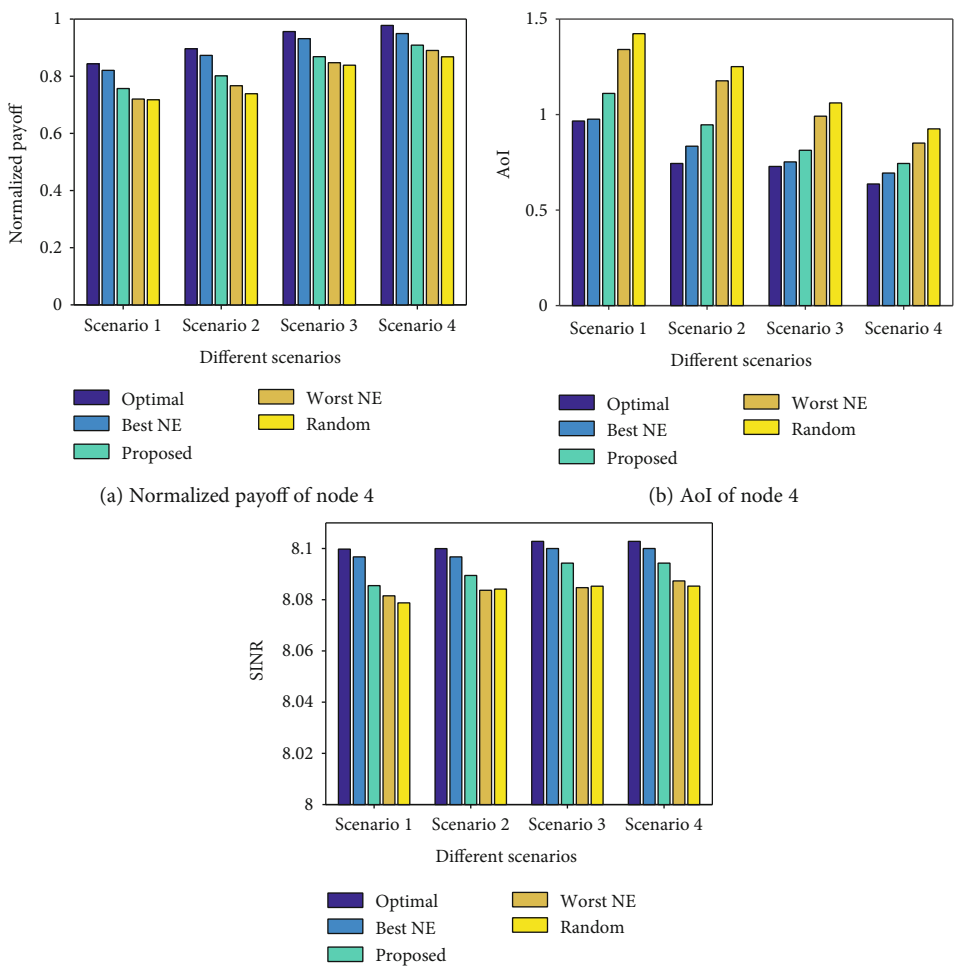
Figure 4: The channel access probabilities among different sensor nodes.

probability of the sensor nodes increases, the performance of the proposal is improved, this is because the probability of successfully accessing to the channel is positively related with the active probability of the sensor nodes; on the other hand, our proposal's performance is always better than the Worst NE and random selection scheme, which verifies the effectiveness of the proposals.

4.5. Discussion

4.5.1. Potential Application. In the Sixth Generation (6G) and Internet of Everything (IoE) era, with the rapid development of the wireless transmission technology, more and more data needs to be timely processed, especially in some time-critical networks. At this time, how to make plenty of wireless devices access within the limited wireless resources, e.g., channels, can be one desperate problem to be solved. Due to the consistent distributed attribution of the wireless devices, the channel access strategies proposed in this paper could be applied in the future, which can make the transmitted data keep fresh and reliable.

4.5.2. Attack Property. The attack property of the attacker is assumed to be stationary in this paper. In the next work, the channel access-based joint optimization of AoI and SINR under dynamic attack will be our focus. To be specific, inspired by the concept of time slicing network, the dynamic attack could be finished by launching attack at several different time slots. Combined with the joint optimization proposal at the particular time slot, the distributed channel access scheme under dynamic attack can be obtained by the method, where the dynamic attack process is divided into several attacking time slots.



(a) Normalized payoff of node 4

(b) AoI of node 4

(c) SINR of node 4

Figure 5: The effectiveness performance verification.

5. Conclusion

This paper proposed an algorithm to jointly optimize the AoI and SINR with channel accessing, when the WSN is under attack. Firstly, system models are established to derive the AoI and SINR indicator under attack. Then, the joint optimization problem is formulated from the perspective of game theory. To reach the NE of the game, one distributed algorithm is proposed next. Finally, simulation experiments are conducted to evaluate the correctness and effectiveness of the proposals. In the future, we will consider the joint optimization-based channel access issue under dynamic attacks.

Data Availability

No additional data is available in this paper.

Conflicts of Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

This work is supported by the National Natural Science Foundation of China (No. 61671471).

References

[1] H. B. Beytur, S. Baghaee, and E. Uysal, "Towards AoI-aware Smart IoT Systems," in *2020 International Conference on Computing, Networking and Communications (ICNC)*, pp. 353–357, Big Island, HI, USA, 2020.

[2] A. M. Bedewy, Y. Sun, and N. B. Shroff, "Age-optimal information updates in multihop networks," in *2017 IEEE International Symposium on Information Theory (ISIT)*, pp. 576–580, Aachen, Germany, jan 2017.

[3] C. Kam, S. Kompella, G. D. Nguyen, and A. Ephremides, "Effect of message transmission path diversity on status age," *IEEE Transactions on Information Theory*, vol. 62, no. 3, pp. 1360–1374, 2016.

[4] R. Talak, S. Karaman, and E. Modiano, "Minimizing age-of-information in multi-hop wireless networks," in *2017 55th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, pp. 486–493, Monticello, IL, oct 2017.

[5] C. Kam, S. Kompella, G. D. Nguyen, J. E. Wieselthier, and A. Ephremides, "Age of information with a packet deadline," in *2016 IEEE International Symposium on Information Theory (ISIT)*, vol. 2016, pp. 2564–2568, Barcelona, Spain, jul 2016.

[6] X. Wei, J. Liu, Y. Wang, C. Tang, and Y. Hu, "Wireless edge caching based on content similarity in dynamic environments," *Journal of Systems Architecture*, vol. 115, article 102000, 2021.

[7] Y. Xu, Y. Xu, and A. Anpalagan, "Database-assisted spectrum access in dynamic networks: a distributed learning solution," *IEEE Access*, vol. 3, pp. 1071–1078, 2015.

[8] W. Wang, H. Xu, M. Alazab, T. R. Gadekallu, Z. Han, and C. Su, "Blockchain-based reliable and efficient certificateless signature for IIoT devices," *IEEE Transactions on Industrial Informatics*, p. 1, 2021.

[9] J. Song, Q. Zhong, W. Wang, C. Su, Z. Tan, and Y. Liu, "FPDP: flexible privacy-preserving data publishing scheme for smart agriculture," *IEEE Sensors Journal*, p. 1, 2020.

[10] L. Zhang, Y. Zou, W. Wang, Z. Jin, Y. Su, and H. Chen, "Resource allocation and trust computing for blockchain-enabled edge computing system," *Computers and Security*, vol. 105, article 102249, 2021.

[11] W. Wang, H. Huang, L. Zhang, and C. Su, "Secure and efficient mutual authentication protocol for smart grid under blockchain," *Peer-to-Peer Networking and Applications*, no. article 1020, pp. 1–13, 2020.

[12] Z. Lejun, Z. Zhijie, W. Weizheng et al., "A covert communication method using special bitcoin addresses generated by vanitygen," *Computers, Materials and Continua*, vol. 65, no. 1, pp. 597–616, 2020.

[13] W. Wang and C. Su, "Ccbrsn: a system with high embedding capacity for covert communication in bitcoin," in *IFIP International Conference on ICT Systems Security and Privacy Protection*, pp. 324–337, Maribor, Slovenia, 2020, September.

[14] L. Zhang, M. Peng, W. Wang, Z. Jin, Y. Su, and H. Chen, "Secure and efficient data storage and sharing scheme forblockchain-based mobile-edgecomputing," *Transactions on Emerging Telecommunications Technologies*, no. article e4315, 2021.

[15] R. B. Myerson, *Game Theory: Analysis of Confict*, Harvard University Press, Cambridge, MA, USA, 1991.

[16] J. Zheng, Y. Cai, N. Lu, Y. Xu, and X. Shen, "Stochastic game-theoretic spectrum access in distributed and dynamic environment," *IEEE Transactions on Vehicular Technology*, vol. 64, no. 10, pp. 4807–4820, 2015.

[17] M. A. Shattal, A. Wisniewska, A. Al-Fuqaha, B. Khan, and K. Dombrowski, "Evolutionary game theory perspective on dynamic spectrum access etiquette," *IEEE Access*, vol. 6, pp. 13142–13157, 2018.

[18] A. K. Lamba, R. Kumar, and S. Sharma, "Joint user pairing, subchannel assignment and power allocation in cooperative non-orthogonal multiple access networks," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 10, pp. 11790–11799, 2020.

[19] S. Gopal, S. K. Kaul, R. Chaturvedi, and S. Roy, "A non-cooperative multiple access game for timely updates," in *IEEE INFOCOM 2020 - IEEE conference on computer communications workshops (INFOCOM WKSHPS)*, pp. 924–929, Toronto, ON, Canada, 2020.

[20] A. Jella and S. L. Sabat, "Dynamic channel access of secondary users in a heterogeneous network using game theory," in *2018 10th International Conference on Communication Systems & Networks (COMSNETS)*, pp. 425–428, Bengaluru, 2018.

[21] L. Toka, M. Szalay, D. Haja, G. Szab, S. Rcz, and M. Telek, "To boost or not to boost: a stochastic game in wireless access networks," in *ICC 2020 - 2020 IEEE International Conference on Communications (ICC)*, pp. 1–6, Dublin, Ireland, 2020.

[22] A. Khodmi, S. B. Rejeb, N. Agoulmine, and Z. Choukair, "Joint user-channel assignment and power allocation for non-orthogonal multiple access in a 5G heterogeneous ultra-dense networks," in *2020 International Wireless Communications and Mobile Computing (IWCMC)*, pp. 1879–1884, Limassol, Cyprus, 2020.

[23] W. Yuan, P. Wang, W. Liu, and W. Cheng, "Variable-width channel allocation for access points: a game-theoretic perspective," *IEEE Transactions on Mobile Computing*, vol. 12, no. 7, pp. 1428–1442, 2013.

[24] Z. Wang, F. Yang, S. Yan, S. Memon, Z. Zhao, and C. Hu, "Joint design of coalition formation and semi-blind channel estimation in fog radio access networks," *China Communications*, vol. 16, no. 11, pp. 1–15, 2019.

[25] B. Wang, Yongle Wu, K. J. R. Liu, and T. C. Clancy, "An anti-jamming stochastic game for cognitive radio networks," *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 4, pp. 877–889, 2011.

[26] S. Kaul, R. Yates, and M. Gruteser, "Real-time status: how often should one update?," in *2012 Proceedings IEEE INFOCOM*, pp. 2731–2735, Orlando, FL, USA, mar 2012.

[27] K. Verbeeck and A. Nowe, "Colonies of learning automata," *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, vol. 32, no. 6, article 772780, pp. 772–780, 2002.

[28] P. S. Sastry, V. V. Phansalkar, and M. Thathachar, "Decentralized learning of Nash equilibria in multi-person stochastic games with incomplete information," *IEEE Transactions on systems, man, and cybernetics*, vol. 24, no. 5, article 769777, pp. 769–777, 1994.

[29] D. Monderer and L. S. Shapley, "Potential games," *Games and economic behavior*, vol. 14, no. 1, article 1243143, pp. 124–143, 1996.