On Physically Secure and Stable Slotted ALOHA System

Yunus Sarikaya, Ozgur Ercetin
Faculty of Engineering and Natural Sciences Sabanci University, Istanbul, Turkey

Abstract—In this paper, we consider the standard discrete-time slotted ALOHA with a finite number of terminals with infinite size buffers. In our study, we jointly consider the stability of this system together with the physical layer security. We conduct our studies on both dominant and original systems, where in a dominant system each terminal always has a packet in its buffer unlike in the original system. For \( N = 2 \), we obtain the secrecy-stability regions for both dominant and original systems. Furthermore, we obtain the transmission probabilities, which optimize system throughput. Lastly, this paper proposes a new methodology in terms of obtaining the joint stability and secrecy regions.

I. INTRODUCTION

Wireless multiple-access broadcast networks have received significant interest from researchers in the past. Slotted ALOHA is one of the basic class of such networks, and a large number of random multiple access algorithms are devised as modifications of this basic system. The two important issues of wireless systems, i.e., the stability and security, have been separately studied in the context of slotted ALOHA and the wireless broadcast networks. Basically, stability requires that queue sizes remain finite when time goes to infinity. Stability in slotted ALOHA has been investigated in [1], [2]. These results have led to further studies, where various bounds and stability regions are obtained for which the queues are stable [3], [4]. In [5], sufficient and necessary conditions for the stability of the system are obtained and for two user case \( (N = 2) \), the stability region is identified. More recent studies have aimed at obtaining tighter bounds for the stability [6]. On the other hand, secure communication over physical layer was first introduced by Shannon [7] and Wyner [8]. Recently, physically secure communication is investigated in [9], [10]. The secure rate allocation vectors are determined for gaussian channels in [11], [12], [13] considers fading channels for which the perfect secrecy regions and the optimal power allocation vectors maximizing secrecy region, are obtained. These works investigated problems only in the security context. In [14], stability and security are combined in the context of wireless broadcast networks, where a base station sends confidential messages to the users. In this system, only downlink channels are considered, where no contention is taking place.

In this paper, we jointly consider the stability and security issues for slotted ALOHA systems, where each user wants to communicate with a single base station. The broadcast channel is modeled as Rayleigh fading channel, where \( N \) user nodes send their confidential messages to a base station as shown in Figure 1. Each message should be kept secret from other users. Hence, all users except the transmitting one are eavesdroppers. In the meantime, the stability of the system should be maintained, i.e., the sizes of the queue for each user should be finite when time goes to infinity. All transmitters are assumed to be synchronized, and the reception of a packet starts at the beginning of a slot and ends at the end of a slot, i.e., each packet transmission occupies exactly one time slot. Also, each user transmits with a probability, \( q_i \), at each time slot.

In prior studies, the secrecy region has always been studied at the symbol level, and thus the secrecy region with respect to transmission probabilities has not been examined before and this perspective is introduced in our paper. Let us define “secrecy-stability region” as the collection of transmission probabilities, \( q_i \), that satisfies both the stability and the security conditions. Our goal is to find the secrecy-stability region and obtain the optimal transmission probabilities, which maximize the system throughput. For \( N = 2 \), we specify the optimal transmission probabilities for the dominant system, where it is assumed that users always have a packet to send in their buffer. In the original system; however the queues may not always have a packet to transmit, and in this case, we show that the maximized system throughput does not depend on the transmission probabilities.

The rest of the paper is organized as follows: In Section II, we introduce the channel model, and give the definitions of the secrecy and the stability. In Section III and IV, we present our results for the dominant and original systems. In Section V, we conclude the paper by summarizing our
II. CHANNEL MODEL AND SECRECY CAPACITY FOR DOWNLINK CHANNELS

We consider a wireless broadcast network operating on a single frequency channel. We assume that the channels from each user to base station and other users are Rayleigh fading broadcast channels, in which each output signals obtained by the base station and other users are corrupted by multiplicative fading gains in addition to an additive Gaussian noise as:

\[ Y_{jn} = h_{jn}X_i + w_{jn}, \text{ for } 1 < i < N, \]

where \( X_i \) denotes the message transmitted by \( i \)th user, \( Y_{jn} \) is the channel output at user \( j \), \( h_{jn} \) is the fading coefficient for the channel between \( i \)th user and \( j \)th user, and \( w_{jn} \) is Gaussian noise term with zero mean and unit variance at the \( n \)th symbol time.

The secrecy level of confidential message, \( W_i \), transmitted from user \( i \) to the base station is measured by the following equivocation rate [14]:

\[ R_i = \lim_{n \to \infty} \frac{1}{n} I(W_i;Y_n^1,...,Y_n^N) \]

The perfect secrecy is achieved when the transmission rate satisfies (2) and the secrecy region is defined as the set of all achievable rate vectors such that the perfect secrecy is achieved [8]. In [14], the secrecy region of fading broadcast channels in the downlink is obtained as:

\[ R_s = \begin{cases} \bigcup \{R_1,R_2,...,R_N\} : & \quad R_i \leq R_{s,i} = \min_{j \neq i, 1 \leq j \leq N} \frac{\log(1 + P|h_i|^2)}{E_{s_{hA(i)}}} - \log(1 + P|h_i|^2) \\ & \text{for } 1 \leq i \leq N \end{cases} \]

where \( h \) defines channel state, \( h_i \) denotes the channel gain between \( i \)th user and the base station, and \( R_{s,i} \) denotes channel gain between \( i \)th and \( j \)th users. \( A(i) \) is the set of all channel states for which the channel gain between \( i \)th user and the base station is the largest. In addition, each user transmits with the same power level denoted as \( P \).

In addition, we define the stability of a queue as in [6], i.e., a queue is stable if it satisfies the following

\[ \lim_{t \to \infty} Pr[s_i(t) < x] = F(x), \quad \lim_{t \to \infty} F(x) = 1, \]

where \( s_i(t) \) is the size of the queue at time \( t \). Namely, the queue size should be finite at any time to achieve stability.

In the following, we investigate the secrecy-stability regions for dominant and original systems.

III. DOMINANT ALOHA UPLINK CHANNEL

The analysis of dominant systems was previously investigated in [1]-[6]. For the dominant system, it is shown that the stability condition is as follows:

\[ \text{Lemma 1:} \quad \text{If} \quad \lambda_i < Q_i \] (5)

for all \( i = 1,...,N \), then the system is stable, where \( \lambda_i \) is the arrival rate and \( Q_i \) is the successful transmission probability for fading channels calculated as:

\[ Q_i = (1 - p_{f,i})q_i \prod_{j=1}^{N} (1 - q_j) \] (6)

where \( p_{f,i} \) is the average failure probability of user \( i \) due to fading. Since \( p_{f,i} \) is constant, we define \( \lambda'_i \) as \( \lambda_i / p_{f,i} \). Then, the stability condition can be rewritten as:

\[ \lambda'_i < q_i \prod_{j=1}^{N} (1 - q_j) \] (7)

Lemma 1 specifies the stability condition, but does not give any result about which specified arrival rates lead to a positive stability region.

\[ \text{Lemma 2:} \quad \text{If} \quad \lambda_i < (q_i - q_{i-1}) \prod_{j=1}^{N} (1 - q_j) \] (8)

For \( N = 2 \), expression in (8) can be written as:

\[ x^{N-1} - \prod_{i=1}^{N} (x + \lambda'_i) > 0 \quad \text{for any} \quad x > 0 \] (9)

\[ \sqrt{\lambda'_i} + \sqrt{\lambda'_j} < 1 \] (10)

The proofs of Lemma 1 and 2 can be found in [3].

Now, we are ready to derive the perfect secrecy condition for dominant ALOHA systems.

\[ \text{Theorem 1:} \quad \text{If} \quad \rho_i \geq q_i \prod_{j=1}^{N} (1 - q_j) \] (11)

for all \( i = 1,...,N \), then the system is secure. Note that \( \rho_i \) defines the ratio between the perfect secrecy capacity, \( R_{s,i} \), and the capacity of fading channels, \( R_i \).

\[ \text{Proof} \]

The security region given in (13) is computed for downlink channels, where there is no channel contention. However, in our model, we consider uplink channels, where packets when transmitted simultaneously collide with each other. We assume that collision results in scrambled bits and thus the received packets cannot be correctly decoded. Therefore, we assume that the packets in collision have no information value. Let us define new events \( Z_1, Z_2 \) and \( W_i \) as:
where $\hat{W}_i$ defines the event where messages are transmitted with no collision.

The relationship between the equivocation rates of $W_i$ and $\hat{W}_i$ is:

$$H(\hat{W}_i|Y^n_1,\ldots,Y^n_{i-1},Y^n_{i+1},\ldots,Y^n_N) = 
\begin{cases} 
1, & \text{transmission for } i^{th} \text{ user} \\
0, & \text{no transmission for } i^{th} \text{ user} 
\end{cases}$$

$$Z_1 = \begin{cases} 
1, & \text{no collision for } i^{th} \text{ user} \\
0, & \text{collision for } i^{th} \text{ user} 
\end{cases}$$

$$Z_2 = \begin{cases} 
1, & \text{transmission for } i^{th} \text{ user} \\
0, & \text{no transmission for } i^{th} \text{ user} 
\end{cases}$$

$$W_i = \begin{cases} 
\hat{W}_i, & \text{if } Z_1 = 1 \text{ and } Z_2 = 1 \\
0, & \text{otherwise} 
\end{cases}$$

(11)

Theorem 2: For $N = 2$, the optimal transmission probabilities are as follows:

(1) when

$$\sqrt{p_1} + \sqrt{p_2} \leq 1$$

(15)

$$q_1 = \frac{(1 + p_1)}{2} + \frac{\sqrt{(1 + p_1)^2 - 4(p_1 + p_2)}}{2}$$

$$q_2 = \frac{(1 + p_2)}{2} + \frac{\sqrt{(1 + p_2)^2 - 4(p_1 + p_2)}}{2}$$

(16)

(2) when

$$\sqrt{p_1} + \sqrt{p_2} \geq 1$$

$$\sqrt{p_1} + \sqrt{\lambda'_1} < 1$$

(17)
Fig. 3: Secrecy-Stability Regions for Dominant System

\[ q_1 = \sqrt{\rho_1}, \quad q_2 = 1 - \sqrt{\rho_1} \text{ or } q_1 = 1 - \sqrt{\rho_2}, \quad q_2 = \sqrt{\rho_2} \]  
\[ q_1 = \sqrt{\lambda_1}, \quad q_2 = 1 - \sqrt{\lambda_1} \text{ or } q_1 = 1 - \sqrt{\lambda_2}, \quad q_2 = \sqrt{\lambda_2} \]  
(3) when

\[ \sqrt{\rho_1} + \sqrt{\rho_2} \geq 1 \]
\[ \sqrt{\rho_1} + \sqrt{\lambda_2} > 1 \]
\[ \sqrt{\rho_2} + \sqrt{\lambda_1} > 1 \]

Proof

The throughput optimization problem can be formulated as follows:

\[ \max S = q_1(1 - q_2)(1 - p_{f,1}) + q_2(1 - q_1)(1 - p_{f,2}) \]  
\[ \text{s.t.} \quad q_1(1 - q_2) \leq \rho_1 \]
\[ q_2(1 - q_1) \leq \rho_2 \]
\[ \lambda_1' < q_1(1 - q_2) \]
\[ \lambda_2' < q_2(1 - q_1) \]
\[ 0 \leq q_1, q_2 \leq 1, \]  
(21)

where \( p_{f,1} \) and \( p_{f,2} \) denote the probability of channel failure of the first and second users respectively.

The objective function in (21) can be rewritten as a sum of two linear variables, e.g., \((X(\text{for } q_1(1 - q_2)) + Y(\text{for } q_2(1 - q_1)))\), while these linear variables are also constrained by linear inequalities. From the basic knowledge of linear programming, the optimal solution is known to be located at the corners of feasible region. Thus, as long as \( q_1 \) and \( q_2 \) are in \([0,1]\), we expect that the optimal solution is to appear on the boundary of the feasible region.

(1) First, we consider the case when the optimal solution is achieved at the boundary of the secrecy region given in Figure 3(a). Then, the Lagrangian to solve optimization problem in (21)-(26) is given by:

\[ L = \beta_1(1 - q_2)(1 - p_{f,1}) + q_2(1 - q_1)(1 - p_{f,2}) - \beta_1(q_1(1 - q_2) - \rho_1) - \beta_2(q_2(1 - q_1) - \rho_2) \]  
(27)
\[ + \alpha_1(q_1(1 - q_2) - \lambda_1') + \alpha_2(q_2(1 - q_1) - \lambda_2'), \]

where \( \beta_1 \) and \( \beta_2 \) are lagrange multipliers for inequalities in (22) and (23), and \( \alpha_1 \) and \( \alpha_2 \) for inequalities in (24) and (25). Since the solution is assumed to be at the boundary of secrecy region, \( \alpha_1 = 0 \) and \( \alpha_2 = 0 \). We take the derivative of the lagrangian with respect to non-zero lagrange multipliers and transmission probabilities, and equate to zero as:

\[ \frac{\partial L}{\partial q_1} = (1 - q_2)(1 - p_{f,1}) - q_2(1 - p_{f,2}) - \beta_1(q_1(1 - q_2) - \rho_1) = 0 \]
\[ \frac{\partial L}{\partial q_2} = (1 - q_1)(1 - p_{f,1}) - q_1(1 - p_{f,2}) - \beta_2(q_2(1 - q_1) - \rho_2) = 0 \]
\[ \frac{\partial L}{\partial \rho_1} = q_1(1 - q_2) - \rho_1 = 0 \]
\[ \frac{\partial L}{\partial \rho_2} = q_2(1 - q_1) - \rho_2 = 0 \]  
(28)

By simple manipulations, we obtain \( \beta_1 \) and \( \beta_2 \) as 1, which satisfies the condition that lagrange multipliers should be greater than zero. For this case, we found \( q_1 \) as \((1 + p_1)^2 - 4(p_1 + p_2) \geq 0\) and \( q_2 \) as \((1 + p_2)^2 - 4(p_1 + p_2) \geq 0\). Note that this solution attains a real root, when the following conditions are satisfied: \((1 + p_1)^2 - 4(p_1 + p_2) \geq 0\) and \((1 + p_2)^2 - 4(p_1 + p_2) \geq 0\). After some manipulations, we see that a real solution is realized when

\[ \sqrt{\rho_1} + \sqrt{\rho_2} \leq 1 \]  
(29)

(2) Figure 3(b) shows the secrecy-stability region, when the condition in (29) does not hold, i.e., \( \beta_1 > 0 \) and \( \beta_2 > 0 \) jointly cannot be satisfied.

First, Let \( \beta_1 \geq 0 \) and \( \beta_2 = 0 \), then we have the following derivatives:

\[ \frac{\partial L}{\partial q_1} = (1 - q_2)(1 - p_{f,1}) - q_2(1 - p_{f,2}) - \beta_1(1 - q_2) = 0 \]
\[ = (1 - q_1)(1 - p_{f,2}) - q_1(1 - p_{f,1}) + \beta_1 q_1 = 0 \]
\[ \frac{\partial L}{\partial q_2} = q_1(1 - q_2) - q_1(1 - p_{f,1}) + \beta_1 q_1 = 0 \]
\[ \frac{\partial L}{\partial p_{f,1}} = q_1(1 - q_2) - \rho_1 = 0 \]  
(30)
From the first two equations in (30), we find \( q_1 = 1 - q_2 \) and by using the third equation in (30), we obtain the solution as: \( q_1 = \sqrt{p_1} \) and \( q_2 = 1 - \sqrt{p_1} \). However, this solution should satisfy the stability condition in (25) as well:

\[
\begin{align*}
q_2(1 - q_1) &> \lambda'_2 \\
(1 - \sqrt{p_1})(1 - \sqrt{p_1}) &> \lambda'_2 \\
\sqrt{p_1} + \lambda'_2 &< 1
\end{align*}
\]  

(31)

Similarly, when \( \beta_2 \geq 0 \) and \( \beta_1 = 0 \), we can follow the same discussion as before to obtain the solution as: \( q_2 = \sqrt{p_2} \) and \( q_1 = 1 - \sqrt{p_2} \) when \( \sqrt{p_2} + \lambda'_2 < 1 \).

Now, the optimal solution is one of these two solutions; however, since the secrecy-stability region is not convex, we cannot determine the optimal closed form solution.

(3) When the conditions in (29) and (31) do not hold, the secrecy-stability region only consists of the stability region as shown in Figure 3(c). Then, we have the following optimization problem:

\[
\begin{align*}
\max & \quad S = q_1(1 - q_2)(1 - p_{f,1}) + q_2(1 - q_1)(1 - p_{f,2}) \\
\text{s.t.} & \quad \lambda'_1 < q_1(1 - q_2) \\
& \quad \lambda'_1 < q_2(1 - q_1) \\
& \quad 0 \leq q_1, q_2 \leq 1.
\end{align*}
\]

(32)

As before, we expect that the optimal solution is to appear at the boundary. Both constraints cannot be active, so we select only one of them as active. First, we consider the first constraint as the active constraint: The lagrange multipliers are: \( \alpha_1 \leq 0 \) and \( \alpha_2 = 0 \). Then, the lagrange function is as follows:

\[
L = q_1(1 - q_2)(1 - p_{f,1}) + q_2(1 - q_1)(1 - p_{f,2}) + \alpha_1(q_1(1 - q_2) - \lambda'_1)
\]

(33)

Then, we have the following derivatives:

\[
\begin{align*}
\frac{\partial L}{\partial q_1} &= (1 - q_2)(1 - p_{f,1}) - q_2(1 - p_{f,2}) + \alpha_1(1 - q_2) = 0 \\
\frac{\partial L}{\partial q_2} &= (1 - q_1)(1 - p_{f,2}) - q_1(1 - p_{f,1}) - \alpha_1 q_1 = 0 \\
\frac{\partial L}{\partial \alpha_1} &= q_1(1 - q_2) - \lambda'_1 = 0
\end{align*}
\]

(34)

If we solve these equations, we obtain the solution as:

\[
q_1 = \sqrt{\lambda'_1} \quad \text{and} \quad q_2 = 1 - \sqrt{\lambda'_1}.
\]

Similarly, if we let \( \alpha_2 \leq 0 \) and \( \alpha_1 = 0 \), then we get the solution as follows: \( q_1 = 1 - \sqrt{\lambda'_2} \) and \( q_2 = \sqrt{\lambda'_2} \).

IV. ORIGINAL ALOHA UPLINK CHANNEL

In this section, we consider systems where the buffers of the users do not always have packets. Let \( p_{e,i} \) be the probability of queue of user \( i \) being empty. Then, the secrecy condition is defined as follows:

**Theorem 3:** If

\[
q_i \prod_{j=1,j\neq i}^{N} ((1 - p_{e,j})(1 - q_j) + p_{e,j}) \leq \rho_i
\]

(35)

for all \( i (i = 1, ..., N) \), then the system is secure.

**Proof**

In Theorem 1, we obtained the secrecy condition for dominant systems, where there are no empty queues. The method of the proof of Theorem 3 is the same, where we want to determine the portion of time when there is a single transmission and no collision. However, in the original system the probability of this event is different from the one in a dominant system. Let us define new event, \( E_i \) as:

\[
E_i = \begin{cases} 
1, & \text{queue of } i^{th} \text{ user is not empty} \\
0, & \text{queue of } i^{th} \text{ user is empty}
\end{cases}
\]

(36)

Then, the equivocation rate for the original system is

\[
H(\tilde{W}_i| Y^n_1, Y^n_{i+1}, Y^n_{i+1}, ..., Y^n_N) =
\]

(37)

\[
P(Z_i^1 = 1, Z_i^2 = 1|E_i = 1) =
q_i \prod_{j=1,j\neq i}^{N} ((1 - p_{e,j})(1 - q_j) + p_{e,j})
\]

(38)

If we make the same mathematical operations as in (13), we obtain the following secrecy condition:

\[
q_i \prod_{j=1,j\neq i}^{N} ((1 - p_{e,j})(1 - q_j) + p_{e,j}) \leq \rho_i
\]

(39)

Note that \( \rho_i \) can be interpreted as proportion of time in all occupied slots with successful transmissions with no collisions.

**Theorem 4:** For \( N = 2 \), the secrecy condition is as follows:

\[
1 + \lambda'_1 - \lambda'_2 - \sqrt{\rho_1^2((\lambda'_2 - 1 - \lambda'_1)^2 + 4\lambda'_1^2)} = q_i^* \leq q_i
\]

(40)

Due to the symmetric behavior of the system, the secrecy condition for the second user is obtained by replacing \( \rho_1 \) by \( \rho_2 \), \( \lambda'_1 \) by \( \lambda'_2 \) and \( \lambda'_2 \) by \( \lambda'_1 \) in (40).

**Proof**

In Theorem 3, we have shown that the system is secure when

\[
q_i \leq \frac{\rho_i}{(1 - p_{e,2})(1 - q_2) + p_{e,2}}
\]

(41)

Also by Little’s theorem [2], we know that

\[
p_{e,1} = 1 - \frac{\lambda'_1}{\mu_1}
\]

(42)
where $\mu_1$ is the average service rate of the first user. We have the following relationship between the service rate, $\mu_1$, and $\rho_1$:

$$\mu_1 = (1 - p_{f,1})q_1((1 - p_{e,2})(1 - q_2) + p_{e,2}) \leq \rho_1(1 - p_{f,1})$$  \hspace{1cm} (43)

Thus, by substituting (43) into (42), we obtain

$$p_{e,1} \leq 1 - \frac{\lambda_i}{\rho_1(1 - p_{f,1})} = 1 - \frac{\lambda_i'}{\rho_1}$$  \hspace{1cm} (44)

By the symmetric behavior of the system, we know that

$$p_{e,2} = 1 - \frac{\lambda_i'}{q_2((1 - p_{e,1})(1 - q_1) + p_{e,1})} \geq 1 - \frac{\lambda_i'}{q_2\frac{\lambda_i}{\rho_1}(1 - q_1) + 1 - \frac{\lambda_i}{\rho_1}}$$  \hspace{1cm} (45)

By substituting (45) into (41), we obtain the following quadratic equation:

$$\lambda_i'q_1^2 + \rho_1(\lambda_i' - 1 - \lambda_i')q_1 + \rho_1^2 \leq 0$$  \hspace{1cm} (46)

Interestingly, the above equation does not depend on the transmission probability of the eavesdropper, $q_2$. From (46), we obtain a bound on $q_1$ as:

$$\max(0, \frac{1 + \lambda_i' - \lambda_i' - \sqrt{\rho_1^2((\lambda_i' - 1 - \lambda_i')^2 - 4\lambda_i')}}{2\lambda_i'}) \leq q_1$$

$$\leq \min(1, \frac{1 + \lambda_i' - \lambda_i' + \sqrt{\rho_1^2((\lambda_i' - 1 - \lambda_i')^2 - 4\lambda_i')}}{2\lambda_i'})$$  \hspace{1cm} (47)

Also note that, the term, $\frac{1 + \lambda_i' - \lambda_i' - \sqrt{\rho_1^2((\lambda_i' - 1 - \lambda_i')^2 - 4\lambda_i')}}{2\lambda_i'}$, is positive, since $\rho_1 \leq 1$ and $\lambda_i' \geq 0$. In addition, the term, $\frac{1 + \lambda_i' - \lambda_i' + \sqrt{\rho_1^2((\lambda_i' - 1 - \lambda_i')^2 - 4\lambda_i')}}{2\lambda_i'}$, is always bigger than one, since from lemma 2 we know that $\sqrt{\lambda_i'} + \sqrt{\lambda_i'} < 1$ and so $\lambda_i' + \lambda_i' < 1$. Then, the solution in (47) becomes:

$$1 + \lambda_i' - \lambda_i' - \sqrt{\rho_1^2((\lambda_i' - 1 - \lambda_i')^2 - 4\lambda_i')} = q_1 \leq q_1$$  \hspace{1cm} (48)

Also, $p_{e,2} \geq 0$ which results in (49) by substituting $q_1^*_{1}$ in (45):

$$q_2 \geq \frac{\lambda_i'\rho_1}{\rho_1 - q_1^*\lambda_i'} = q_2^*$$  \hspace{1cm} (49)

Note that, when $q_1$ is equal to $q_1^*$ and $q_2$ is $q_2^*$, then $p_{e,2}$ is zero, which means that the second user always has a packet to transmit as in a dominant system.

Finally, we attain the following condition:

$$1 + \lambda_i' - \lambda_i' - \sqrt{\rho_1^2((\lambda_i' - 1 - \lambda_i')^2 - 4\lambda_i')} = q_1 \leq q_1$$

for $q_2 \geq \frac{\lambda_i'\rho_1}{\rho_1 - q_1^*\lambda_i'}$  \hspace{1cm} (50)

**Lemma 3:** In order to have a stable system, the average service rate, $\mu_i$, should be greater than the arrival rate. Then, we have the following stability condition:

$$\mu_i = (1 - p_{f,1})q_i \prod_{j=1, j \neq i}^N ((1 - p_{e,j})(1 - q_j) + p_{e,j}) > \lambda_i$$

$$q_i \prod_{j=1, j \neq i}^N ((1 - p_{e,j})(1 - q_j) + p_{e,j}) > \frac{\lambda_i}{1 - p_{f,i}} = \lambda_i'$$  \hspace{1cm} (51)

The secrecy and stability regions for the original system are shown in Figure 4(a) and Figure 4(b) respectively. The proof for the stability region can be found in [3].

By combining both regions, we obtain the secrecy-stability region as illustrated in Figure 4(c). At the points, $(q_1^*, q_1^*)$ and $(q_2^*, q_2^*)$, the probability of queue 2 and queue 1 being empty are zero, which is the same in the dominant system.

Thus, the point $(q_1^*, q_2^*)$ is located on the intersection of two stability curves as seen in Figure 4(c).

**Theorem 5:** The optimum throughput, $S^*$, for any transmission probabilities in the secrecy-stability region is equal to sum of arrival rates:

$$S^* = \sum_{i=1}^N \lambda_i$$  \hspace{1cm} (52)

**Proof**

The system throughput is formulated as:

$$S = \sum_{i=1}^N (1 - p_{f,i})(1 - p_{e,i})q_i \prod_{j \neq i}^N ((1 - p_{e,j})(1 - q_j) + p_{e,j})$$

We know that $1 - p_{e,i}$ is equal to $\lambda_i/\mu_i$ and the term, $(1 - p_{f,i})q_i \prod_{j \neq i}^N ((1 - p_{e,j})(1 - q_j) + p_{e,j})$, is defined as the average service rate, then for $\mu_i > 0$ we obtain the following result:
In theorem 5, we find out that the optimum throughput can be any point in the secrecy-stability region. That is because, increasing the transmission probabilities leads to a decrease in the probability of having empty queue, and this results in a decrease in successful transmission probability. Thus, even if we increase the transmission opportunities, success out of these opportunities will not change.

V. CONCLUSION

In this paper, we have studied slotted ALOHA network, for which we have obtained secrecy-stability conditions for the dominant and original system. We have further obtained the optimal transmission probabilities for $N = 2$. This is the first work that jointly addresses both the secrecy and stability of a wireless network with contention.

REFERENCES

[1] N. Abramson, “The ALOHA system—another alternative for computer communication,” in AFIPS Conf. Proc., vol. 37, pp. 281-285, 1970.
[2] D. Bertsekas and R. Gallager, Data Network, 2nd ed. Englewood Cliffs, NJ: Prentice-Hall, 1992.
[3] B. S. Tsybakov, V. A. Mikhailov, “Ergodicity of a Slotted ALOHA System”, Problemy Preedachi Inf., vol. 15, no. 4, pp. 73-87, March 1979.
[4] R. Rao and A. Ephredemis, “On the stability of interacting queues in a multi-access system,” IEEE Trans. Inform. Theory, vol. 34, pp. 918-930, Sept. 1988
[5] W. Malyshev, “A classification of two-dimensional markov chains and piecewise-linear martingales,” Dokl. Akad. Nauk USSR, vol. 3, pp. 526-528,1972.
[6] W. Luo abd A. Ephredemis, “Stability of N interacting queues in random-access Systems”, IEEE Trans. Inform. Theory, vol. 45, pp. 1579-1587, July 1999.
[7] C. E. Shannon, “Communication theory of secrecy systems,” Bell Syst. Tech. J., vol. 28, pp. 656-715, Oct. 1949
[8] A. D. Wyner, ”The wire-tap channel,” Bell Syst. Tech. J., vol. 54, no. 8, pp. 1355-1387, Oct. 1975.
[9] I. Csiszar, J. Kner, “Broadcast Channels with Confidential Messages”, IEEE Transaction on Information Theory, Vol 24, No. 3, pp. 339-348, May 1978.
[10] R. Liu, I. Marie, P. Spasojevic, R. Yates, “Discrete memoryless interference and broadcast channels with confidential messages: Secrecy capacity regions,” IEEE Transaction on Information Theory, Vol. 54, No. 6, pp. 2493-2507, June 2008.
[11] T. Liu, V. Prabhakaran, S. Vishwanath, “The Secrecy Capacity of a Class of Parallel Gaussian Compound Wiretap Channels”, International Symposium on Information Theory 2008, ISIT 2008, pp. 116-120, July 2008.
[12] S. Shaﬁee, N. Liu, S. Ulukus, “Secrecy capacity of the 2-2-1 gaussian MIMO wire-tap channel”, 3rd International Symposium on Communications, Control and Signal Processing, ISCCSP 2008, Vol. 12, No. 14, pp. 207-212, March 2008.
[13] Y. Liang, H. V. Poor, Shamai S., “Secure Communication Over Fading Channels”, IEEE Transaction on Information Theory, Vol. 54, No. 6, pp. 2470-2492, June 2008.
[14] Y. Liang, H. V. Poor, L. Ying, “Wireless Broadcast Networks: Reliability, Security and Stability”, Information Theory and Applications Workshop 2008, ITA 2008, pp. 249-255, Feb. 2008.
[15] J. C. Arnbak and W. van Blitterswijk, “Capacity of Slotted Aloha in Rayleigh-fading channels,” IEEE J. Select. Areas Commun., vol. SAC-5, pp. 261-269, Feb. 1987.