Received: 10 June 2016 | Revised: 6 September 2016 | Accepted: 6 October 2016

DOI: 10.1002/dac.3237

WILEY

RESEARCH ARTICLE

Attack modeling and intrusion detection system for 5G wireless communication network

Akhil Gupta[1] | **Rakesh Kumar Jha**[1] | **Sanjeev Jain**[2]

[1] Department of Electronics and Communication Engineering, Shri Mata Vaishno Devi University, Jammu and Kashmir, India

[2] Department of Computer Science and Engineering, Shri Mata Vaishno Devi University, Jammu and Kashmir, India

Correspondence
Akhil Gupta, Research Scholar in Department of Electronics and Communication Engineering, Shri Mata Vaishno Devi University, J&K, India.
Email: akhilgupta112001@gmail.com

Rakesh Kumar Jha, Assistant Professor in Department of Electronics and Communication Engineering, Shri Mata Vaishno Devi University, J&K, India.
Email: jharakesh.45@gmail.com

Summary

Research has been going around the globe to overcome the challenges that are associated with the increase in the number of users, such as interference management, load sharing, and increased capacity. 5G is emerging as a budding prospect for fulfilling demand and overcoming these challenges. For meeting the increased demands, new technologies such as relays in device-to-device communication and small cell access points have been introduced. However, these introductions have opened up security issues in the 5G wireless communication networks. This article focuses on security issues of the 5G wireless communication networks and analyzes the effect of a bandwidth spoofing attack using game theory on the small cell access point in 5G wireless communication network. This article also proposes an adaptive intrusion detection system using a hidden Markov Model for detecting an intrusion on small cell access point in a 5G wireless communication networks.

KEYWORDS

5G, bandwidth spoofing, game theory, hidden Markov model, intrusion detection system

1 | INTRODUCTION

Wireless communication has evolved from analog voice calls to high-quality broadband services with high-speed data. With the rapid increase in the demand of the users in the near future, wireless network has to come up with new technologies. High-speed packet access (HSPA) and long-term evolution (LTE) are the current advancements of wireless-based technologies. With the news of the arrival of 5G, the researchers as well as the users are now thinking of a fully interconnected and mobile society having limitless access to information anywhere and anytime. For realizing this vision, some new emerging technologies such as device-to-device communication (D2D), massive MIMO, moving networks, millimeter wave communication, and ultrareliable networks need to be incorporated in the prevailing wireless technologies such as 3GPP, LTE technology, HSPA, and Wi-Fi. With the introduction of these new technologies, wireless and mobile traffic will increase hundred times in the next few years.[1] However, this advance development has come up with a lot of challenges such as coverage region, security, energy efficiency, spectrum utilization, cost, latency, data rate, and so on.

To overcome these challenges, the performance criteria in terms of throughput, latency, and connectivity density need to be raised while ensuring the security. The main ideology of the security is to protect the identity and privacy of the subscribers while maintaining the confidentiality and integrity of their communication. In recent times, communication networks are becoming the prime objectives of the cyber attacks because of their high vulnerability. With the increased use of communication networks in next generation use cases such as control of critical infrastructures, car traffic control, or remote surgery, there arises a need of a superior degree of network availability. Also in the past, the vulnerabilities in the implementation of mobile network nodes grab the attention from the security researchers or hackers, which correspondingly results in the security breach or attack.[2–5]

In the next generation networks, ie, 5G, the introduction of flat IP architectures and the extensive involvement of cloud in the network processing and communication increase the vulnerability to hackers.[6] Hence, it has become obvious

that in 5G networks, security must be built-in and the security aspects must be accompanied with the architectural design while designing 5G networks.

According to this discussion, it is concluded that there is a lot of scope in developing the security for the 5G. This article is a small step contributing toward the 5G security. The main focus of this article is toward the security of 5G wireless communication network (WCN). For this, we have to take a look toward the 5G cellular network architecture that has been proposed by Gupta and Jha,[1] which is heterogeneous in nature. It includes relays, small cells, microcells and macrocells. These divisions of the architecture help in increasing the coverage region and also mitigate the low signal problem. However, these divisions of the architecture sooner or later act as an active site for the intruders to attack. Relays and small cell access (SCA) points are highly prone to attacks, as they can be easily accessed by any unauthorized user.

1.1 | Contribution

This article focuses on the security analysis of 5G WCN. Possible cases of security breach in the 5G WCN has been analyzed. Overdependence on cloud in the Internet of things will be considered as one of the attack-prone areas that need to be addressed. However, the prime focus of this article is on the 2 security cases in which the security breach will be through relays and SCA. In this article, a mathematical analysis of bandwidth spoofing attack using game theory has been done on SCA in 5G WCN. This article has also proposed an adaptive intrusion detection system (IDS) using the hidden Markov model (HMM) for detecting an intrusion on SCA in 5G WCN.

2 | PROBABLE SECURITY ATTACKS FOR 5G NETWORK ARCHITECTURE

With the evolving technologies, wireless communication has also evolved through generations. Evolution is the need of the hour. With the increasing user demands, wireless communication has to evolve to meet these demands. Our wireless network architecture and equipment are changing to meet the demands of the user. From closed hierarchical networks, we have shifted toward the flat networks, which are more porous and easier to penetrate.[6] Thus, developing technologies paved the way for the wireless network attacks. Now irrespective of using expensive radio access network equipment, we make use of femto cells, small cells, and Wi-Fi hot spots for reaching to the end user with better quality of service.[7] However, these act as an entry point in to the mobile networks, providing an intrusion site for the attacker. Wireless network attacks are classified and explained in detail on the basis of access control, authentication, availability, confidentiality, and integrity.[8] Evolution in the wireless communication industry has also forced the attackers or intruders to evolve for intruding in to the network. Now the intruders are finding new ways to intrude into the evolved wireless network architecture, as given by Paolini.[7] These attacks are active in 4G and are still vulnerable.

A general 5G wireless network under threat is depicted in Figure 1. It is showing that the different base stations (BSs) are connected to the backbone network with the help of an ethernet router, and all the valid clients in a particular cell are reporting to a particular BS inside that cell. The security threat condition has arisen when an intruder client, who is behaving as a valid client tries to capture the BS and intrude in to the network.

Among the attacks given by Paolini,[7] denial-of-service (DoS) attack is the most common and dreadful attack, which aims at exhausting the resources of the target. This attack generally targets the web services and is very common in today's Internet. In the present generation, mobile networks are now becoming an integral part of day today life. However, these networks are the most probable targets for the DoS attacks and mostly carried out by mobiles using a mobile botnet. They are targeting the control plane elements such as mobility management entity in 4G networks.[2] Traynor[9] has shown an attack against the home location register by following the simple means.

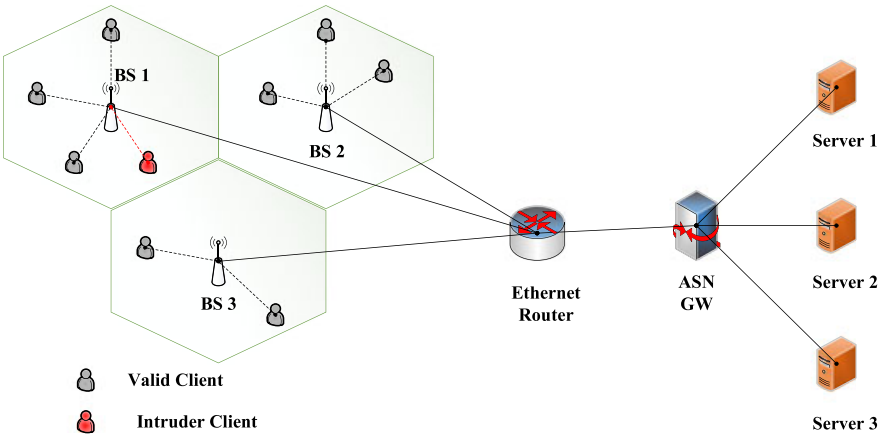

FIGURE 1 A general wireless network scenario under threat

In the near future, the increased use of protocol stacks in the form of an open source software will increase the threat of DoS attack supported by mobile botnets.[2]

There is another type of DoS attack in the form of radio interface jamming. This type of jamming is carried out by transmitting a high power signal to block frequency bands. However, for jamming against 3GPP-specified mobile networks, it has become essential that the control channel should be selectively blocked for the complete operation of the radio interface. However, the more effective and dangerous jamming attack is carried out by a regular mobile in which the attacker can acquire a botnet of mobile devices and can turn them into jamming devices.[2]

The distributed denial-of-service (DDoS) attack is a combination of coordinated attacks from many distributed sources and is difficult to counter. However, there are certain measures that will provisionally provide limited protection. It is done by controlling the rate of incoming traffic from the Internet or by blocking the offending sources. These provisional measures can also be applied in today's 5G mobile networks. There are some more measures that will help in lowering the effect of jamming. One of the measures is to design control plane protocols between mobiles and network in a way so that network side will not require to apply significant effort to detect illegal request. The other measure is to develop an overload protection mechanisms which will make the network functions remain operational even in the presence of any amount of requests. However, for mitigating the effect of smart jamming, it is important that there will be cooperation between radio and security researchers.[2]

In the 5G WCN architecture, the relays and SCAs are introduced to extend the coverage region and mitigate the low signal problem. However, they are now acting as an active site for the attackers or intruders to intrude. Any attacker can eavesdrop between the 2 communicating parties just by behaving as a relay. The Rouge relay can initiate man-in-the-middle attack by intercepting and manipulating the communication between 2 parties. Moreover, the external jammers can interrupt the communication between the relays and the clients by intentionally introducing the noise signals, which initiates the DoS or the DDoS attack. SCAs are also vulnerable to attacks because an external entity can capture the SCA and initiate the man-in-the-middle attack. Recently, bandwidth spoofing attack is proving to be a tough ride for the security developers of present architectures. In this attack, the attacker will spoof the maximum part of the bandwidth by flooding in to a network. In the scenario shown in Figure 2, BS, SCA, and relay are the 3 different entities that are communicating with each other for successful transmission and reception of data to/from the clients. However, the probability of attacks at the relay is highest followed by the SCA and then the BS.

Figure 2 composes of the massive MIMO and small cell scenario in which a fixed number of SCA's are deployed in the fixed range of the BS for offloading the traffic and increasing the capacity. The users that are inside the SCA will report to the SCA and then SCA will correspondingly report to the BS. However, this case has come up with the vulnerability on the SCA because now there is a chance of security breach through the SCA. The intruder or the attacker who

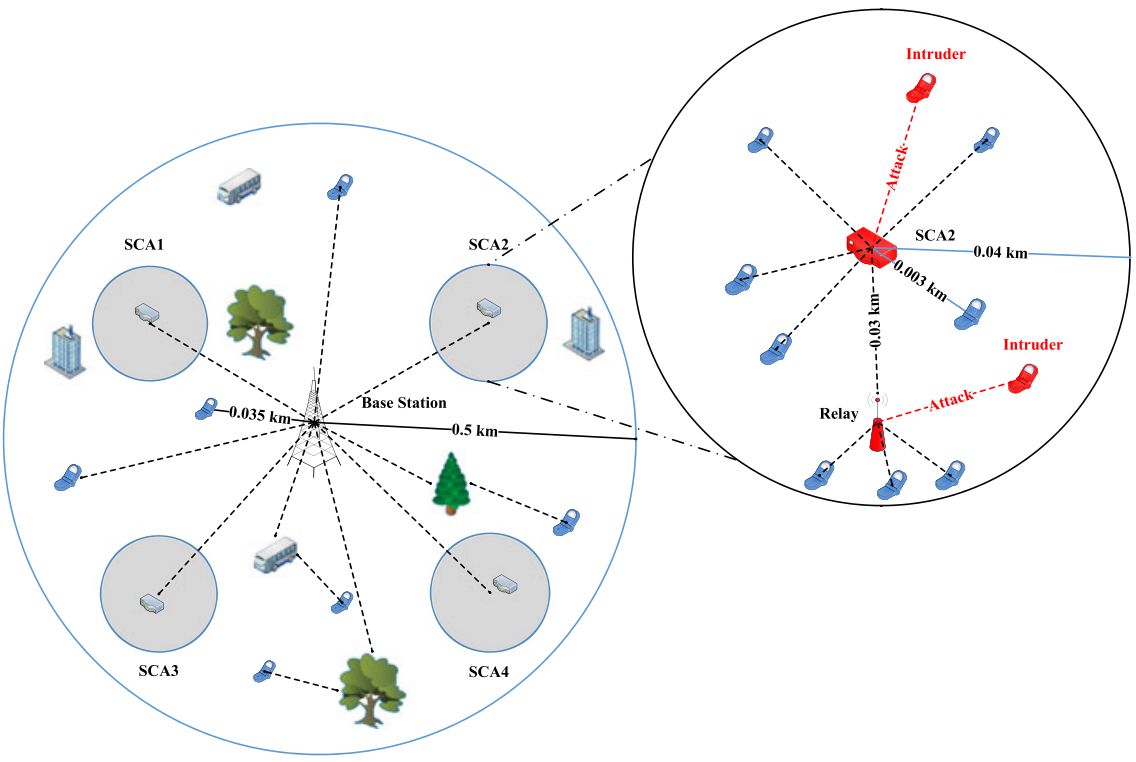

FIGURE 2 Security attack on SCA and relay in the 5G WCN

will enter the network as a client to the SCA can now attack the SCA and acquire the SCA for having control on all the devices that are reporting to the SCA.

The scenario in Figure 2 also composes of a subnetwork in the form of a relay depicting a D2D. In this scenario, the users that are inside the SCA will report to the SCA, and SCA will correspondingly report to the BS. However, the users that are at the edge of the SCA have not been able to report the SCA. These users will now report to the SCA through another device in the form of a relay that receives better signal strength as compared with the user at the edge by using the concept of D2D. However, this case has come up with the vulnerability on the relay because now there arises a chance of security breach through the relay. The intruder or the attacker who will enter the network as a client to the SCA can attack the relay and acquire the relay for having control on all the devices that are communicating through the relay.

These 2 cases of security breach on 5G WCN can be minimized by implementing IDS on the SCA and relay for the respective cases. The implementation of IDS as per the given cases not only enhances the security of the network but also consumes less power and helps in achieving power optimization in 5G WCN.

According to this discussion, it is concluded that DoS attacks are posing major threat to the future 5G networks. Mitigating the threat will be one of the prime research areas during the next few years. The next section composes of a mathematical analysis of bandwidth spoofing attack (a kind of DOS attack) using game theory on SCA in 5G WCN.

3 | BANDWIDTH SPOOFING ATTACK IN 5G WCN

In the previous section, it is clear that DoS attacks are posing major threat to the 5G WCN. This section introduces game theory formation for bandwidth attack,[10,11] which is one of the types of DoS attack in 5G WCNs. In this attack, the attacker has the knowledge about the traffic pattern of the network, ie, the downlink/uplink (DL/UL) mapping of SCA with BS. The entire process of communication between BS and SCA is in 3 phase. In the first phase, BS perform the operation of ranging. In the second phase, once the ranging has been done, the SCA are able to send request to server from BS (UL). In the third phase, server respond the particular application from BS (DL) to SCAs. For this process, bandwidth is needed, so BS will now assign bandwidth to all the SCAs.

In the third phase of assigning the bandwidth, the attacker has the chance to acquire the bandwidth that is going to be assigned to the SCA. In this section, the bandwidth attack by attacker which is an unauthorized client on SCA or defender using game theory is examined. This section helps in analyzing the way in which the attacker client wins the game by spoofing the bandwidth. This section also helps in analyzing the way in which SCA will protect the bandwidth by using Nash equilibrium.

3.1 | Game theory

The game theory deals with the situation where there are at least 2 entities interacting according to the rules of the game. In this theory, game is open, when each client has finite number of moves available but ends, when it has finite numbers of moves.[12] In this article, game theory is applied for analyzing the way in which the attacker client or intruder wins the game by spoofing the bandwidth. Two interacting entities of this article are SCA and attacker client, represented as A and B, respectively. They are playing the game for acquiring the bandwidth.

In this article, game theory is applied with linear programming in all the areas, and the expected result in terms of mathematics is as follows:

{For a zero sum game, one will gain (A) then other will lose (B)}.

3.1.1 | Illustration

Client A and B are playing a game with coin and both have decided that if both the faces are same, ie, (H, H) and (T, T) then B will pay, ie, A will win the game, and if both the faces of the coin are opposite, B will win and A will pay; remember toss is always unbiased:

$$\text{Payoff}A = \begin{matrix} \\ H \\ T \end{matrix} \begin{matrix} \begin{matrix} H & T \end{matrix} \\ \begin{bmatrix} +1 & -1 \\ -1 & +1 \end{bmatrix} \end{matrix}.$$

Here H is head and T is tail. Because this matrix is the payoff matrix A, so payoff matrix B can easily be deducted from the above matrix.

However, while applying game theory, we came across 2 types of clients, ie, intelligent and rational. The intelligent clients mean that they are able to take fruitful decision on the basis of their experience and think logically. Rational means that preferences are consistent with final outcomes of the decision-making process and are intended to maximize these preferences. The maximization is carried out by trying to achieve a certain gain, which is expressed through utility function. Hence, both A and B being the intelligent client, B realizes after some time that A is playing the game and showing H continuously, so he adapts and show T. With the game progresses, both A and B will act as an intelligent clients in a manner that A will maximize the gain and B will minimize the loss. Thus, now the matrix will be

$$\begin{matrix} \text{Min Max loss for B} \\ \text{Max Min gain} \quad \text{of A} \end{matrix} \begin{bmatrix} +1 & -1 \\ -1 & +1 \end{bmatrix}$$

Here, A wants to maximize the minimum gain and B wants to minimize the maximum loss. Hence, game is therefore the steps between multiple entities.

3.2 | Nash equilibrium

The games in the game theory are initially classified as cooperative and noncooperative games. Cooperative games study the formation of coalitions with binding agreements that may be of benefit to the individual components. Noncooperative games are concerned with the mechanism of individual decisions, based on individual reasoning, in the absence of mandatory alliances. The formal discretion of a noncooperative game takes 2 forms and is classified as extended form and strategic form. In the extended form, the description of game is made with a tree structure. In the strategic form, the number of clients, the space of strategies, and the utility function of each client is specified.

In this article, the strategic form of noncooperative game is considered, and Nash equilibrium is a solution concept of a noncooperative game in the game theory. It involves 2 or more players, in which each player is assumed to know the equilibrium strategies of the other players, and no player has anything to gain by changing only their own strategy. To explain the Nash equilibrium, several definitions related to the Nash equilibrium seeking problem for noncooperative games are provided as follows[13]:

Definition 1. *The game to be considered is defined as*

$$\Gamma \triangleq \left\{ \mathbb{N}, (u_i)_{i\in\mathbb{N}}, (Q_i)_{i\in\mathbb{N}} \right\}$$

where $\mathbb{N}$ is the set of N players, $u_i(t)$ is the strategy for player I, $U \subset R^{\mathbb{N}} = \{u_i \mid i\in\mathbb{N}\}$ denotes the strategy space, and Q_i is the payoff function for player i. $Q_i \triangleq Q_i(u_i(t), u_{-i}(t), \varsigma_i(t))$, where $\varsigma_i(t)$ is a time-varying unknown vector and $u_{-i}(t)$ denotes the strategy for all the players other than player i.

Definition 2. *The strategy vector of the game defined in Definition 1 is said to be at the Nash equilibrium if any unilateral change of a player's strategy does not increase its payoff value in the sense that*

$$Q_i\left(u_i^*(t), u_{-i}^*(t), \varsigma_i(t)\right), \forall i\in\mathbb{N}.$$

The strategic game is a model involving interacting decision makers referred to as clients. It consists of following parameters:

a) A set of clients
b) A set of strategies for each client
c) Preferences over the set of strategic profiles for each client

Each client has a choice of strategies among pure strategies and mixed strategies. A pure strategy is one in which clients deterministically choose their moves, whereas a mixed strategy is one where clients randomly choose one out of many different strategies. For example, clients can choose a probability distribution over the set of possible strategies and randomly pick one before playing the game. However, the best strategy for a client in a game may be a mixed one. In some games, however, it is possible for a pure strategy to be optimal. In this article, the mixed strategy with iterated prisoner's dilemma has been applied by both the clients for bandwidth spoofing. It is because of the fact that 1 client is a defender and other is an attacker, and no one will want to share and loose the bandwidth in any situation.

The prisoner's dilemma is a standard example of a game analyzed in game theory that shows why 2 completely rational individuals might not cooperate, even if it appears that it is in their best interests to do so. An extended iterated version of the game also exists, where the classic game is played repeatedly between the same prisoners, and consequently, both prisoners continuously have an opportunity to penalize the other for previous decisions. If the number of times the game will be played is known to the players, then (by backward induction) 2 classically rational players will betray each other repeatedly, for the same reasons as the single shot variant. In an infinite or unknown length game, there is no fixed optimum strategy, and prisoner's dilemma tournaments have been held to compete and test algorithms. The prisoner's dilemma game can be used as a model for many real world situations involving cooperative behavior.

There are 4 different conditions, represented as below cases, which has been used in this article.

Case 1. *Clients A and B are consoling to be the valid user for BS. There are a lot of parameters that are same among both the clients, for being a valid user, but do not have enough evidences to convict either of the valid client unless any one of them produces a better response in terms of validation.*

Case 2. *If both acts as valid clients in terms of authentication, authorization, and accounting (AAA), then both have the chance to be assigned with the bandwidth, but the possibility for this condition is very minimum.*

Case 3. *Client A is an intelligent client because of the highly secured link between the BS and client. Hence, it will play a game or strategy such that client B will not be able to beat and loose in every condition.*

Case 4. *However, after some time, client B has also become intelligent and recognize the client A's strategy. Now once the client B finds the loophole in the security between BS and client A link, client B will spoof the bandwidth at the cost of client A.*

These 4 cases are summarized in the following way. Two clients (attacker and defender) are showing 1-by-1 validation to BS, whether they are authorized or nonauthorized client. If

attacker been able to show the authorization in all existing ways, then defender will lose the assigned bandwidth. However, if attacker is not been able to verify it in the second step, then it will lose the assigned bandwidth to the valid user or defender.

3.2.1 | Implementation of bandwidth attack based on Game theory on SCA in 5G WCN

The 5G WCN scenario for bandwidth attack on SCA is shown in Figure 2 of Section 2.

The flowcharts given in Figures 3, 4, and 5 will explain how the bandwidth attack is performed on the SCA using game theory in 5G WCN. The steps that have been used for implementing the bandwidth attack on the SCA using game theory in 5G WCN have been thoroughly explained and represented in the form of flowcharts. Figure 3 represents the flowchart for bandwidth accessibility between valid and invalid users.

Figures 4 and 5 represent the set of strategy for player A and player B using iterated prisoner's dilemma.

The implementation is started by initializing both the players, ie, A and B, seeking for same bandwidth and then

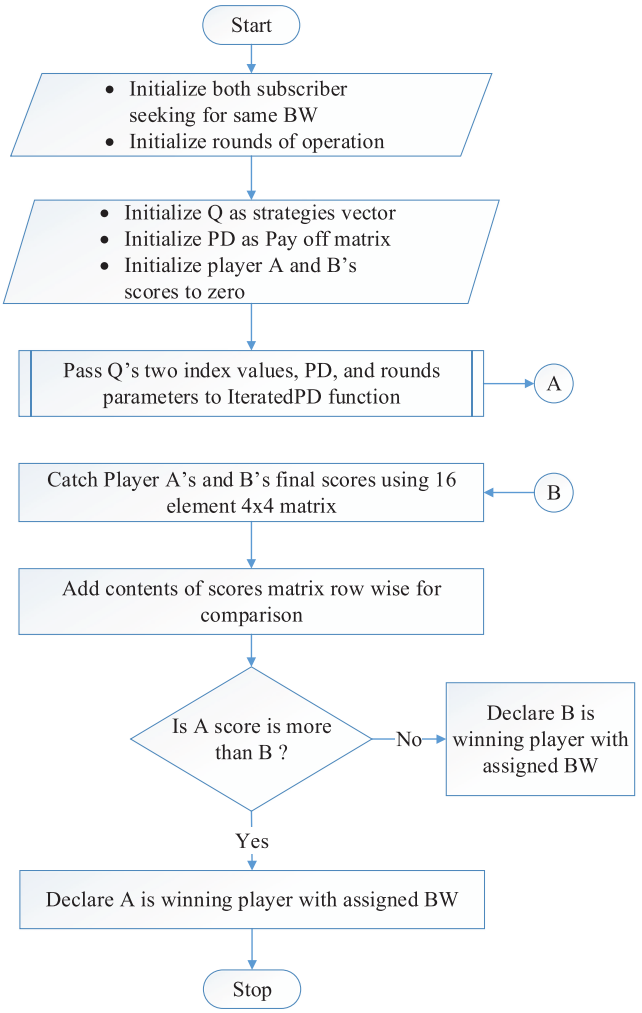

FIGURE 3 Flowchart for bandwidth accessibility between valid and invalid users using game theory

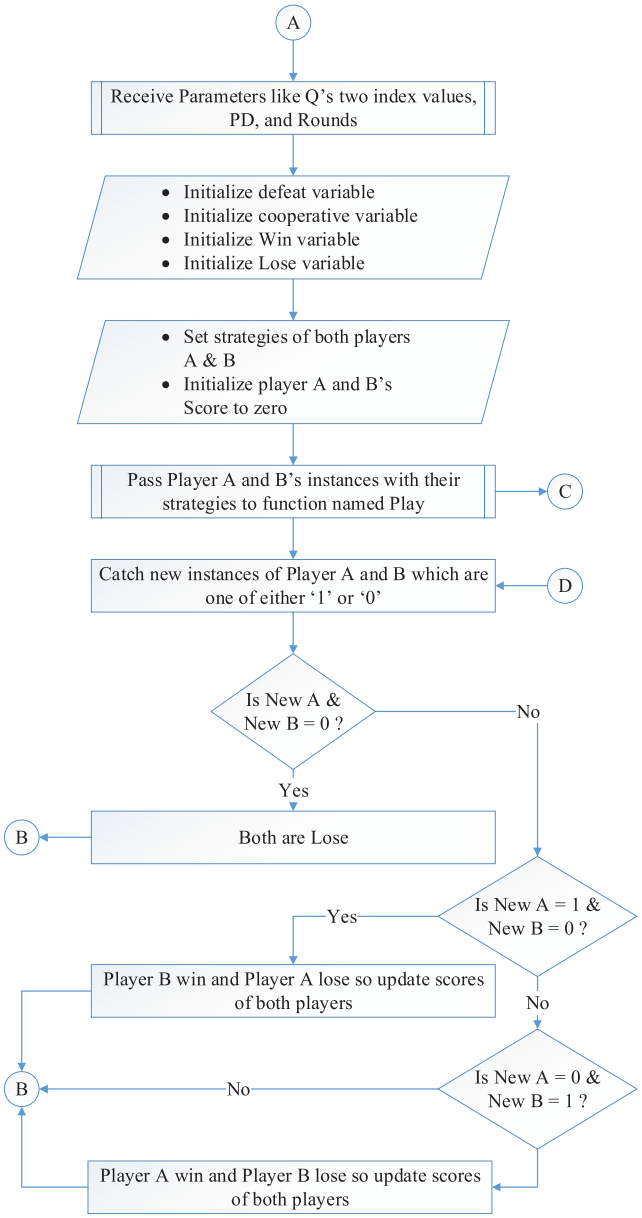

FIGURE 4 Set of strategy for players A and B using iterated prisoner's dilemma (PD) for bandwidth spoofing

by initializing the rounds of operation. Designate Q as strategies vector and PD as payoff matrix. Now initialize Q and PD to their respective designation and initialize scores of player's A and B to zero. Then for the strategic form of noncooperative game, a mixed strategy with iterated prisoner's dilemma has been applied by both the clients for bandwidth spoofing. After initialization, the values of the parameters such as Q's 2 index values, which represents the different strategies in the form of indexes, PD, and rounds, are passed to the iterated prisoner's dilemma function shown in Figure 4.

In this function, first the defeat, cooperative, win and lose variables are initialized, which are representing the outcomes after applying the mixed strategy. Then the strategies for both the players A and B are set with certain instances and pass them to the function named *play*, as shown in Figure 5. In this function, depending on the strategies, new instances in the

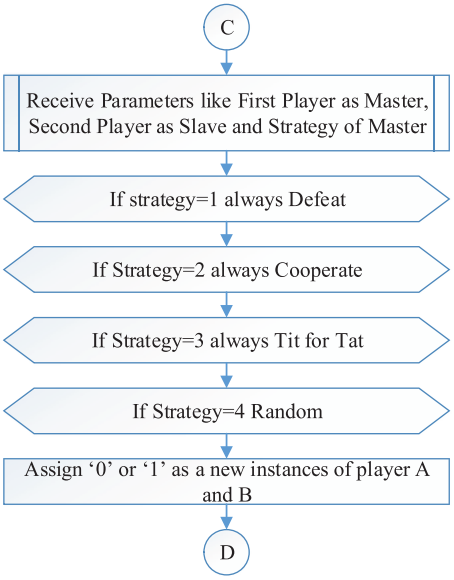

FIGURE 5 Flowchart of a function representing set of strategies

form of "1" and "0" are assigned to players A and B, which represents the attack and nonattacked conditions, respectively. Now depending on the instances, the winning and losing of the players is decided for each round. Now the final scores of all the rounds of both the players are taken in 16 element 4 × 4 matrix and then compared. Depending on the number of winning rounds based on the average score, the winner will be decided and bandwidth will be assigned to that player.

The steps that have been explained in the previously mentioned flowcharts are simulated for 8 iterations of 4 rounds.

3.2.2 | Simulation results

While following the steps shown in the flowcharts, simulation has been performed and results have been taken. The simulation has been done for 8 iterations of 4 rounds each. The results of the simulation performed using game theory for the bandwidth spoofing attack are shown in Table 1. Here player A is the genuine client and player B is the attacker. The simulation has been performed in 4 rounds, and the average score of each player coming after following the steps shown in the flowchart is recorded.

Now the average score of each player is compared with its counterpart, and the player who wins more number of rounds will be able to acquire the bandwidth. For the case of 8 iterations as in Table 1, it is clear that player A wins in the first 4 iteration with a fixed strategy. However, in the fifth iteration, player B understands the strategy of player A and changes its strategy accordingly, which results in the win for player B. Now the bandwidth is with player B. Thus, for the next 3 iterations, the bandwidth is with player B. However, when we run the simulation for different number of iterations, still the bandwidth acquiring percentage of the attacker is

TABLE 1 Results of the game theory for bandwidth spoofing attack

	Round 1	Round 2	Round 3	Round 4	No. winning round	Result
Iterations 1						
Player A average score	106	109	81	63	2	Player A wins with an average score of 20
Player B average score	106	81	69	83	1	
Iterations 2						
Player A average score	98	111	74	73	1	Player A wins with an average score of 16
Player B average score	98	75	74	93	1	
Iterations 3						
Player A average score	94	112	77	100	3	Player A wins with an average score of 84
Player B average score	94	80	65	60	1	
Iterations 4						
Player A average score	104	114	66	68	1	Player A wins with an average score of −8
Player B average score	104	74	90	92	2	
Iterations 5						
Player A average score	94	112	60	79	1	Player B wins with an average score of −4
Player B average score	102	80	76	83	3	
Iterations 6						
Player A average score	94	101	64	77	1	Player B wins with an average score of 0
Player B average score	102	81	72	81	3	
Iterations 7						
Player A average score	102	108	62	76	1	Player B wins with an average score of 16
Player B average score	110	76	94	84	3	
Iterations 8						
Player A average score	107	111	58	76	1	Player B wins with an average score of 24
Player B average score	111	75	90	100	3	

significant enough for the bandwidth spoofing attack to make an impact.

The simulation for different iterations was carried out, and the winning percentage of the attacker has come out as shown in Figure 6.

3.3 | Analysis

From the previously mentioned results, it is concluded that game theory proves to be a useful method in examining the bandwidth attack, as attacker is able to spoof the bandwidth from defender with prisoner's dilemma game theory with a significant winning percentage of the attacker. Hence, it has become a challenge for the security of 5G WCN, where resources are allocated based on IP. It is also concluded that the bandwidth spoofing attack is more harmful if the attacker targets only 1 client because if he will play with more number of valid clients, then the probability of wining will be very low and complexity will also increase. These results are based on an assumption that the channel condition should be good; otherwise, the prediction of payoff matrix will change, and it will become very difficult to acquire the bandwidth from defender clients. This section has shown the bandwidth attack based on game theory on the SCA for 5G WCN. The next section will help in detecting the intruder that has tried to attack the SCA for acquiring the bandwidth.

4 | ADAPTIVE IDS USING HMM FOR 5G WCN

Previous section has concluded that, Game theory proves to be a useful method in examining the bandwidth attack, as attacker is able to spoof the bandwidth from defender with prisoner's dilemma game theory with a significant winning percentage. Hence, the need to secure the 5G WCN has now become the prime concern. The most common method that came forward for detecting an intruder will be IDS. Earlier, for maintaining the security of the network, an IDS runs at each BS. Each incoming request is submitted to the IDS for verification. It receives the client details in terms of MAC ID and BS ID to verify whether the request is genuine or not. However, the types of services that are offered in that request are not known to the IDS. It tries to find out any anomaly in the request based on the spending profile of the requester. If the IDS confirms the request to be malicious, it raises an alarm, and the BS declines the request. The concerned client may then be contacted and alerted about the possibility that the security of BS is compromised.

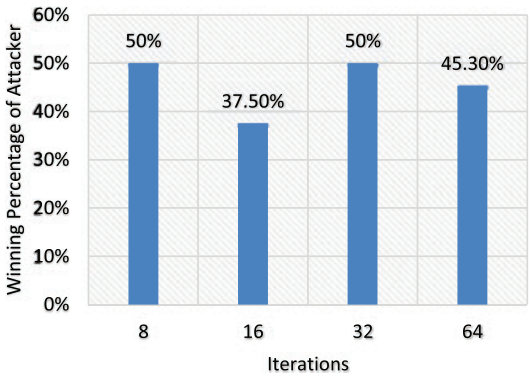

FIGURE 6 Winning percentage of attacker for different iterations

With the arrival of new types of attacks and new sites to be attacked, the typical IDS needs some additional features for better intrusion detection. Hence, HMM is introduced with the IDS to form an adaptive IDS, which can be used for the detection of an intruder. However, for 5G WCN, an IDS will run at the sites that are going to be attacked, ie, either at SCA or at relay.

An HMM is capable of modeling more complicated stochastic processes than a traditional Markov model because it is a double embedded stochastic process, which is having 2 hierarchy levels. An HMM has a limited set of states administered by a set of transition probabilities. An observation can be generated conferring to an associated probability distribution for a specific state. It is only the observation and not the state that is evident to a peripheral observer.[14]

In the previous years, HMM is used in various types of application such as speech recognition, bioinformatics, and genomics. However, in the present generation, the researchers are using HMM in the security perspective. Joshi and Phoha[15] have investigated the proficiencies of HMM for anomaly detection by classifying the TCP network traffic in the form of an attack or normal using HMM. Ourston et al[16] have proposed the application of HMM in detecting multistage network attacks. Cho and Park[17] have suggested an IDS based on HMM, which considered the privilege transition flows centered on the domain knowledge of attacks for improving the performance and modeling time. A new method by Hoang et al[18] uses HMM for process sequences of system calls for anomaly detection by building a multilayer model of program behaviors based on both HMM and different methods for anomaly detection. HMM model is also used for modeling the human behavior, as given by Lane.[19] Hence, any detected deviation due to an attacker that is not having a behavior similar to the genuine user raises an alarm. An HMM is generally described as follows[14]:

1) The number of states in the model are denoted by N. The set of states are denoted as $S = \{S_1, S_2, \ldots \ldots S_N\}$, where $S_i, i = 1, 2, \ldots N$, is an individual state and q_t is the state at time instant t.
2) The number of distinct observation symbols that correspond to the physical output of the system per state are denoted by M. The corresponding set of symbols will be $V = \{V_1, V_2, \ldots V_M\}$, where $V_i, i = 1, 2, \ldots M$, is an individual symbol.

3) The state transition probability matrix is denoted as

$$A = [a_{ij}],$$

where

$$a_{ij} = P(q_{t+1} = S_j), 1 \le i \le N, 1 \le j \le N; t = 1, 2.. \quad (1)$$

4) However, for the general case, where any state j can be reached from any other state i in a single step, we have $a_{ij} \ge 0\ \forall i, j$. Also $\sum_{j=1}^{N} a_{ij} = 1, 1 \le i \le N$.
5) The observation symbol probability matrix is denoted as $B = [b_j(k)]$, where

$$b_j(k) = P(V_k | S_j), 1 \le j \le N, 1 \le k \le M,$$

and

$$\sum_{k=1}^{N} b_j(k) = 1, \quad 1 \le j \le N. \quad (2)$$

6) The initial state probability vector is denoted as

$$\pi = [\pi_i]$$

where

$$\pi_i = P(q_1 = S_i), 1 \le i \le N, \text{such that} \sum_{i=1}^{N} \pi_i = 1. \quad (3)$$

7) The observation sequence is represented as

$$O = O_1, O_2, O_3, \ldots O_R,$$

where each observation O_t is one of the symbols from V, and R is the number of observations in the sequence.

It is clear from this discussion that a comprehensive description of an HMM is not complete without estimating the 2 model parameters, N and M, and 3 probability distributions, A, B, and π. These notations are used as $\lambda = (A, B, \pi)$ to specify the complete set of parameters of the model. The N and M are indirectly included in A and B. The above-mentioned observation sequence O can be generated by many possible state sequences, and one of them will be as follows:

$$Q = q_1, q_2, \ldots . q_R, \quad (4)$$

where q_1 is the initial state.

The probability that the observation sequence O is generated from the given state sequence while assuming statistical independence of observations is specified as

$$P(O|Q, \lambda) = \prod_{t=1}^{R} P(O_t | q_t, \lambda). \quad (5)$$

This equation can be expanded as

$$P(O|Q, \lambda) = b_{q1}(O_1), b_{q2}(O_2), \ldots . b_{qR}(O_R). \quad (6)$$

The probability of the state sequence Q is specified as

$$P(Q|\lambda) = \pi_{q_1} a_{q_1 q_2}, a_{q_2 q_3}, \ldots . a_{q_{R-1} q_R}. \quad (7)$$

Therefore, the probability of generation of the observation sequence O by the HMM indicated by λ can be transcribed as

$$P(Q|\lambda) = \sum_{\text{all } Q} P(O|Q, \lambda) P(Q | \lambda). \quad (8)$$

$P(Q|\lambda)$ can be computed by using forward-backward procedure as given by Rabiner.[14] This article has considered threshold level sequence T_R in place of O_R sequence.

4.1 | HMM model for IDS processing

There are 6 steps for mapping the IDS processing operation using HMM:

1) *Deciding observation symbols*

In this model, the first step is to decide the observation symbols. These can be formed at the BS by quantizing the number of request values into M service ranges as $V_1, V_2, \ldots V_M$. The spending habit of each client will decide the actual service range for each symbol. A specific clustering algorithm technique can be applied for dynamically determining the service ranges, depending on the values of each client's service request. In this article, we are using V_k to characterize both the observation symbol, as well as the corresponding service range, where k = 1, 2….M.

2) *Deciding the state representation and determining the transition probabilities*

After deciding the number of observation symbols, there is a need to consider the number of states. In our approach, the 3 states will be BS, SCA, and intruder. These are represented as

S = (BS, SCA, and intruder).

The next step to complete the HMM representation after determining the state and symbol representations is to determine the probability matrices A, B, and BS. The Baum-Welch algorithm[15] is used in the training phase for determining these 3 model parameters.

Figure 7 depicts the special case of fully connected HMM in which every state of the model can be reached in a single step from every other state with a transition probabilities as shown in Table 2. Here each client will be trained and maintained by HMM.

3) *Dynamic generation of observation symbols*

Similar to the client, BS's will also be trained and maintained by HMM. Hence, for finding the observation

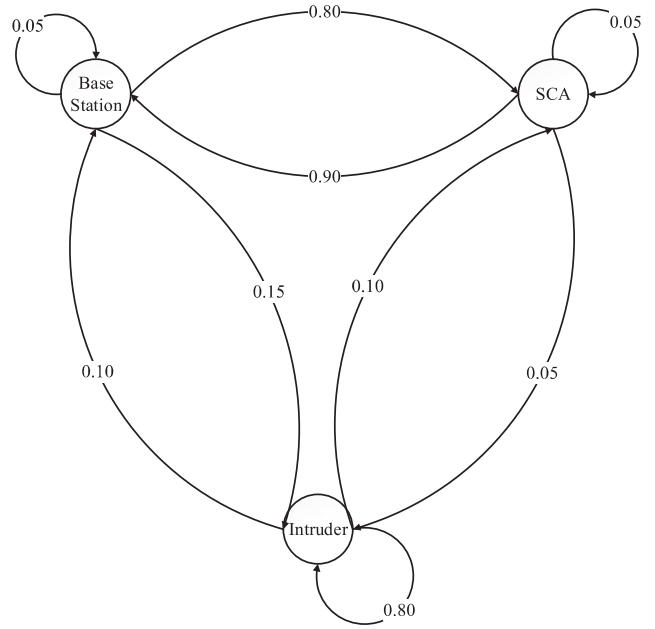

FIGURE 7 HMM for intruder detection with transition probabilities according to Table 2

TABLE 2 Proposed HMM for intruder detection with transition probabilities

	Response		
Demand	**Base station**	**SCA (A)**	**Intruder (B)**
Base station	0.05	0.80	0.15
SCA (A)	0.90	0.05	0.05
Intruder (B)	0.10	0.10	0.80

symbols corresponding to individual clients, a dynamic request is sent and on the basis of the past request, clustering algorithm is compiled and executed. Generally, the BS database contains requests of many attributes. However, this article has considered only those attributes that the client has spent in his request. To achieve this, K-means clustering algorithm[20] is used to determine the clusters. K-means is an unsubstantiated learning algorithm that will group a specified set of data built on the resemblance in their feature values and named it as cluster. The K clusters are fixed a priori. The clusters are formed by minimizing the sum of squares of distances between each data point and the centroid of the cluster to which it belongs.

4) *Spending profile of clients*

Normal spending behavior represents the spending profile of a client. Centered on the spending habits, the clients are characterized into 3 groups explicitly, high spending group, medium spending group, and low spending group. Video on demand is the normal used service for the clients of high spending group. The other 2 groups follow the related classification. At the end of the clustering step, the spending profiles of clients are determined. Let the percentage of total number of request of the clients that belong to cluster with mean c_i be π. Then the spending profile (SP) of the client u is determined as

$$\mathrm{SP}(u) = \arg\max_i (\pi). \tag{9}$$

5) *Model parameter estimation and training*

To estimate the HMM parameters for each client, the Baum-Welch algorithm is used in which the initial estimates of HMM parameters such as A, B, and π converges to the nearest local maximum of the likelihood function. The initial state probability distribution of N states is considered to be uniform, so the initial probability of each state will now be $^1/_N$. The initial guess of observation symbol probabilities are uniform, but still for more accurate initial guess of observation symbol probabilities, spending profile is considered which is calculated in the previous step. This will lead to accurate learning of the model. The initial guesses were considered to be uniform in the training of HMM because there is no a priori knowledge about the state transition probabilities. The training algorithm has the following steps:

a) *Initialization of HMM parameters*
b) *Forward procedure*
c) *Backward procedure*

The details about the training steps are available in the training of HMM.[14] At the end of the training phase of HMM, the corresponding sequences of each client that were formed from the observation symbols are derived. This step does not affect the performance of the processing clients because it is performed offline.

6) *Intruder detection*

After the learning from the HMM parameters, an initial sequence of symbols is formed from the symbols of a client's training data. Let $T_1, T_2 \ldots . . T_R$ be some sequence of length R. This recorded sequence is made from the clients request up to time t. Now the probability of acceptance is computed by inputting this sequence to the HMM. Let the probability be α_1, which can be inscribed as

$$\alpha_1 = P\left(T_1, T_2, T_3 \ldots . . T_R \mid \lambda\right). \tag{10}$$

Let T_{R+1} be the symbol generated by a new symbol at time t + 1. To form another sequence of length R, drop T_1 and append T_{R+1} in that sequence, generating T_2, $T_3 \ldots . . T_R, T_{R+1}$ as the new sequence. Then input this new sequence to the HMM and the probability of

acceptance is calculated. Let the new probability be α_2, which can be inscribed as

$$\alpha_2 = P\left(T_2, T_3, T_4 \ldots ..T_{R+1} \mid \lambda\right). \tag{11}$$

$$\text{Let } \Delta\alpha = \alpha_1 - \alpha_2. \tag{12}$$

If $\Delta\alpha \geq 0$, then it is clear that the new sequence is accepted by the HMM with low probability, and it could possibly be an intruder. The newly added symbol is determined to be fake if the percentage change in the probability is above a threshold (Th), ie,

$$\Delta\alpha \Big/ \alpha_1 \geq \text{Threshold}. \tag{13}$$

The threshold value can be learned empirically. If T_{R+1} is malicious, then the BS does not accept the request, and the IDS rejects the symbol. Otherwise, T_{R+1} is added in the sequence permanently, and then the new sequence will now be used as the base sequence for defining the validity of the next request. The main reason behind including the new number of malicious symbols in to the sequence is to apprehend the changing spending behavior of the clients. The complete process flow of the proposed model of IDS is shown in Figure 8, whereas Figure 9 shows the process flow of training data set for IDS. The training phase is performed offline, whereas detection is an online process.

The above-proposed model of IDS using HMM will help in detecting the intruder in the 5G WCN scenario, as shown in Figure 2 of Section 2. The process of intrusion detection will take place in 2 steps. The flowchart in Figure 10 shows the process of training data set for IDS in the first step, whereas the flowchart shown in Figure 11 shows the process of Intrusion Detection using proposed model in the second step.

In the first step, first the total number of users and active users in each iteration is initialized. In our work, we have consider the total number of users to be 10, whereas the active number of users will be random in every iteration. The next step involves the generation of priority, transmitted probability and obstruction probability matrix. After that, the intruder will try to intrude in to the network. If the intruder

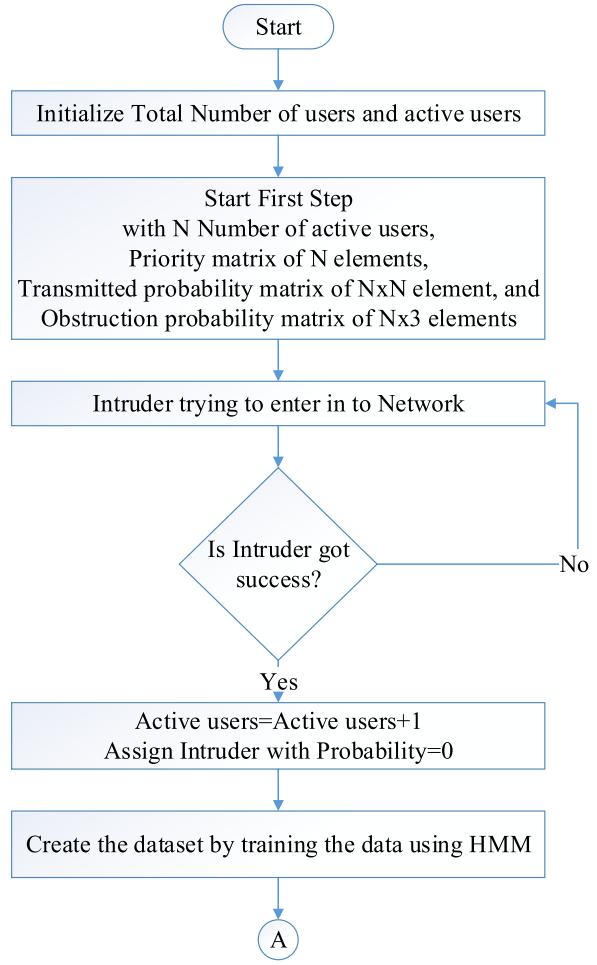

FIGURE 10 Flowchart showing the process of training data set for IDS in the first step

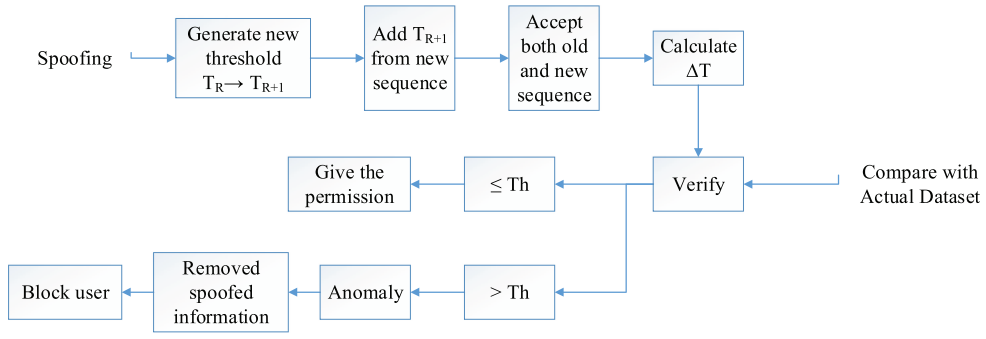

FIGURE 8 Process flow of training data set for IDS

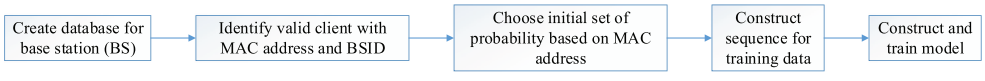

FIGURE 9 Process flow of proposed model of IDS

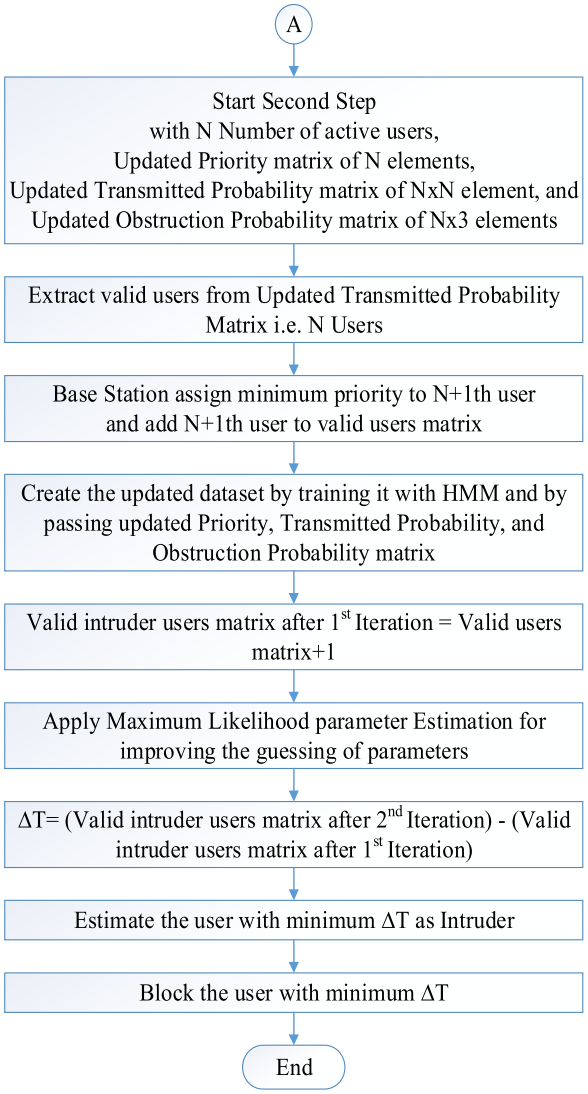

FIGURE 11 Flowchart showing the process of intrusion detection using proposed model in the second step

will not get to intrude in to the network, it will try again. However, if the intruder is successful in intruding in to the network, then the number of active user data is incremented by 1 and the intruder will be assigned with a probability of zero.

The next step is to create the database by training the data using HMM. In the second step, the valid users, ie, N users, are extracted from the updated transmitted probability matrix, and a magnitude of 1 is added to all the valid user's probability before storing them in to the valid user's matrix after first step. The $N+1$th user is assigned with a minimum priority and is added in to the valid users matrix after second step. Then a maximum likelihood parameter estimation is applied for improving the guessing of the parameters. After that, ΔT is calculated, which represents the difference between the probabilities of valid user's matrix after first step and valid users' matrix after second step. The user with a minimum value of ΔT is considered as an intruder and is blocked and removed from the network.

4.2 | Simulation results

For detecting the intruder that has been performing the bandwidth spoofing attack on the SCA in 5G WCN, an adaptive IDS has been proposed. By following the above given steps in Figures 10 and 11, the simulation has been performed and the probability of valid users and intruders after each iteration has been recorded in Table 3. In this simulation, we have assumed a total of 10 users in the network and left 1 space for the intruder to intrude in to the network. We have recorded the probabilities for 8 number of iterations.

After analyzing the recorded table, it is concluded that there will be different number of active users in each iteration and the user with a probability minimum than the valid user's probability will be considered as intruder and is blocked and removed in the next step.

The probabilities shown in the red color are the intruder probabilities in each iteration. The graph shown in Figure 12 clearly shows that the intruder probability is always less than the valid user probability. Hence, it is easy to detect and remove the intruder from the model by using this proposed model of IDS.

4.3 | Analysis

From the above results, it is concluded that the proposed adaptive IDS will be able to detect the intruder that is executing the bandwidth spoofing attack on the SCA in a 5G WCN.

TABLE 3 Probability of valid users and intruders after each iteration

No. users No. Iterations	1	2	3	4	5	6	7	8	9	10	11
1	0.8176	0.8381	0.9867	0.9432	0.9841	0.9543	0.9850	0.8731	0.9097	***0.2540***	
2	1.3248	0.6050	***0.2570***								
3	1.1927	0.3680	***0.0763***								
4	1.0763	0.7529	0.9794	0.7273	0.7863	***0.0494***					
5	0.8161	0.9010	0.9030	0.8516	0.9725	0.8957	0.9393	0.8711	***0.0149***		
6	0.9373	0.8563	0.9328	0.7610	0.9594	0.9053	0.9917	0.8936	0.9186	0.8993	***0.0960***
7	1	***0.0226***									
8	0.9529	1.0365	0.7668	1.0613	0.7945	0.7348	0.8694	0.8553	***0.0824***		

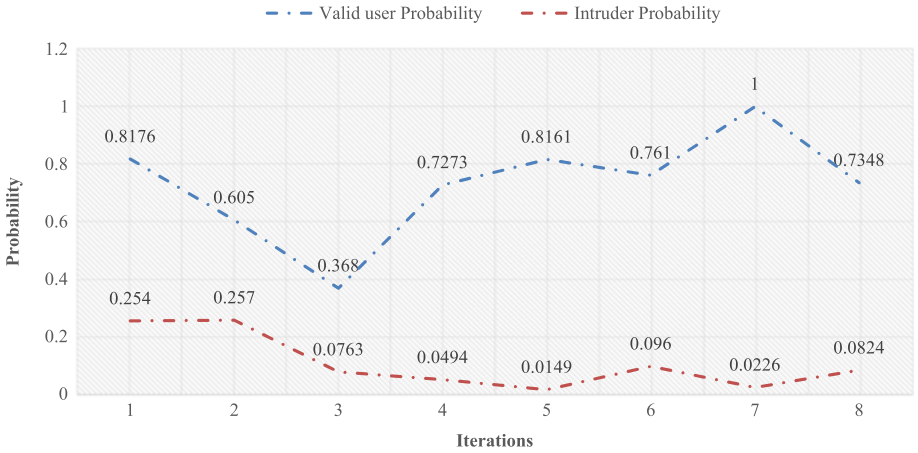

FIGURE 12 Valid user probability vs intruder probability

Simulations have shown that in all the iterations, the probability assigned to the intruder is always less than the valid user probability. Hence, it has become easy for the proposed model of IDS in the SCA to detect the intruder in the first step and remove it from the database in the next step.

5 | CONCLUSION

With the growing number of users in the network, it has become very important to maintain the security. In the present generation, the level of the security needs to be raised. In this article, we have analyzed the different aspects of security threats in 5G WCN. The major goal of 5G WCN is to increase the capacity as well as to reduce the load at the BS. To achieve this, researchers have introduced the concept of relays, SCAs and Wi-Fi hotspots. However, this introduction has paved the way for the possible security breach in to the network, as they provide active sites for the attackers. Hence, 5G WCN has now become highly vulnerable to security threats. The key focus of the article is on the security threats, particularly the bandwidth spoofing attack on the SCA. This article has concluded that the Game theory has proven to be a useful method in examining the bandwidth spoofing attack. In addition, with the use of prisoner's dilemma game theory, attacker is able to spoof the bandwidth from the defender with a significant winning percentage. This article has also proposed an adaptive IDS which is capable of detecting and removing the intruder which is executing the bandwidth spoofing attack on the SCA in a 5G WCN.

In the present generation, there is a lot of scope in 5G security. Researchers all over the world are working on to fill the loop holes in security that has left behind while evolving. The security in D2D and Internet of things will be of prime concern in the near future.

REFERENCES

1. Gupta A, Jha RK. A survey of 5G network: architecture and emerging technologies. *IEEE Access*. 2015;3:1206–1232.
2. Schneider P, Horn G. Towards 5G security. In: *IEEE Trustcom/Big DataSE/ISPA*, 1:1165–1170.
3. Wang C, Wang H. Physical layer security in millimeter wave cellular networks. *IEEE Trans Wireless Commun*. 2016; accepted to appear
4. Wang H, Zheng TX, Yuan J, Towsley D, Lee MH. Physical layer security in heterogeneous cellular networks. *IEEE Trans Commun*. 2016;64(3)12041219.
5. Zhang Y, Wang H, Yang Q, Ding Z. Secrecy sum rate maximization in nonorthogonal multiple access. *IEEE Commun Lett*. 2016.
6. Cao J, Ma M, Li H, Zhang Y, Luo Z. A survey on security aspects for LTE and LTE-A networks. *IEEE Commun Surveys Tuts*. 2014;16(1):283–302. First Quarter
7. Paolini M. Wireless Security in LTE Networks, White paper, 2012.
8. Gupta A, Jha RK. Security threats of wireless networks: a survey. In: 2015 International Conference on Computing, Communication and Automation (ICCCA). May 15–16, 2015:389–395.
9. Traynor P, et al. On cellular botnets: measuring the impact of malicious devices on a cellular network core. Proceedings of the 16th ACM conference on Computer and Communications Security; 2009.
10. Geva M, Herzberg A, Gev Y. Bandwidth distributed denial of service: attacks and defenses. *IEEE Security Privacy*. January–February 2014;12(1):54–61.
11. Snyder ME, Sundaram R, Thakur M. A game-theoretic framework for bandwidth attacks and statistical defenses. In: 32nd IEEE Conference on Local Computer Networks, 2007. LCN 2007. 556–566, October 15–18, 2007.
12. Tom L. Game-theoretic approach towards network security: a review. In: 2015 International Conference on Circuit, Power and Computing Technologies (ICCPCT). 1-4, March 19–20, 2015.
13. Ye M, Hu G. Distributed seeking of time-varying Nash equilibrium for non-cooperative games. 2013 10th IEEE International Conference on, Control and Automation (ICCA), Hangzhou, 2013:1674–1679.
14. Rabiner LR. A tutorial on hidden Markov models and selected applications in speech recognition. *Proc IEEE*. 1989;77(2):257–286.
15. Joshi SS, Phoha VV. Investigating hidden Markov models capabilities in anomaly detection. Proceedings of the 43rd ACM Annual Southeast Regional Conference. 1, 98–103;2005.
16. Ourston D, Matzner S, Stump W, Hopkins B. Applications of hidden Markov models to detecting multi-stage network attacks. Proceedings of the 36th Annual Hawaii International Conference on System Sciences. 9, 334–344; 2003.
17. Cho SB, Park HJ. Efficient anomaly detection by modeling privilege flows using hidden Markov model. *Comput Security*. 2003;22(1):45–55.
18. Hoang XD, Hu J, Bertok P. A multi-layer model for anomaly intrusion detection using program sequences of system calls. Proceedings of the 11th IEEE International Conference Networks. 531–536; 2003.

19. Lane T. Hidden Markov models for human/computer interface modeling. Proceedings of the International Joint Conference on Artificial Intelligence, Workshop Learning about Users. 35–44;1999.

20. Kaufman L, Rousseeuw PJ. *Finding Groups in Data: An Introduction to Cluster Analysis*. *Wiley Series in Probability and Math. Statistics*; 1990.

How to cite this article: Gupta A, Jha RK, Jain S. Attack modeling and intrusion detection system for 5G wireless communication network. *Int J Commun Syst*. 2017;30:e3237. https://doi.org/10.1002/dac.3237