Wireless Personal Communications (2019) 108:2261–2277
https://doi.org/10.1007/s11277-019-06521-9

Countermeasure with Primary User Emulation Attack in Cognitive Radio Networks

Seyed Abdolazim Vaziri Yazdi[1] · Mahdieh Ghazvini[1]

Published online: 21 May 2019

Abstract

One of the most challenging issues in Cognitive Radio Networks (CRN) is to detect Primary User Emulation Attack (PUEA). In the absence of Primary Users (PU), the attackers mimic PUs' signal characteristics to fool legitimate Secondary Users (SU) that evacuate the channel for them, in order to use the channel selfishly. Many works have been done to detect PUEA; among them, localization and encryption and so on are the examples. Recently, game theory has been used to detect PUEA. In this paper, a method based on game theory is proposed, that without using any complex calculation and second methods (RSS, GPS and so on), PUEA can be detected. This method is especially proposed for MANET and can be used in any circumstance of CRNs (ad-hoc, centralized, distributed…). It is reliable, with minimum miss detection and no false alarm of PU. Simulation results show that the proposed method has good operations even in dense networks and ultra-dense networks.

Keywords Primary User Emulation Attack (PUEA) · Game theory · Cognitive radio · Attack · Security

1 Introduction

Nowadays, with the development of technology and the increasing use of computer networks, some limitations gradually have been occurred; among these, the frequency of bandwidth limitations are worth mentioning. In the wireless networks all of the bandwidths resold or reserved for certain purposes. In order to fix this problem, cognitive radio networks were born. Here, the users that purchase a bandwidth (so called PUs[1]) do not use this bandwidth constantly, as a result, whenever the bandwidth is empty, other nodes can

[1] Primary users.

✉ Mahdieh Ghazvini
mghazvini@uk.ac.ir; Mgk-ghazvini@yahoo.com; mghazvini@gmail.com

Seyed Abdolazim Vaziri Yazdi
azimvaziri@eng.uk.ac.ir

[1] Department of Computer Engineering, Faculty of Engineering, Shahid Bahonar University of Kerman, Kerman, Iran

use it with certain rules. The second category of users that can use the bandwidth in the absence of PUs, are called SUs.[2] SUs must evacuate the channel whenever one or more PU planned to use it; otherwise the offender node must be punished. As regards to the nature of CRNs, the SUs spend a period of time, making the presence pattern of posing the network for future channel evacuation predictions. This phase is called learning phase and helps SUs to take care of conflicts with PUs. As a result, if an SU is transmitting data, and a PU plans to use the same channel, the other SUs make a signal to tell the transmitting SU to evacuate the channel, and the SU give way to the PU.

Unfortunately, the presence of selfish infields is inevitable, and cognitive radio networks are no exception. CRNs are a subset of the large family of wireless networks; in addition to the general threats of wireless networks, this type has its own specific threats: Jamming, learning threats, Secondary Spectrum Data Falsification and Primary User Emulation Attack[3] are the most important threats that these networks encounter.

The most dangerous threat is PUEA, because detecting is far more difficult than the others. In this type of attack, when PUs are not using the channel and SUs are using it, actually the hostile nodes are emulating the PUs' signal and forcing the SUs to evacuate the channel. With repeating this scenario, the PUEA prevents SUs to have the access to the channel, and vanish the objective of cognitive radio networks, i.e. enjoying the shared use of bandwidth frequency. A number of works have been done to identify and detect this type of nodes, each has its own advantages and disadvantages.

The proposed method is for detecting PUEA in Mobile Ad hoc Networks. In the proposed method there is no need to secondary method for detecting malicious users. The other game theory based methods need a secondary method, including localization and encryption and so on. In the proposed method, the number of miss detection is at most equal to the number of PUs, and the false alarm is zero. Simulation result shows, this proposed method has a better operation than the others in spars and dense networks and also has a good operation in ultra-dense networks.

The rest of this paper is organized as follow. In Sect. 2 the related work has been proposed with their advantages and disadvantages. Section 3 shows, how proposed method find an attacker in details. Section 4 shows, the simulation result supports the assertion that proposed method has a better operation. Finally, in Sect. 5, the conclusion of our work is shown.

2 Related Work

A lot of researches have been done on different applications in order to establish the security in cognitive radio networks. One way to detect PUEA is localization [1]. Generally this is for IEEE 802.22 and it uses TV antenna location for detecting PUEA [1–6]. In [7, 8], GPS is used to locate PUs and detect PUEA However, weather conditions, buildings and obstacles affect localization with GPS. O. León et al., uses RSS[4] to locate PUs [9], but one of the most important things about localization is inability to support nodes mobility. In [10] authors report that the hostile nodes use their mobility to become undetectable. These

[2] Secondary users.

[3] PUEA.

[4] Received signal strength.

of TDOA[5] and FDOA,[6] two methods of localization, has been presented in [11, 12] respectively. Dikita Salam et al. [13], proposed a method called Hyperbolic-based Transmitter Localization technique using TDOA. Obviously, this method with using TDOA, pinpoints PUs' location. However, this method has good results for TV transmitter, but in the network with mobile nodes, this method doesn't work.

The other way to detect PUEA is authentication and encryption methods. Borle et al. [14], uses Cryptographic Signatures in physical layer to detect PUs. In [15], Advanced Encryption Standard chip has been proposed to manipulate sender signals, and in the receiver side this chip decrypts signals.This chip has been declared as cheap. Still a third method [16], uses extra nodes nearPUs to decrease overhead of PU nodes. But these methods still have extra costs for extra accessories. Ureten and Serinken proposed a method called radio frequency fingerprinting [17]. In this method, sampling of signal in a short period of times and signal processing, resulted in detecting PUs. The advantage of this method is reliability; but overhead of signal sampling and complexity of signal processing are its most serious disadvantages. The authors in [18], proposed a method, based on cryptographic technique, that combine Secure Hash Algorithm with Advanced Encryption Standard to enhance the security performance of CRNs. However, this method has a small miss detection and false alarm but huge amount of computation and processing is still its disadvantage. Generally, all these methods require numerous computations and time overhead are costly for networks.

The methods of the third class are based on game theory. In [19] a method is presented that uses a non-zero-sum game to identify selfish node. In this case, there are two types of nodes which include secondary user and controller nodes. Also, there are two phases: sensing and sending. If the controller, in sensing phase, declares that the channel is under use and a node attempts to reach the channel, the controller considers that this node is hostile and selfish. Otherwise, in the sending phase, the controller may, or may not, place the channel under surveillance to detect selfish nodes. If it detects a selfish node, it gains a benefit greater than its surveillance cost; otherwise, it loses its energy and pays an extra cost. For hostile nodes there is a similar scenario. If the attack is performed and the controller is not able to place the channel under surveillance, the selfish node gains a benefit; otherwise, it will be trapped by the controller and declared as a selfish node.

Ta et al. [20] uses a zero-sum game to detect malicious node, unlike [19] that a non-zero-sum game detecting selfish. In the game, the user's gain results in loss of another user. Because of that, the game is a zero-sum game. But in both methods, if more than one malicious and selfish node exist, it won't be working.

In [21], a method has been proposed that design a non-zero-sum game to detect malicious or selfish nodes. First of all, a game has been proposed, then the article continues with detecting all kinds of hostile nodes (selfish, malicious, hybrid). The simulation result shows that Nash equilibrium point is directly depended on a hostile node type.

In [22], a method is proposed which is based on RSS and using game. We have proposed a method based on [22] with a difference, it just uses game theory to detect PUEA node. The other game theory methods are using a secondary method to detect PUEA. For example, the authors in [22] use RSS to detect PUEA. Summary of the related work is shown in Fig. 1 as follow.

[5] Time difference of arrival.

[6] Frequency difference of arrival.

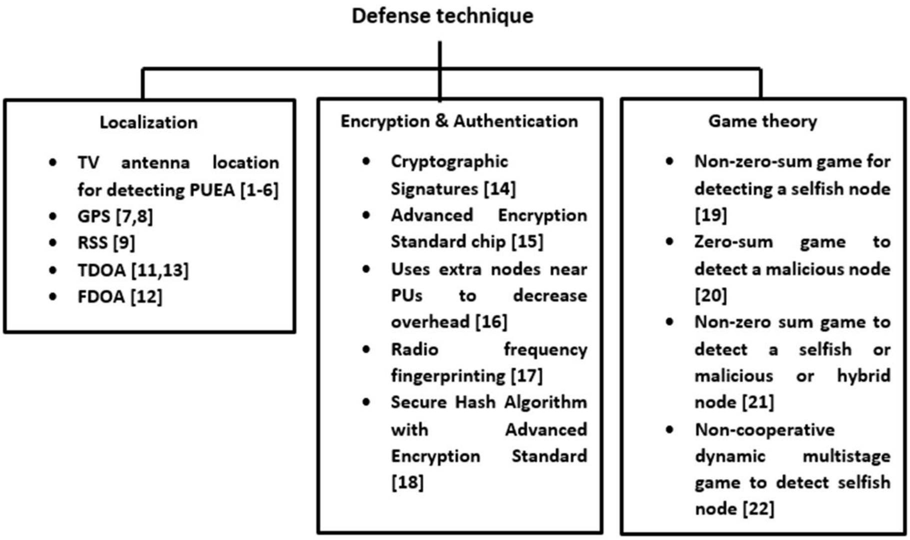

Defense technique
Localization
TV antenna location for detecting PUEA [1-6]
GPS [7,8]
RSS [9]
TDOA [11,13]
FDOA [12]
Encryption & Authentication
Cryptographic Signatures [14]
Advanced Encryption Standard chip [15]
Uses extra nodes near PUs to decrease overhead [16]
Radio frequency fingerprinting [17]
Secure Hash Algorithm with Advanced Encryption Standard [18]
Game theory
Non-zero-sum game for detecting a selfish node [19]
Zero-sum game to detect a malicious node [20]
Non-zero sum game to detect a selfish or malicious or hybrid node [21]
Non-cooperative dynamic multistage game to detect selfish node [22]

Fig. 1 Summary of Defense Techniques to Detect PUEA

3 Proposed Method

The aim of the proposed method is to minimize channel gain of malicious users. In mobile ad-hoc networks, the nodes are moving and there is no centralized controller to supervise the channel all the time. For minimizing malicious users' gain, the false alarm must be decreased and while the false alarm decreasing we must pay attention miss detection not to increase. So, the aim of our proposed method is decreasing false alarm and miss detection; because, false alarm resulted in malicious attacker's benefit and miss detection resulted in PUs not accessing the channel. If false alarm equals to zero, that means the attackers are unable to reach the channel and in this method false alarm is zero.

There are two phases in the proposed method: 1-clustering, 2-using game theory in every cluster. First of all, a periodic coverage based clustering has been done and cluster's head election is done according to the nodes location. Each node that attempts to send data must be a member of a cluster; first of all, the node will send this data to its Cluster Head (CH). Secondly, the CH sends the data to CH of the cluster that contains the destination node. Lastly, CH will send this data to the destination node. All of this steps are performing, if there is no PUs using the channel.

A coverage based clustering is for cooperation of SUs to evacuate the channel and detect PUEA. Since periodic clustering is done, if a node was not a member of a cluster at this time, because of its movement, it would be a member of a cluster at the next time.

Game theory is a tool from Mathematics and Economics. In competition situation, somebody follows the rules and someone breaks the rules by trying to maximize his benefit, the game theory is a good solution. Game theory shows, with following the rules, everyone has gotten fair benefit. Notice, in game theory it's assumed that everyone plays the game rationally.

In CRN, attackers trying to use the channel all the time by breaking the rules. Therefore, game theory is a good solution for countermeasure with these nodes. In this paper, a competition of non-zero-sum game for detecting PUEA is formulated. Since, game theory is a

Table 1 PU = on (with probability of P)

	PUEA	
	Attack	Not-attack
SU		
Switch	R-Cs,-Cm	R-Cs,0
Stay	-C,C'-Cm	-C,0

Table 2 PU = off (with probability of 1-P)

	PUEA	
	Attack	Not-attack
SU		
Switch	-C,G-Cm	–
Stay	G,-Cm	G,0

subset of mathematics, its proofs are more valuable than other methods and for this reason game theory is chosen.

Malicious users with mimicking PU's signal trying to fool SUs. In the proposed method, a game was formulated not to allow the attackers to reach the channel. Whenever, an evacuating signal is propagating, the SUs search an internal table; this internal table is called Trust List Table (TLT) which is an innovation of our method. The TLT is created by first miss detection and by each miss detection is updating and broadcasting. If TLT contains the ID of propagating node, it derives that the node is PU and the channel evacuates; otherwise, the SU stays in the channel. We assume that the attackers are not jammer; so, the interference between SU and PUEA will not happen. It means, if a PUEA propagates an evacuation signal and SU does not evacuate the channel, PUEA is doesn't send data.

According to the formulated game, the SUs and PUEA are the players that compete for using channel. The SUs' have two actions {Switch, Stay} in the channel for legitimate using of the channel. Similarly, PUEA's actions might be in two states {Attack, Not-Attack} for fooling SUs, and these taken actions are in the presence or absence of PUs. Let's define some parameters for the game:

G: This parameter refers to the channel gain. If there is no PUs in the channel and the attacker node has won, this benefit is for attacker; otherwise if there is no PUs and PUEA in the channel this gain is for SUs.

c_s: Cost for switching between the channels.

c_m: Cost for the attack.

C: Penalty for interference of SUs with PUs that happens when a SU fails to evacuate the channel. This penalty is including the number of cycles that SU is not valid to use the channel.

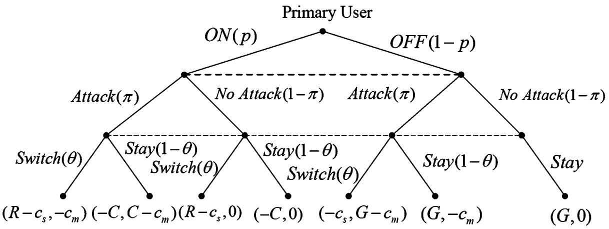
C': Benefit of interference of SUs with PUs.

R: Reputation factor for the SUs that evacuates the channel for PUs.

The relation between these parameters for the SU is:

$$C > G > c_s; R > c_s \tag{1}$$

Fig. 2 The Game's Tree [22]



C must be greater than G, that's why the SUs want to evacuate the channel for more payoff. G must be greater than C_s because the SUs' switching cost is smaller than gain of the channel. R > C_s because the SUs evacuate the channel for PUs and earn more benefit.

And for the PU is:

$$G > c_m;\ C' > c_m \tag{2}$$

If G is smaller than C_m the attacker dose not perform attack, because the benefit of attack is smaller than its cost. C' must be greater than C_m because of same reason.

Details of these strategies have been shown in Tables 1 and 2 as follow:

In Fig. 2, the game's tree is illustrating that summarized in Tables 1 and 2:

The first branch of the tree is interpreted like that: If PUs are on the channel and PUEA are performing an attack and SUs switch to another channel, SUs gain R-c_s and attackers gain -c_m and so on. Another exceptional state is, when there is no PU in the channel and PUEA are not Performing, it is not logical to switch; because, the SUs are not sensing any energy to evacuate channel.

In game theory, if the actions of the players are not predictable, the strategy of the game is a mixed strategy. Whereas in the formulated game, also the actions of all players are not predictable, the strategy of the game is a mixed strategy.

According to the Fig. 1, expected payoff for SUs is calculated by (3), where P is the probability of a PU's existence in the channel, Q is the probability of attack by PUEA, and T is the probability of SU's switching [22]:

$$\boldsymbol{E(s) = P\big(T\big(R - c_s\big) - (1 - T)C\big) + (1 - P)\big(Q\big(-Tc_s + (1 - T)G\big) + (1 - Q)G\big)} \tag{3}$$

The big problem occurs in the false alarm case. As it is shown in Table 2, when no PU exists in the channel and a PUEA is performing the attack and the SUs switch to another channel, it is called a false alarm. In this case, the attacker's gain G-c_m score and the SUs gain -C score that is the worst case. In the proposed method there is no false alarm.

Whereas, inattention to the PU's evacuation signal results in a "C" score penalty, it also contains "G" for not gaining the channel use. So, the simulation result is computed in the worst case.

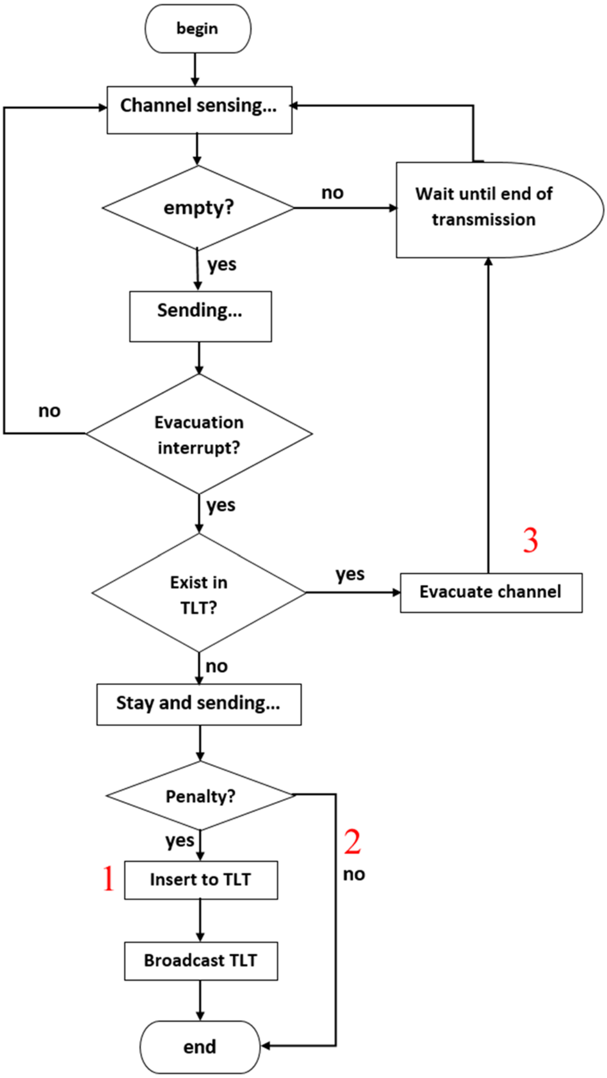
In our method, thee quation (3) is turned into (4):

$$\boldsymbol{E(s) = P\big(T\big(R - c_s\big) + (1 - T)(-C - G)\big) + (1 - P)(G)} \tag{4}$$

The firs reason of these changes, is not to evacuate the channel for PUEA in the case of false alarm. The second one as mentioned before, penalty score is calculated by "-C-G".

The formulated game, is a multistage game that uses previous information (e.g. in stage T the game uses the information of T-1). In the proposed method, whenever the channel evacuation signal is produced, SUs will not evacuate the channel because we don't know that signal is for PU or PUEA. This method will have three outcomes, illustrated in Fig. 3, as follow:

Fig. 3 Flowchart of the Proposed Method



1. The evacuation signal is for a PU. In this case, the SU which does not follow the rule is punished by -C-G scores. After that, the TLT will be created and a unique id of the punisher PU will be placed on top of it. Next time, when evacuation signal is broadcast; first of all, TLT is checked for the id of the producer of node if there is one, the channel will be evacuated and the PU will use the channel. Otherwise this will not evacuate the channel. The TLT will continue broadcasting with every update.
2. The evacuation signal belongs to a PUEA. The channel will never be evacuated for PUEA, and this defines our proposed method with an advantage. Since PUEA is not allowed to emit penalty signals and the channel will not be evacuated, PUEA earns $–C_m$ scores, according to Table 1. So, if PUEA attempts to reach the channel, the SUs prevent that by staying in the channel. That's why the false alarm in proposed method is zero.

3. The evacuation signal is for PU from the second time, onwards. In this case, with checking TLT, the channel is evacuated for PU and the SU, while earning -c_s score.

Whereas, in the learning phase, the existence pattern of PUs was known, the probability of not following this pattern by PU will be weak, unless in the learning phase the pattern is unrecognized or PUs are changing their pattern. So, the probability of, the evacuation signal belongs to a PU, is very weak. That's why, the SUs don't care about evacuation signal. Obviously, if the signal is belonging to a PU, the SU is punished.

The most important aim of the proposed method is to decrease the false alarm and miss detection as possible; because these two parameters is resulted in minus payoff for SUs. In the proposed method, false alarm is zero because the method does not care about the evacuation signal which are sent by PUEA. The value of the miss detection is at most equal to the number of the PUs; because with each miss detection, the ID of the punisher node is storing in TLT. The simulation result is shown in the next section.

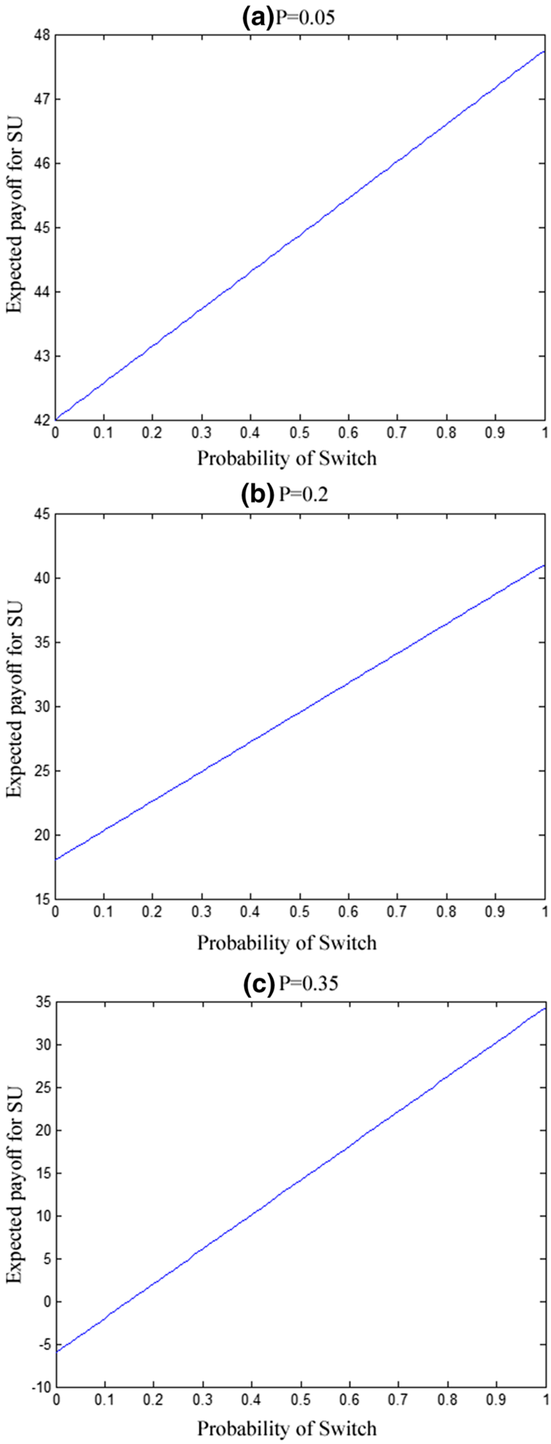
4 Simulation Result

For the time being, MATLAB is using our simulation, and the simulation repeats 1000 times for each stage of the game (20, 40, 60, 80, and 100). The result will be an average of 1000 simulations for every game stage. The simulation was performed on a 500 × 500 square-meter land. That is assumed, the network has noise free and attacker nodes can't punish any node. This assumption that the attacker would not punish the SUs, is acceptable; because there is only one fusion center in whole network that punish SUs and PUEA and the PUEA will not mimic its signal (there is only one fusion center with one unique ID).Each game stage contains clustering and transmitting data that maybe belong for PU or SU or PUEA. The number of SUs is 40 and number of PU and PUEA is 1. Because of satisfying Eqs. (1) and (2), the value for the parameters is: $G=50$, $C=60$, $R=20$, $C'=40$, $c_s=15$, $c_m=25$ and also use three different value for $P=0.05$, 0.2, and 0.35.The punishment of miss detection is -110.

According to the Eq. (4), Fig. 4 illustrates expected payoff results for SU with three different values of P (0.05, 0.2, and 0.35). The Y axis shows earned payoff for SUs, and the X axis shows different switch probabilities for SUs. As it is shown, if switch probability increase, the expected payoff also must increase. Figure 4 is for proving the simulation result that tell us how much the maximum payoff is, and how much simulation result is close to the theoretical number. In Fig. 4a, $P=0.05$, the min payoff for SUs is 42, and the max is 47.75. In part b of the same figure, the min and max payoffs for SUs are 18, 41, respectively, and in last part of Fig. 4, the min and max payoffs are -6, 34 and 25. As seen, how much P increases, domain of expected payoff subsequently increases.

Figure 5 shows, the average per-stage payoff for three different value of p (0.05, 0.2, and 0.35) and for each value of p, the game stages have five different values (20, 40, 60, 80, and 100). In our proposed method, channel evacuation does not happen, we are expecting more benefit than other methods. The simulation result supports this assertion. As it is shown in Fig. 5, how much the game stages increase, simulation result is close to maximum of theoretical result. If SUs switch all the time when a PU exists, we can reach the maximum; But since, we don't care about evacuation signal, the SUs can't reach the absolute maximum. Probability of switch in this figure means, if a PU is in

Fig. 4 Theoretical Result of Expected Payoff for a SU with Three Diffrent Values of *p*



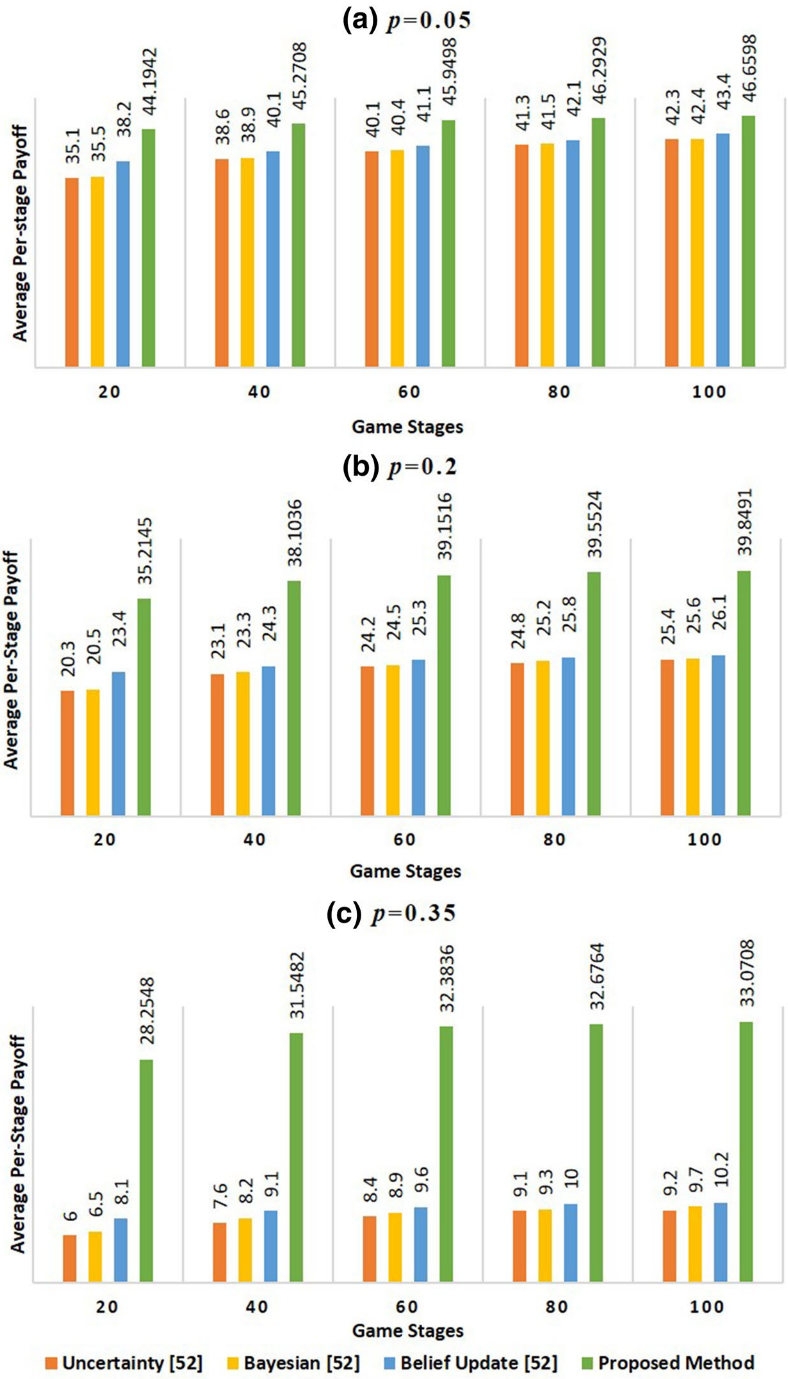


Fig. 5 Average Per-Stage Payoff for Three Diffrent Values of p

the channel and the SUs are switching to another channel, the SUs got specific payoff according to the switch probability. It doesn't mean weather a PU exists or not, the SUs got the same payoff, because of PUEA.

Figure 5a shows the proposed method in the worst case (20 stages game) which earned 6 more points of score payoff in average, and in the best case (100 stages game), SUs give more than 3 scores payoff.

In Fig. 5b, payoff is far more than others. This is because in our proposed method with increasing of the P, the number of miss detections is at most equal to the number of PUs and it is fixed. Same as the previous case, the best and worst cases are 100 and 20 stages respectively. The worst case happened in the 20 stages game, it is because of the ratio of miss detection to the number of stages. With the higher value of p, the probability of miss detection number is increasing and compensation for these miss detections in 20 stages game is so hard. In a 100 stages game, the ratio of miss detection on the number of stages is still a small value, and the chance of compensation is more than 20 stages.

In part c of Fig. 5, like parts a and b, the worst and the best cases are 20 and 100 game stages, respectively. This is the same reason that was discussed before in equation to Fig. 5a, b. The huge difference, in the results of the proposed method against the others, is because of the fact that with increase of p, the probability of miss detection is also increases, and in this case the number of miss detections for the proposed method is one, because there is only one PU in network.

Since there are many nodes in ad-hoc networks, and we have 40 SUs, it is not logical to have only one PU node and one PUEA node in 500×500 square meters. So we take one step forward and repeat simulation with 5 PUs and 5 PUEA, it is totally 10 nodes with PU's behavioral. This is a dense network for cognitive radio, and again with 10 PUs and 10 PUEA, 20 nodes with PU's behavioral which is an ultra-dense network in cognitive radio. As a proof that PUEA aren't affected in the proposed method's results and false alarm is zero, the simulation is repeated with 1 PU and 5 PUEA. As it is shown in Fig. 6, the result is same as the case that 1 PU and 1 PUEA exist in the channel.

The results for dense and ultra-dense networks have been illustrated in Fig. 6. In Fig. 6, the proposed method has been shown in green bars, to provide a comparison with the other method. Dense and ultra-dense networks have been shown in blue and brown, respectively. In dense networks, our proposed method still has phenomenal results against other methods that we have illustrated it in Fig. 5. In Fig. 6a, the ultra-dense network, compared with the other methods, shows a worse operation only in 20 stages of the game. This is because the game stages are very few (20 stages) and the probability of PU's existence is high. On the other hand, the inattention to the evacuation signals from PUs only resulted, at most, in a $10\times(-110)$ penalty score; and the compensation for this penalty with 50 and 5 scores in few game stages is very hard. That is why our proposed method is worse than others, in this case.

In part b of Fig. 6, ultra-dense networks, such as the previous one, have a weak acting in a 20 stage game just in comparison with belief update method. The reason for this was explained in the previous paragraph, but this time the probability of PU's existence is not too high, and the proposed method is better than Bayesian and Uncertainty methods.

In Fig. 6c, where $p=0.05$, the results of ultra-dense network compared with the other methods, are good and higher; there is only one exception in a 100-stage game. The ultra-dense network is a little bit worse than belief update method.

Whereas, 20-stage games are not performing in real world's situations, our proposed method is capable of acting well even in ultra-dense networks. Our proposed method's miss detection is at most equal to the number of PUs; and because of its simplicity and lack

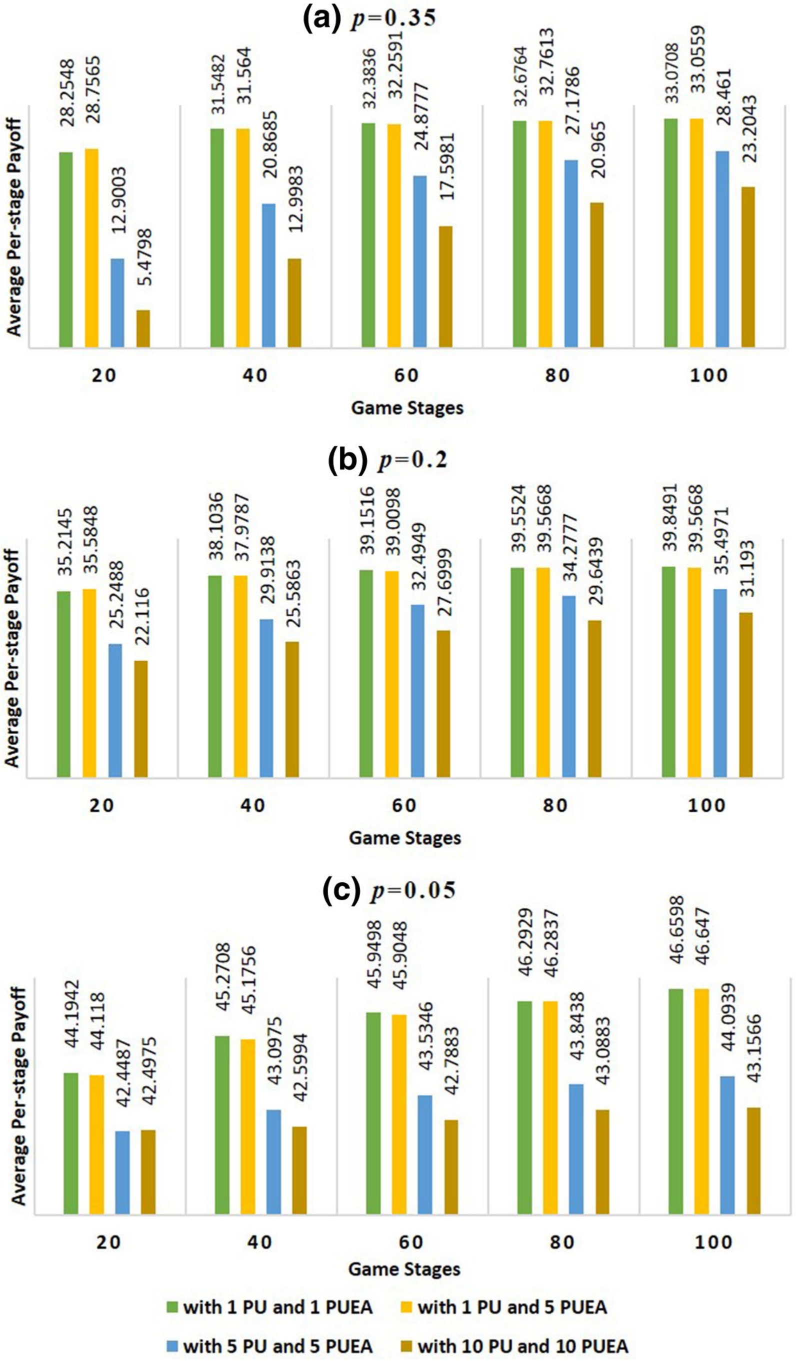


Fig. 6 Average Per-Stage Payoff for Dense and Ultra-Dense Networks with Three Diffrent Values of p

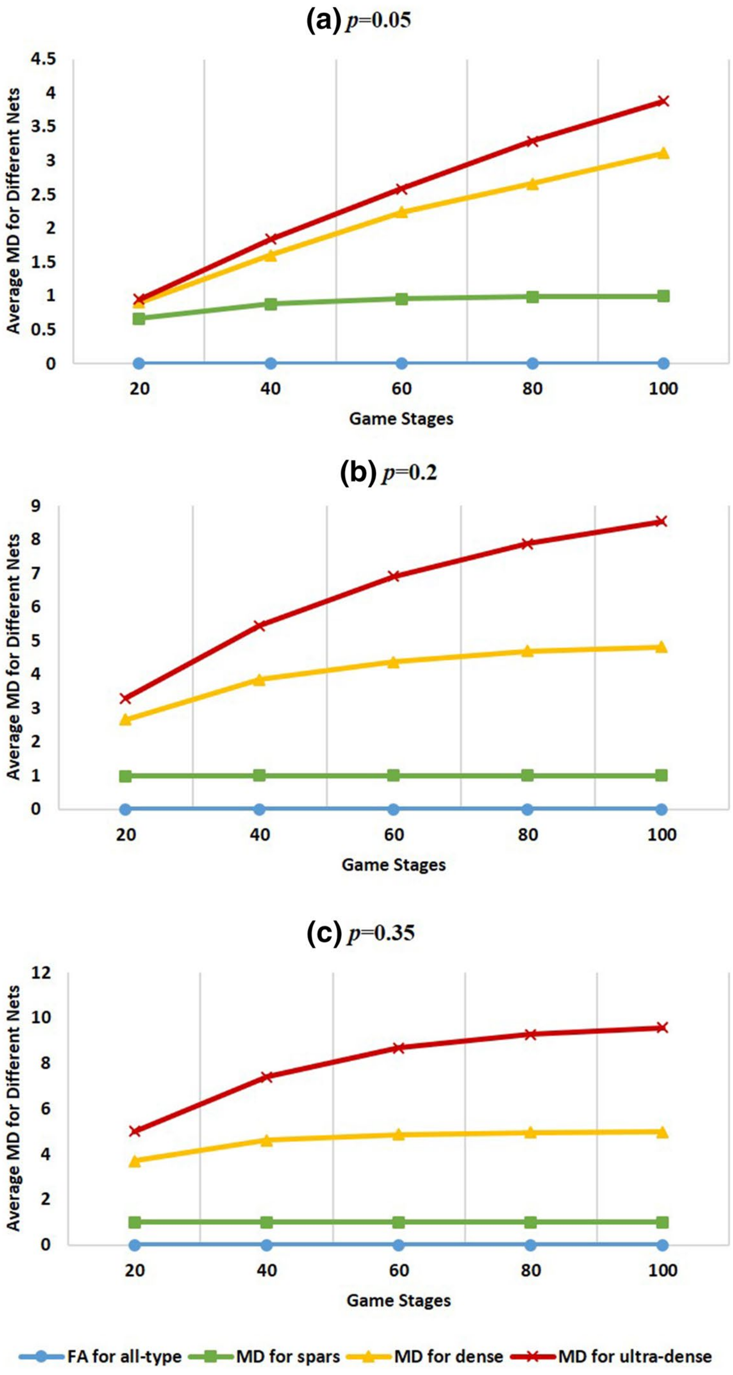


Fig. 7 Average MD and FA in Spars, Dense and Ultra-Dense Networks for Proposed Method

of complex computations, it is proved as very useful for practical usages. In [22], belief update method needs complicated computation and it's hard to find the exact value of α (Fig. 7).

Figure 7 shows the average values for MD and FA parameters in spars, dense and Ultra-dense networks with different probability ($p = 0.05$, 0.2, 0.35) and different game stages (20, 40, 60, 80, 100). The simulation results show the value of FA parameter is zero in all situations, as expected. Moreover, there are three factors which are effecting on MD, including increasing the number of PUs, the value of p and the game stages.

The reason of proposed method's weak operation in 20 game stages for dense and ultra-dense networks is the ratio of MD to the number of game stages. In dense networks and for 20 game stages, there are 16.4% MD happening of total game stages. This percentage for ultra-dense networks is 24.9%. That's why the proposed method has a weaker operation than the other methods in this case.

In Fig. 8, the average percentage of throughput for proposed method are compared with belief update method. When $p = 0.05$, proposed method has a weak acting against belief update method. That's because, in proposed method the probability of MD is 100% even in the case of not attacking. In the belief update method, occurrence of MD is less than the proposed method. In other words, if there is a PU in the network, in the proposed method MD occurs unavoidably but in belief update method MD may not occur.

In the case of $p = 0.2$ and $p = 0.35$, proposed method has a better operation than belief update. Whereas, the probability of p is increased and in this case of network (that there is one PU in the channel) there is only one MD in the network, the proposed method has a better acting than belief update. The reason of throughput decrement by p increment is the overhead of PU detection. PU detecting for the proposed method is TLT checking and for belief update is checking the record of the nodes, and for both methods, if the node is PU then the channel will be evacuated. That's why the increment of p caused decreasing of throughput.

5 Conclusion

In this paper, a method is proposed based on game theory. A competitive non-zero-sum game is designed to detect PUEA in MANETs. Simulation results show, the proposed method has a better operation than the other methods. We repeat the simulation in dense and ultra-dense networks. As it is shown, the proposed method has a better operation even in dense networks. In ultra-dense networks, there are exceptions for better operation than the others in case 20 stages game; however, 20 stages games often don't perform in the real world. In the proposed method, false alarm is zero, that's because we don't evacuate the channel for the attackers and the number of miss detections is at most equal to the number of PUs in the network. The proposed method is very useful for practical usage, because of its simplicity and low memory consumption.

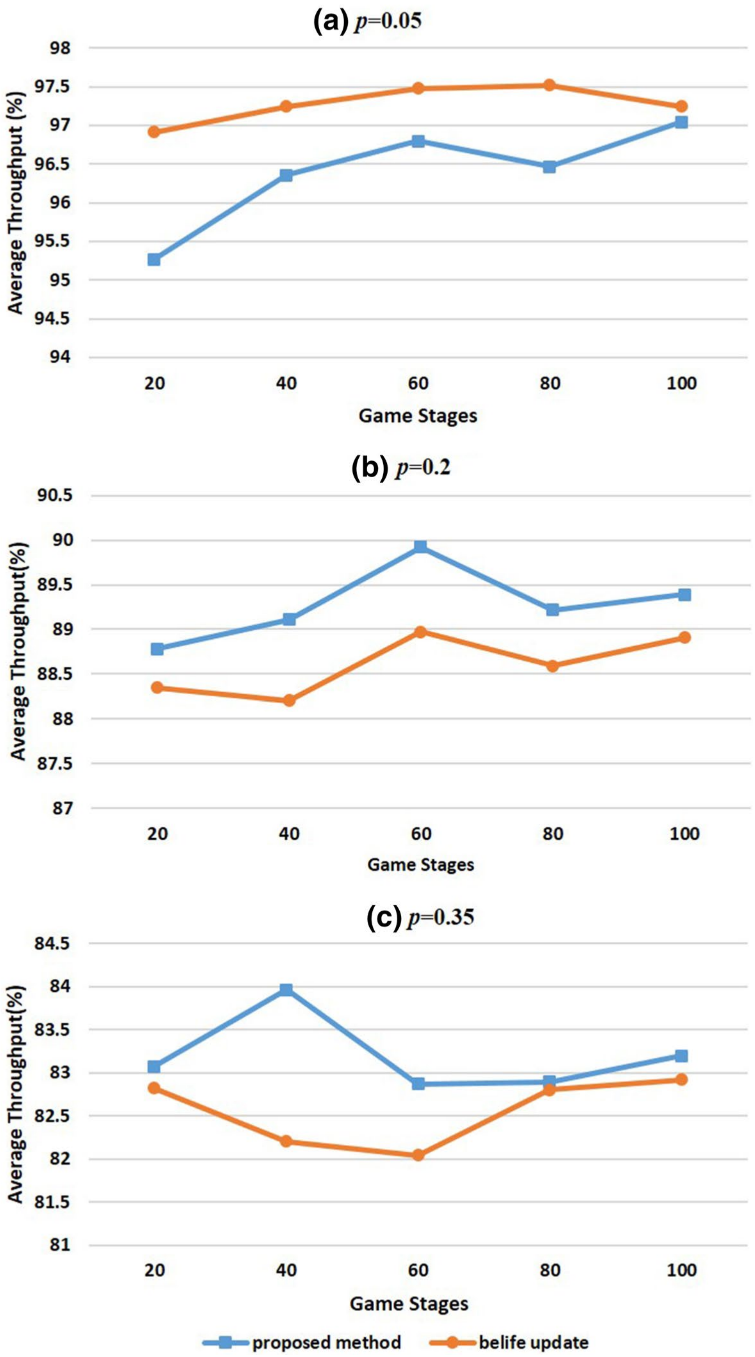


Fig. 8 Average Percentage of Throughput for the Proposed Method and the Belief Update Method

References

1. Ruiliang, C., & Jung-Min, P. (2006). Ensuring trustworthy spectrum sensing in cognitive radio networks. In *1st IEEE workshop on networking technologies for software defined radio networks, 2006. SDR '06* (pp. 110–119).
2. Fragkiadakis, A. G., Tragos, E. Z., & Askoxylakis, I. G. (2013). A survey on security threats and detection techniques in cognitive radio networks. *IEEE Communications Surveys & Tutorials, 15,* 428–445.
3. Ruiliang, C., Jung-Min, P., & Reed, J. H. (2008). Defense against primary user emulation attacks in cognitive radio networks. *IEEE Journal on Selected Areas in Communications, 26,* 25–37.
4. ChunSheng, X., & Song, M. (2014). Detection of PUE attacks in cognitive radio networks based on signal activity pattern. *IEEE Transactions on Mobile Computing, 13,* 1022–1034.
5. Jin, Z., Anand, S., & Subbalakshmi, K. P. (2009). Mitigating primary user emulation attacks in dynamic spectrum access networks using hypothesis testing. *ACM SIGMOBILE Mobile Computing and Communications Review, 13,* 74–85.
6. Zhou, Y., Niyato, D., Husheng, L., Ju Bin, S., & Zhu, H. (2012). Defeating primary user emulation attacks using belief propagation in cognitive radio networks. *IEEE Journal on Selected Areas in Communications, 30,* 1850–1860.
7. Celebi, H., & Arslan, H. (2007). Utilization of location information in cognitive wireless networks. *IEEE Wireless Communications, 14,* 6–13.
8. Niculescu, D. (2004). Positioning in ad hoc sensor networks. *IEEE Network, 18,* 24–29.
9. León, O., Hernández-Serrano, J., & Soriano, M. (2012). Cooperative detection of primary user emulation attacks in CRNs. *Computer Networks, 56,* 3374–3384.
10. Blesa, J., Romero, E., Rozas, A., & Araujo, A. (2013). PUE attack detection in CWSNs using anomaly detecttion techniques. *EURASIP Journal on Wireless Communications and Networking, 2013,* 1–13.
11. Lianfen, H., Liang, X., Han, Y., Wumei, W., & Yan, Y. (2010). Anti-PUE attack based on joint position verification in cognitive radio networks. In *2010 International conference on communications and mobile computing (CMC)* (pp. 169–173).
12. Caidan, Z., Wumei, W., Lianfen, H., & Yan, Y. (2009). Anti-PUE attack base on the transmitter fingerprint identification in cognitive radio. In *5th International conference on wireless communications, networking and mobile computing, 2009. WiCom '09.* (pp. 1–5).
13. Salam, D., Taggu, A., & Marchang, N. (2016). An effective emitter-source localisation-based PUEA detection mechanism in cognitive radio networks. In *2016 International conference on advances in computing, communications and informatics (ICACCI)* (pp. 2557–2561).
14. Borle, K. M., Biao, C., & Wenliang, D. (2013). A physical layer authentication scheme for countering primary user emulation attack. In *2013 IEEE international conference onacoustics, speech and signal processing (ICASSP)* (pp. 2935–2939).
15. Alahmadi, A., Abdelhakim, M., Jian, R., & Tongtong, L. (2014). Defense against primary user emulation attacks in cognitive radio networks using advanced encryption standard. *IEEE Transactions on Information Forensics and Security, 9,* 772–781.
16. Chandrashekar, S., & Lazos, L. (2010). A primary user authentication system for mobile cognitive radio networks. In *2010 3rd international symposium on applied sciences in biomedical and communication technologies (ISABEL)* (pp. 1–5).
17. Ureten, O., & Serinken, N. (2007). Wireless security through RF fingerprinting. *Canadian Journal of Electrical and Computer Engineering, 32,* 27–33.
18. Harini, S. V. V., & Aruna, T. (2016). A mitigation strategy for primary user emulation attacks in cognitive radio networks. In *2016 10th international conference on intelligent systems and control (ISCO)* (pp. 1–5).
19. Nguyen-Thanh, N., Ciblat, P., Pham, A. T., & Nguyen, V. T. (2014). Attack and surveillance strategies for selfish primary user emulator in cognitive radio network. In *2014 IEEE global conference on signal and information processing (GlobalSIP)* (pp. 1199–1203).
20. Ta, D. -T., Nhan, N.-T., Ciblat, P., & Van-Tam, N. (2015). Extra-sensing game for malicious primary user emulator attack in cognitive radio network. In *2015 European conference on networks and communications (EuCNC)* (pp. 306–310).
21. Nhan Nguyen, T., Ciblat, P., Pham, A. T., & Van-Tam, N. (2015). Surveillance strategies against primary user emulation attack in cognitive radio networks. *IEEE Transactions on Wireless Communications, 14,* 4981–4993.
22. Tan, Y., Sengupta, S., & Subbalakshmi, K. P. (2012). Primary user emulation attack in dynamic spectrum access networks: a game-theoretic approach. *IET Communications, 6,* 964–973.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Seyed Abdolazim Vaziri Yazdi received the B.S. from University of Kerman, Kerman, Iran in 2012 in computer hardware engineering and the M.S. in computer architecture from Shahid Bahonar University of Kerman, Kerman, 2017. His research interests are in the area of QOS for wireless networks and digital systems.

Mahdieh Ghazvini received her B.Sc. from Shahid Bahonar University of Kerman, Iran in 2000, and her M.Sc. and Ph.D. from the University of Isfahan, Isfahan, Iran in 2004 and 2013, in Computer Architecture Engineering, respectively. Currently she is assistant professor of Computer Engineering Department at Shahid Bahonar University of Kerman. She is the author of several technical papers in signal processing and telecommunications journals and conferences. Her research interests are wireless networks, game theory, signal processing and neural networks.