RESEARCH ARTICLE OPEN ACCESS

Adaptive Detect and Protect Against Jamming Attacks on Ad Hoc Networks using Game Theory and Channel Switching (GTCS)

Alaa Mahfoud [1], Boushra Maala [2], Haisam Alradwan [3]
Tishreen University
Lattakia, Syria

ABSTRACT
Ad Hoc networks are decentralized and self-organizing networks. The nodes communicate with each other using multi-hop wireless connections. The applications of these networks vary between civil, military, wireless sensors and up to the modern and future applications of the Internet of Things. These networks are characterized by the fact that they do not include infrastructure and are deployed in open environments. These characters make them vulnerable to security challenges. The attacks on the network are the most prominent of these challenges. A jamming attack is one of the most dangerous attacks on these networks because it makes the network unavailable to actual users. In this paper, we present new algorithm, we called it GTCS to detect and avoid jamming attacks in multi-channel wireless networks. This algorithm depends on continuous monitoring of network parameters and runs a repeated game to obtain the best channel to switch to immediately after jamming is detection. Simulation scenarios were built using NS3 software and applying the proposed algorithm. Simulation results show that GTCS performs better than the reference method in terms of throughput, delay, and power consumption.
Keywords :— jamming attack, Ad Hoc networks, game theory, channel switching.

I. INTRODUCTION

Wireless networks are the most popular and widespread types of networks recently, because of the development of wireless technologies, ease of deployment and installation, flexibility, and low cost. The development of computing and networking technologies opened the way for the emergence of new types of wireless networks, such as wireless sensor networks, smart transport networks, etc. [1], [2], [3]. The wireless and mobile networks have become part of our modern lives and daily activities. These networks vary in terms of topology and applications used for them. Ad Hoc wireless networks are defined as wireless networks that do not include infrastructure. This network depends on establishing a direct connection between the nodes or using the multi-hop to connect to the remote nodes. Therefore, the applications of these networks existing in various fields, including MANET networks, intelligent transport systems, some wireless sensor applications, the Internet of things, and others.

Ad Hoc networks are cost-effective, fast to deploy, and open environment. But these features pose many challenges to these networks in terms of routing, reliability, and security. The attacks on Ad Hoc networks are the most serious challenges because they threaten the continued functioning of the network and the access of services. The attacks differ in terms of methods of implementation and the target network layer. A jamming attack is one of the most dangerous attacks on wireless networks because it makes the network unavailable. It causes packets not to reach the target. Therefore, retransmissions occur and network performance will decrease.

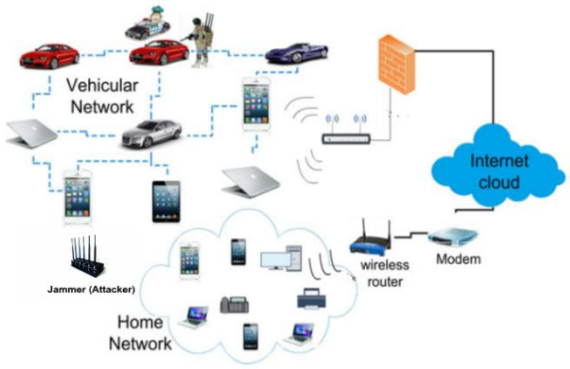

Fig.1 example of a jamming attack on wireless networks

A jamming attack is a special level of DoS (Denial of Service) attack. It works to affect the transmission in the network by flooding the network with fake information [4], as shown in Fig.1. Jamming can attack MAC, network, or application layers. Therefore, it difficult for detection. The node that attacks the network is named the jammer. While the jamming region is the area where the attack occurs [5], [6].

II. THE JAMMING ATTACKS ON WIRELESS NETWORKS AND THEIR EFFECTS

The jammer uses deliberate radio interference to damage the wireless connection. It keeps the communication medium busy. This leads to a failure of the real connections among the nodes. This can be done by affecting the received signal by reducing the signal-to-noise ratio (SNR) or by pushing the transmitter into the waiting space. Since the wireless medium is busy [7]. There are several jamming attack strategies. They

can be divided into multiple classes according to the time and the frequency models or to the layer [8,9]:

1) Constant jammer: Continuous radio signals which are always random. It is disregarding the MAC protocols. But they are a random bit sequence. The attacker generates random data and forms packets. Then, it broadcasts them continuously in the channel during fixed intervals without regard to channel busy. After sending the data in the channel, it collides with the actual data, which leads to loss of the data, and a lack of reaching its target.
2) Deceptive jammer: The attacker injects real packets into the channel without any separation between the sequence of sent packets (i.e. broadcasting packets quite similar to the real sent packets between nodes). As a result, the real connection will fool and the nodes will believe that these packets are real and receive them. In this type of jamming, the attacker must have the ability to know the sender, receiver, and the type of sent data to generate deceptive packets, then broadcasts them in the communication channel. When spoofed packets reach the target with real packets, the node will consume its resources to process packets and distinguish fake data.
3) Random jammer: This type of jamming depends on the alternation between sleep and wake up modes. After the jammer attack for some time, it turns off its radio unit and enters sleep mode for period of time. The goal of applying sleep and wake up mode is to conserve jammer energy. Sleep and wake periods are randomly determined.
4) Reactive jammer: The principle of its operation is that there is no need to jam the channel when there is no connected node [10]. The attacker remains idle as long as the channel is vacant. The attacker begins to transmit the radio signal when it senses that there is an activity in the channel. Thus, affecting the channel's operation. The jammer in this attack needs to monitor the channel permanently, thereby consuming energy effectively.

III. GAME THEORY

It is a set of mathematical models developed to study conflict and cooperation situations. The game aims to obtain the best decisions for stable result. Game theory is applied in many disciplines such as economics, biology, computer science, etc. [11]. Game theory can enable players to predict each other's rational behaviour and suggest a course of action to be taken in any given situation. The game is the main component of game theory. In general, the game should include the following components:

1) At least two players: such as companies, sample space, wireless nodes, etc. For example, a game can consist of A and B players who compete for a benefit. We define the group of players as I = {1,2,…, n}. where n is a positive integer representing the number of players in the game.
2) Strategies for each player: Each strategy has a specific action or a choice. Each strategy takes a specific probability so that the total probability of the strategies for each player equals 1. If we take a player i. We define Si = {s1, s2, .., sn} a set of available strategies For player i, each strategy is called a pure strategy.
3) The strategies chosen by the players determine the outcome of the game.
4) Each outcome determines a set of gains or benefits for each player. For the set of strategies S, the benefits for player i is Ui (s1, s2, .., sn).

In terms of player-to-player relations, games can be divided into two types, cooperative and non-cooperative games. In cooperative games, more than one player can participate in a strategy. While non-cooperative games, each player is independent of the other. The games classified into static and dynamic games. In static games, all players apply their strategies simultaneously while the dynamic games depend on a series of moves.

A. Nash equilibrium

It is chosen by the players to maximize their gains. It is a set of strategies (strategy for each player). This strategy is the best of all strategies available to each player [12].

B. Repetitive games

Players make their decisions simultaneously in static games. But some games enable players to make decisions during the game and respond to their opponents. Games can be either finished or unfinished. Such as, repeated games in which a player repeatedly plays the game and can see the results of previous games [12].

C. Related works

There are a lot of researches has dealt with the topic of detecting jamming attacks on Ad Hoc networks. In [13], researchers presented a method for detecting jamming, based on taking a set of samples for network parameters with jamming and without jamming. Then, building a scheme for these samples and training the network in detecting jamming. In [14], the researchers presented a method for detecting the attack that depended on several parameters such as energy, received power, and rate of received packets. After that mathematical calculation of a threshold for each parameter. Then, detected jamming when one of the parameters exceeded the threshold. The researchers adopted in [15] to measure changes in time intervals between the received packets to detect the state of jamming in the wireless sensor networks. In the research [16], the researchers did not use a specific threshold. The threshold was calculated in real-time based on a time-dependent analysis method. In [17], the researchers relied on observing two parameters, the Packet Sent Ratio (PSR) and the received packet rate. The work of the proposed algorithm is divided into two parts:

1) The first section is PSR && SS aims to detect jamming. If the received packet rate is low, it will expect jamming, but it also measures the received signal strength. If the signal strength is large and the received packet rate is low, it will

be considered jamming and move to the second section.

2) The second section is PSR && PDR aims to find the type of jamming according to the four types of jamming. It depends on the parameters of MaxPSR and MinPDR.
3) jamming type is determined according to the four types of jamming by comparison of MaxPSR and PSR threshold.

In [18], The researchers presented an algorithm called DJAVAN (Detecting Jamming Attacks in Vehicle Ad hoc Networks). This algorithm relies on measuring the rate of packets received during specific time intervals. After that it calculates the difference in the rate of packets received over time (the rate of PDR decrease). This method determines the state of jamming if the value of the PDR is below the threshold or if the speed of the decrease of the PDR is greater than the decreasing threshold. In [19], the researchers presented a statistical study-based detection method for RTS (Request to Send) and CTS (Clear to Send) control frame information changes in CSMA (Carrier-Sense Multiple Access) wireless networks. It concluded a detection threshold to improve the process of Jamming attack detected. In [20] the researchers presented a study of network throughput in the IEEE 802.11 standard under the jamming. The study based on stochastic geometry theory, provides a vision for the distribution of network nodes and jammers. It examines the possibility of network collision from the perspective of the physical layer and the MAC layer. In [21], the researchers proposed a method called Countermeasure Detection and Consistency Algorithm (CDCA). This method measures the signal strength of the channel and compares it with the signal strength threshold. Then, it measures the location of the node and compares it with the site threshold. The method includes two types of monitoring, periodic and continuous. The algorithm includes a zero-sum game consisting of two players. The first is the monitoring node and the second is jammer. Also includes the strategies and benefits of each strategy are calculated. It chooses the strategy that yields the greatest gains for the first player and the lowest gains for the second player.

IV. SUGGESTED GAME

Our game consists of three components: the player group, the strategy group, and the benefits group. In our proposed model, each node is a rational player trying to get the best channel without jamming. The set of strategies includes wireless channels that available to the node, expressed in C = {c_1, c_2, ...c_n}, where n is the number of available channels. The set of benefits reflects the gains that the player gets from choosing each strategy. These gains calculated via a set of parameters related to the wireless channel. In selecting the channel, we will rely on weights that are calculated based on the impact of the jamming on the network parameters. We define w_t (c) as the weight when selecting channel c in time t from the set of available channels C. This following equation is calculating the probability of selecting the channel:

$$Pt(c) = \frac{W_t(c)}{\Sigma c \epsilon C\ W_t(c)} \quad [22], [23] \quad (1)$$

At the beginning of the game, the values of all weights are determined by 1. We update the weights after each channel selection according to the following equation:

$$W_t(c) = W_{(t-1)}(c)\beta^{Mi(c)} \quad [23] \quad (2)$$

β is the game parameter, which is a number in the field [0-1]. M_i(c) is the loss experienced by node i on channel c as a result of jamming on this channel. We used a PDR that is the ratio of correctly received packets to total transmitting packets. PDR takes a range from 0 to 1. PDR is one of the most important network parameters that are affected by jamming. We will use the loss in the value of the PDR as a parameter in calculating the loss suffered by the node due to the jamming, where: PDR * = 1- PDR.

The node measures the signal strength received on the RSS channel. It is one of the main network parameters in the jamming detection. When jamming occurs, the jamming signal is added to the signal transmitted across the channel, thereby increasing the signal strength that the receiver measures. We define RSSstart as the initial signal strength measured by the node on the specified channel. We define averageRSS as the average signal strength that measured during of channel working. We define the percentage of change in the received signal strength RSSratio:

$$\text{RSSratio} = \frac{|averageRSS - startRSS|}{startRSS} \quad (3)$$

We calculate the amount of loss due to interference by using the equation:

$$Mi(c) = \frac{1}{2}\ (RSSratio + PDR^*) \quad (4)$$

Each player calculates the loss for each available strategy and stores it in the M_i Matrix which is the Loss Matrix. Weights are updated according to equation (2) and stored for each strategy in the loss matrix. The game is repeated several times we call it game rounds [1, T], and each time the channel is chosen according to the calculated weights. These weights are refreshed after each repetition.

A. Game validation

We will use the Markov chain to represent the game and the transition between channels [24]. The channel state is determined as the state space of the Markov model. The benefit is Pi = 1- M_i represents the reward for moving from channel c to channel c'. The probability that the node will choose a channel is given using the Boltzmann distribution. The probability of moving the node from channel c to channel c' is represented by equation (5), which expresses the reward at the target channel over the sum of the rewards for all channels:

$$Qi,c = \frac{e^{\frac{Pi\,[c]}{\lambda}}}{\Sigma k \epsilon C\, e^{\frac{Pi\,[k]}{\lambda}}} \qquad [24] \qquad (5)$$

λ an important parameter in the learning process and the smaller its value, the less random.

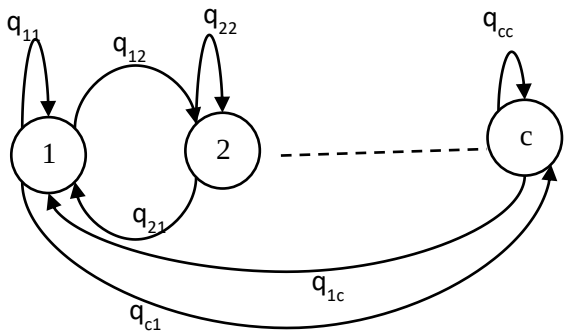

Fig.2 Markov diagram of the channel selection process.

The representation of the proposed game according to the Markov chain, as in Fig. 2 is useful in calculating the number of game repetitions. Therefore, the results are accurate by comparing the resulting probabilities with the Markov model. We do not need to use the concept of Nash Equilibrium in the proposed game to reach the best solution, because we use the principle of updating double weights. The learning algorithm cannot work with Nash Equilibrium because the game is a bi-matrix game [22].

We used MATLAB Environment to validate the game by calculating the final possibilities for selecting channels. After that comparing them with the Markov model and calculating the number of game repetitions to consider the game results correct. The tested model includes 11 wireless channels that are jammed in different ratios. We define the loss matrix M with fixed values as in Table (1). We calculate the probabilities according to the Markov test model Equation (5). Apply the proposed game and increase the number of repetitions gradually (number of times weights update). When the value of β increases, the accuracy of the game increases. But it becomes slower and requires more repetitions [23]. After validation, we adopted a value of λ in the Markov equation equal to 0.1. Therefore, the value of β (we named it the game characteristic) is β = 1- λ = 0.9. In Fig. 3, we can see that the number of repetitions that required to get a high accuracy is about 90 repetitions. But when we using β equal to 0.8, The game becomes faster (about 25 repetitions) but less accurate.

TABLE I

CHANNEL LOSSES IN THE TEST MODEL

Channel	1	2	3	4	5	6	7	8	9	10	11
Lose	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.8	0.8	0.9

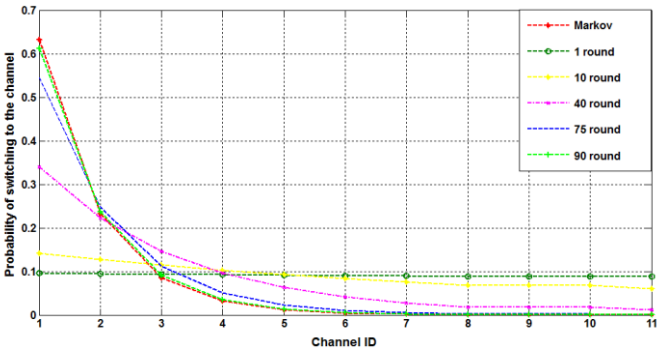

Fig.3 game validation

V. RESULTS AND DISCUSSION

We built our simulation scenarios using Network Simulator 3. We used additions to support jamming on wireless networks [25]. NS3 is an open-source network simulator that supports a large number of network protocols besides the ability to make improvements, study different parameters, show results and analysis. We built an Ad hoc network of six nodes exchange data among them. The jammer node can jam all nodes over the network, as shown in Fig. 4. Node 0 sends data for node 2 and node 6 is jammer.

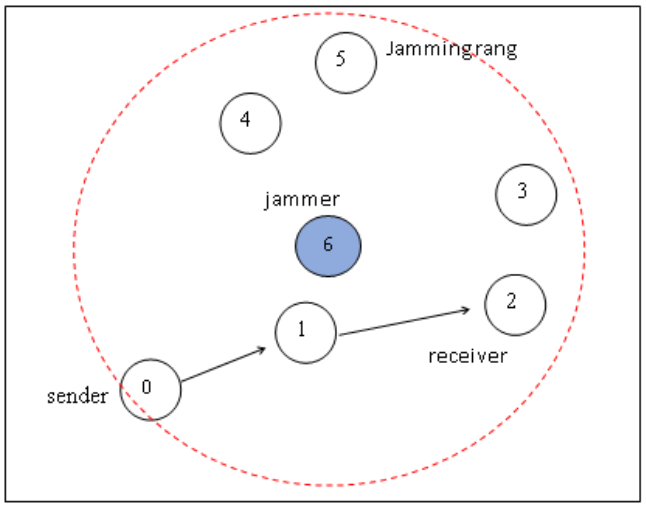

Fig. 4 The studied network

We choose Direct Sequence Spread Spectrum (DSSS) technology in the physical layer because it is the highest technology that resists noise, interference, and fading. We used standard 802.11 wireless networks. The simulation parameters used are shown in Table 2.

TABLE II

SIMULATION PARAMETERS

Network type	Ad hoc	Data rate	1Mbps
Network size	500x500m²	Physical layer protocol	802.11b-DSSS
Number of nods	6	Number of channels	11
Number of jammers	1	Transmission power	1mw
Simulation time	100s	Node energy	0.1J
Number of packets	10000	Jamming start time	5s

A. *The first scenario*

We performed simulations on the previous network by applying reactive jamming. We increased the rate of network generation data by using interval value in a range from 0.1 to 1. The scenario aims to study the effect of increasing the data sent on the performance of the algorithm. We studied the parameters of the network according to three cases:

1) Without using protection.
2) CDCA reference study [21].
3) Suggested proposed method: with a value of β = 0.9 and the number of repetitions = 90.

Fig. 5 presents a chart of the average energy consumption when using the previous three cases compared to the interval data generation rate. We note that the proposed method achieves the lowest energy consumption among the three studied cases. Because it works to switch the channel at every sense of jamming. Therefore, there are no retransmissions, so energy consumption decreases. We note that the power consumption increases with the decrease in the value of the time interval, this is due to the increasing of the number of transmitted packets. Thus, the consumed energy increases in transmission and receiving.

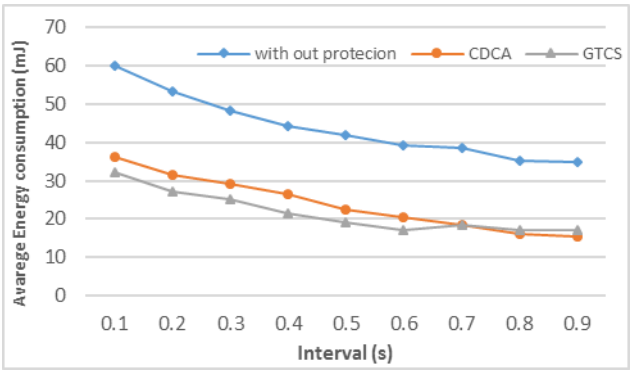

Fig. 5 Average consumed energy according to the value of the time interval

The power consumption increases if no jamming techniques are used. This increases up to 29 mJ at a 0.3-second interval because of the jamming effect that causes transmission failure and more retransmission. We find that the power consumption in the reference method is higher than the proposed method. This difference is about 3.7 mJ at a 0.2-second interval. At large interval values, power consumption is converged between the two methods because the number of packets transmitted is low, so the jamming effect is low. Fig.6 shows a chart of the average total delay compared to the change in the interval value. Note that the delay value is greater at low interval values. Due to the increased number of generated packets which results in increased packet waiting time and congestion. In the first case, the delay value is high due to the effect of jamming and repeated retransmissions. The delay values in the GTCS case are less than CDCA values around 3.9 ms. Because the proposed method is more active in detecting jamming and avoids it by applying channel switching.

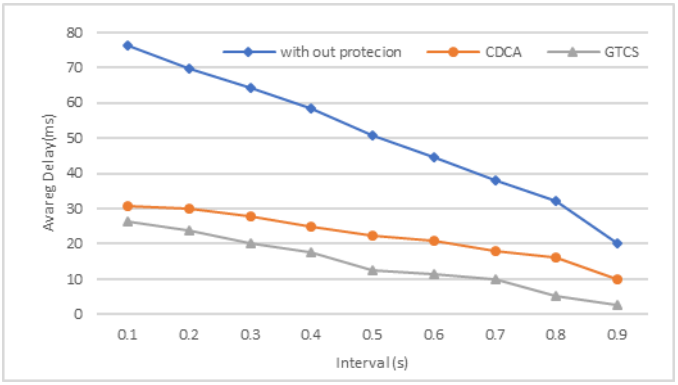

Fig. 6 average total delay according to the value of the time interval

Fig. 7 shows a chart of the average throughput for each value of interval. We found that the proposed method GTCS achieved the highest throughput between the three cases because of the speed of the jamming detection and the decrease in the overall delay. The proposed case throughput value is approximately 1.5kbps on average over the reference method. When the rate of packet generation increases, the throughput increases. This increases because the number of packets arriving correctly becomes larger. The throughput decreases with a decrease in the rate of packet generation. So, the performance of reference and proposed methods converge because all of the packets that sent reach their goal using the two methods.

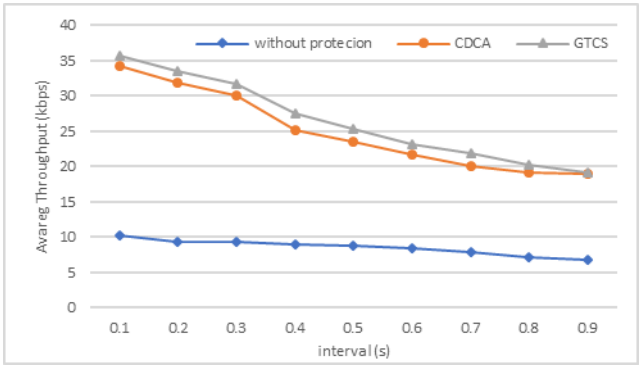

Fig. 7 Average network throughput according to the value of the interval

B. *The second scenario*

We simulated the network with the same parameters, but with the number of attackers gradually increasing from 1 to 4.

The results are collected as an average when the network is running for 50 seconds. The goal of this scenario is to study the effect of increasing the number of attacking nodes on the algorithm performance.

Fig. 8 shows a chart of the average consumed energy when changing the number of attackers from 1 to 4. We notice that the energy that is consumed in the first case is higher (up to 19.3 mJ) compared to the reference method for four attacking nodes. We noted that the average consumed energy in the proposed method is smaller than the reference (about 11 mJ in the case of four attacking nodes). The reason for this decrease is that the increase in the number of attacking nodes increases the effect of the jamming. The proposed method responds to each jamming process with dynamic channel switching. The reference method depends on the positions of nodes. These positions affected by the increase in the number of attacking nodes, which increases energy consumption.

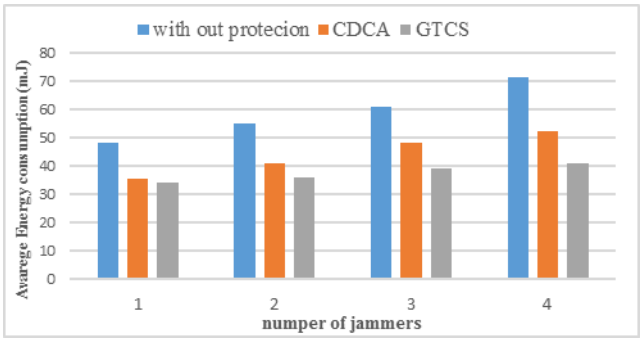

Fig. 8 The energy consumed according to the number of attackers

Fig. 9 shows a chart of the average total delay according to the number of attacking nodes. We notice that the average delay is large in the first case and increases as the attacking nodes increase due to the increased jamming effectiveness. We note that the average delay in the proposed method is smaller than the reference method (for example, about 20 milliseconds when attacking by four nodes). This decreasing because of GTCS attack protection technics depends on the fast transition to the best channel chosen by the game. The delay increases with the increase in the number of attacking nodes because of the additional delay to detect the effect of each attacking nodes separately.

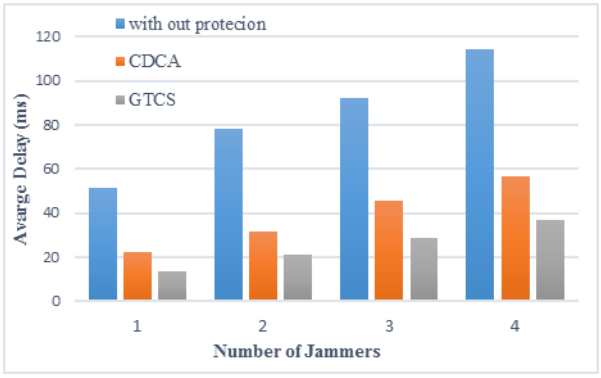

Fig. 9 Average total delay according to the number of attacking nodes

Fig.10 shows a chart of the average throughput depending on the number of attacking nodes. We note that the throughput value is close between the proposed and reference method in the case of one attacking node (about 5kbps). This difference increases with the number of attacking nodes increasing to about 21kbps when attacking with four nodes. The reason is due to the speed of detection of jamming in the proposed method and thus higher throughput.

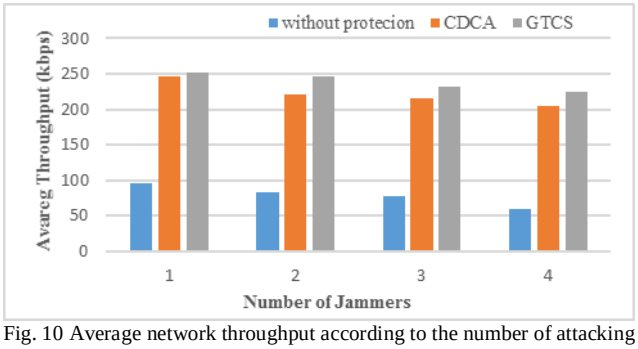

Fig. 10 Average network throughput according to the number of attacking nodes

C. *The third scenario*

We simulated for 50 seconds and studied the three cases according to the network parameters. Fig.11 shows a diagram of the amount of energy consumed during the simulation time. We notice that the amount of energy consumed before the moment of start jamming in the case of non-use of protection is less than the reference method CDCA and the proposed method GTCS. This is due to the use of protection methods that increases the processing works. Therefore, increasing energy consumption. We found that GTCS consumes less energy than CDCA over the entire simulation time. For example, this difference reaches to 3.2 mJ at time 35 seconds. The speed in detecting jamming causes this enhanced energy consumption in the proposed method. Hence the speed in avoiding its impact on the network. Also, GTCS used less processing then consuming less energy.

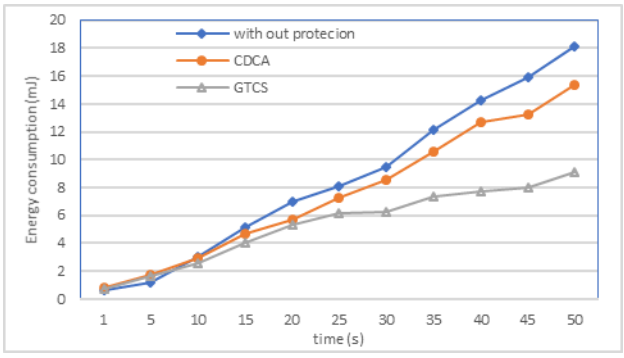

Fig. 11 is the amount of energy consumption during simulation time

Fig. 12 shows a chart of the total network delay during simulation time. When the network simulation begins and before the jamming starts, the delay in the first case which does not include protection is smaller than other methods. Because it does not add any calculations then it does not add delay on the network. This difference about 1.2 mJ at time 1

second. We find that the proposed method GTCS suffers less delay than the reference method. We note that this delay is approximately stable at 15 milliseconds in the GTCS compared to 23 milliseconds in CDCA. We explain the decrease delay in the case of GTCS due to the speed of jamming detection and switching to a new channel. Because it uses continuous monitoring and does not work only When jamming is detected (like CSCA).

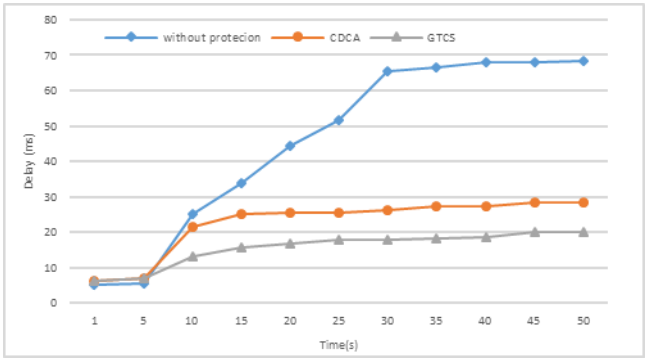

Fig. 12 Total delay during simulation time

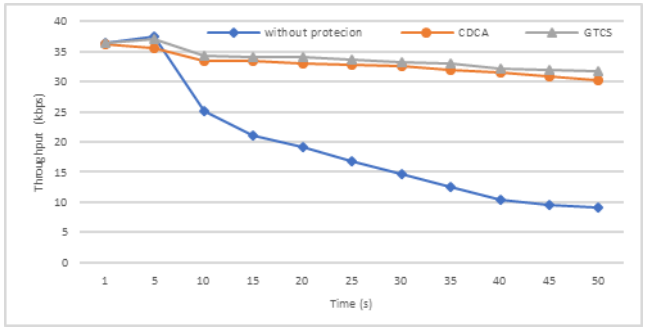

Fig. 13: Network throughput during simulation time

Fig. 13 shows a chart of measured throughput during simulation time. We notice that the value of throughput before jamming occurs is approximately equal in the three cases. After jamming occurs, throughput in the first case decreases pointedly to 31.76 kbps at time 50 seconds. Because the packets don't reach their target. We note that the value of the throughput in the proposed case is higher than the reference case value. Because of the speed of jamming detection and channel switching dynamically. Therefore, the receiving packets continue. The difference between the two methods is about 2.5 kbps.

VI. CONCLUSIONS

In this paper, we present an algorithm to detect and respond to jamming attacks in Ad Hoc networks. Our algorithm based on game theory and channel switching. We compared them with reference studies using different scenarios built using the NS3 simulation environment. After studying the simulation results, we found that the impact of the jamming attack on the performance of Ad Hoc networks is high. It causes energy consumption increases, throughput decreases, and the delay increases because the packets don't reach their target. The proposed algorithm offers better performance in terms of energy consumption. The energy consumption is reduced to about 5% compared to the reference method. Because it requires fewer calculations but we found that the energy consumption is close in case of a low load network. We found the delay in the proposed GTCS algorithm lower than the CDCA reference algorithm by about 7% on average. The reason is the speed of jamming detection and switching to the best channel in GTCS. Throughput in the proposed algorithm increases by about 3.6% over the reference case. This increasing is because of the speed of detection and the change to a new channel. Then, the transmission returns and the throughput value increases. The proposed algorithm provides a fast and low-power method to detect and respond to jamming attacks. It also reduces jamming delay and raises throughput.

ACKNOWLEDGMENT

The research that has led to this work has been supported by the Department of Communication and Electronics, Faculty of Mechanical and Electrical Engineering, Tishreen University. The authors wish to thank everyone contributed to this work.

REFERENCES

[1] LU, Z. WANG, C and WEI, M. *On detection and concealment of critical roles in tactical wireless networks*, in Military Communications Conference. MILCOM -IEEE, Oct 2015, 909–914.

[2] SHARMA, K and BHATT, S. Jamming Attack – A Survey. International Journal of Recent Research Aspects, Vol. 5, Issue 1, March 2018, pp. 74-80.

[3] SINGH, J and GUPTA, S. *Impact of Jamming Attack in Performance of Mobile Ad hoc Networks.* International Journal of Computer Science Trends and Technology (IJCST) – Volume 5 Issue 3, May – Jun 2017, 184-190.

[4] ANWAR, A. ATIA, G. and GUIRGUIS, M. *Adaptive topologies against jamming attacks in wireless networks: A game-theoretic approach.* Journal of Network and Computer Applications, Vol. 121, November 2018, 44-58.

[5] JAIN, A. BHUSHANWAR, K and MALVIYA, V. *A Survey on Jamming Attacks and Its Types in Wireless Networks.* International Journal of Technology Research and Management, Vol. 4, no.6, June 2017, 1-8.

[6] LU, Z. WANG, C and WANG, M. *Modeling, evaluation and detection of jamming attacks in time-critical wireless applications.* Mobile Computing IEEE Transactions, vol. 13, no. 8, 2014, 1746–1759.

[7] SIVANESHSAN, B and THARMALINGAM, A. *Impacts and prevention techniques of jamming attacks in Wireless ad hoc networks*. SSRG International Journal of Mobile Computing & Application (SSRG-IJMCA) ,vol. 4, Issue1, 2017, 13-18.

[8] VARMA, K and SATYANARAYANA, B. *Jamming Attacks: An Approach for Prevention*. IJCST Vol. 5, Iss ue 3, July - Sept 2014.

[9] CHOWDARY, N and GUMPULA, R. *Efficiently Detecting and Solving the Wireless Network Attacks – Jammers.* IJCST Vol. 3, Iss ue 3, July - Sept 2012.

[10] PAHUJA, S and JINDA, P. *Cooperative Communication in Physical Layer Security: Technologies and Challenges.* Springer Science+Business Media, LLC, part of Springer Nature 2019.

[11] IQPAL, A. GUNN, L. GUO, M. BABAR, A and ABBOTT, D. *Game theoretical modelling of network/cybersecurity*. IEEE. Vol. 7. 18 October 2019

[12] CHARILAS, D and PANAGOPOULOS, A. *A survey on game theory applications in wireless networks.* Computer Networks 54(18):3421-3430. December 2010.

[13] WEI, X. SUN, Q. HU, F and WANG, T. *Association Graph based Jamming Detection in Multi-Hop Wireless Networks*, 2017 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC), 397-402.

[14] HYMLIN, S and JAYASREE, T. *Detection of Jamming Attacks in a cluster WSN using Statistical Approach*. International Conference on Recent Trends in Computing, Communication and Networking Technologies (ICRTCCNT‟19), October 18-19, 2019, Chennai, Tamilnadu, India.

[15] OSANAIYE, O. ALFA, A and HANCKE, G. *A Statistical Approach to Detect Jamming Attacks in Wireless Sensor Network*, Sensors (Basel). Vol. 18, Issue 6, May 2018.

[16] CHENG, M. LING, Y and WU, W. *Time Series Analysis for Jamming Attack Detection in Wireless Networks.* GLOBECOM 2017 - 2017 IEEE Global Communications Conference, 4-8 Dec. 2017.

[17] YU, B and ZHANG, L. *An Improved Detection Method for Different Types of Jamming Attacks in Wireless Networks.* IEEE Explore, 15 January 2015, 553-558.

[18] MOKDAD, L. OTMAN, J and NGUYEN, T. DJAVAN: *Detecting Jamming Attacks in Vehicle Ad hoc Networks.* Elsevier, Performance Evaluation (2015), Vol. 87, May 2015, 47-59.

[19] FANG, F. LI, Y. NIU, Y. WANG, Y and HAN, *CH. Research on Attacks Detection in CSMA Wireless Networks*. 2019 11th International Conference on Wireless Communications and Signal Processing (WCSP). IEEE, 09 December 2019.

[20] WEI, X. WANG, T and TANG, CH. *Throughput Analysis of Smart Buildings-oriented Wireless Networks under Jamming Attacks*. Springer, Mobile Networks and Applications (2019).

[21] FADELE, A. OTHMAN,M. HASHEM, I. YAQOOB, I. IMRAN, M and SHOIB, M. A *novel countermeasure technique for reactive jamming attack in internet of things.* Springer Science+Business Media, LLC, part of Springer Nature 2018.

[22] DASKALAKIS, C. FRONGILLO, R. PAPADIMITRIOU, C. PIERRAKOS, G and VALIANT, G. *On Learning Algorithms for Nash Equilibria*. Springer Berlin Heidelberg, 2010. 114–125.

[23] NEZHAD, M and ALABERN, L. *Adaptive Channel Assignment for Wireless Mesh Networks Using Game Theory.* 2011 Eighth IEEE International Conference on Mobile Ad-Hoc and Sensor Systems, 746-751.

[24] L Weibing, W Xianjia, H Binbin, *Evolutionary Markov games based on neural network, in Proceedings of the 6th International Symposium on Neural Networks: Advances in Neural Networks - Part III.* ISNN 2009 (Springer, Berlin, Heidelberg, 2009), pp. 109–115.

[25] Ns3. Portal. [Online]. Available: http://www.nsnam.org, LAST VISITE 1/4/2020.