Secured operating regions of Slotted ALOHA in the presence of interfering signals from other networks and DoS attacking signals

Jahangir H. Sarker, Hussein T. Mouftah *

School of Information Technology and Engineering (SITE), University of Ottawa, Ottawa, Ontario, Canada K1N 6N5

Received 14 October 2010; revised 8 April 2011; accepted 10 April 2011
Available online 14 May 2011

Abstract It is expected that many networks will be providing services at a time in near future and those will also produce different interfering signals for the current Slotted ALOHA based systems. A random packet destruction Denial of Service (DoS) attacking signal can shut down the Slotted ALOHA based networks easily. Therefore, to keep up the services of Slotted ALOHA based systems by enhancing the secured operating regions in the presence of the interfering signals from other wireless systems and DoS attacking signals is an important issue and is investigated in this paper. We have presented four different techniques for secured operating regions enhancements of Slotted ALOHA protocol. Results show that the interfering signals from other wireless systems and the DoS attacking signals can produce similar detrimental effect on Slotted ALOHA. However, the most detrimental effect can be produced, if an artificial DoS attack can be launched using extra false packets arrival from the original network. All four proposed secured operating regions enhancement techniques are easy to implement and have the ability to prevent the shutdown of the Slotted ALOHA based networks.

Introduction

To improve the secured transmission over vulnerable wireless networks, assessment of the wireless multiple access schemes in the presence of jamming or attacking signals is an important issue [1]. It is well known that the Code Division Multiple Access (CDMA) system has a special resistance against the interference signals from other networks and the attacking signals. Thus the CDMA scheme may be the first choice as a multiple access scheme in the presence of interference signals from other networks or/and attacking signals. The attacker should spread its energy evenly over all degrees of freedom in order to minimize the average capacity of the original signals [2,3]. In a sim-
plified CDMA transmission system, with the knowledge of spreading code, the receiver is able to detect the users’ signals from interfering signals from other networks and attacking signals. Using the attacker state information and the effects of fading, the channel capacity can be enhanced further. For enhancing uplink channel capacity, the attacker state information is more important than that of the effects of fading.

Preventing the attacking signals becomes very difficult, if the attackers use the same code as the legal users and transmit. A specific Frequency Hoping Speed Spectrum (FHSS) technique can prevent this type of attack [4]. However, a specific FHSS technique is inefficient for a large number of mobile nodes. An innovative message-driven frequency hopping was introduced and analyzed to improve the system capacity [5]. The mobile nodes can exploit channel diversity in order to create wormholes in hostile jamming or attacking environment, [6].

In infrastructure-less wireless Ad Hoc and sensor a network, mobile nodes not only behave as transmitters and receivers but also as network elements, i.e., switches or routers, without any established network infrastructure. As a result, low power consumption systems are becoming important for infrastructure-less wireless Ad Hoc and sensor networks. The Slotted ALOHA is the most spectral and power efficient multiple access scheme [7,8]. Although, the CDMA has especial resistance against interference and attacking signals, Slotted ALOHA is a widely used random access protocol not only for its simplicity also for its higher spectral and power efficiency.

The Slotted ALOHA multiple access schemes is used exclusively in newly developed Radio Frequency Identification (RFID) technology [9]. The Slotted ALOHA is also used as a part of different multiple access protocols especially for the control channels in many new wireless technologies. For instance, it is used in the random access channels of Global System for Mobile (GSM) communications [10] and its extension General Packet Radio Services (GPRS) [11,12], Wideband Code Division Multiple Access (WCDMA) system [13], cdma2000 [14,15], IEEE 802.16 [16], IEEE 802.11 [17], etc. A smart power saving jammer or attacker can attack only in the signaling channels, instead of attacking whole channels [18–20]. Therefore, defending the control channels from external and internal attacks [21] are very important issue. If the total network is based on Slotted ALOHA based protocol, then defending the network against the DoS attack is one of the most important factors [22,23] and has been discussed in this paper.

A special type of Denial of Service (DoS) attack, called random packet destruction that works by transmitting short periods of noise signals is considered as attacking signals. This random packet destruction DoS packets can effectively shut down Slotted ALOHA based networks [9] and the networks use the Slotted ALOHA based signaling channels [10–20]. One of the main drawbacks of Slotted ALOHA is its excessive collisions at higher traffic load condition. The current anti-attack measures such as encryption, authentication and authorization [24,25] cannot prevent these types of attacks. Since the random packet destruction DoS packets increase the collision further, the receiver cannot read the message packets.

The effect of attacking noise packet signals on the Slotted ALOHA scheme without autonomic is investigated [26–28]. The stability of Slotted ALOHA in the presence of attacking signals is presented in Sarker and Mouftah [29], where dynamic channel load and jamming information are needed to maximize the channel throughput, which makes the system implementation difficult. Recently, there has been an increasing interest in the autonomic networks, i.e., networks should be self-stabilized without the use of feedback information [30]. Excellent work in self-stabilized Slotted ALOHA without the use of feedback information is presented in Bing [31], where the effect of attacking signals is not considered. A self-stabilized random access protocol in the presence of random packet destruction DoS attack for infrastructure-less wireless autonomic networks is presented in Sarker and Mouftah [32]. In this paper we have investigated the combined effect of the interfering signals from other networks and the DoS attacking signals on Slotted ALOHA. Three different types of noises are considered in this paper. First, noise related to interfering packets from the same network. Second, noise related to interfering packets from the other networks and third, noise related to attacking packets from DoS attack. The contributions of this paper are outlined as follows.

1. The throughput of Slotted ALOHA in the presence of the interfering signals from other networks and the random packet destruction DoS attack is presented.
2. It is shown that for any positive value of message packet arrival rate, the throughput decreases with the increase of the interfering signals from other networks’ signal rate. Similarly, the throughput decreases with the increase of the random packet destruction DoS attacking packet rate.
3. A sufficient number of channels can prevent the shut-down of Slotted ALOHA in the presence of interfering signals from other networks or/and the random packet destruction DoS attack by reducing the collisions.
4. In the presence of other message packets, a message packet is captured, if its power is higher than the message capture ratio times of all other interfering message packets’ power for a certain section of time slot to lock the receiver. Similarly, a message packet is captured, in the presence of interfering packets from other networks, if its power is higher than the interfering capture ratio times of the power of the interfering packets from other networks. At the same way, a message packet is captured, in the presence of attacking noise packets, if its power is higher than the attacking capture ratio times of other attacking noise packets’ power. Results show that a lower value of the message capture ratio is the most effective solution comparing with the interfering packet capture ratio or the attacking packet capture ratio.
5. The approximate value of the number of channels that provides the maximum throughput is derived.
6. The security improvement region using the number of retransmission trials control is presented.
7. The security improvement region using the new packet rejection is also presented.

Rest of the paper is organized as follows. The system model and assumptions are described in the next section. The third section shows the security improvement using multiple channels and capture effects. The security improvement by limiting the number of retransmission trials is evaluated in the fourth section. The fifth section presents the security improvement by new packet rejection. The conclusion is provided in the last section.
Secured operating regions of Slotted ALOHA in the presence of interfering signals from other networks and attacking signals

System model and assumptions

Let us consider a system, where a base station is located in the middle of a very large number of users having mobile units (nodes). Assume that the average value of the new message packet arrival rate from all active mobile nodes per time slot is \( \lambda \) packet per time slot. In Slotted ALOHA, the throughput initially increases with the increase of the new packet generation rate, \( \lambda \). The throughput reaches its maximum value for a certain value of the new packet generation rate from all active nodes. The throughput collapse is known as the security or stability problem in Slotted ALOHA. The reason for throughput collapse is excessive collision. The interference from other networks’ jamming packets will transmit at the same slot of an attacking signal from other networks and attacking signals. In multiple L-channel Slotted ALOHA system, the attacker should spread its energy evenly over all degrees of freedom in order to minimize the average capacity [2,3]. Let us assume that the attacking packets also transmitted at L parallel Slotted ALOHA channels to increase the collision. The effect of receiver noise has not been considered in this analysis, since it is very small compared to the collision.

The probability that \( j \) attacking noise packets out of \( n \) attacking noise packets will be transmitted at the same slot of an L-channel Slotted ALOHA system is

\[
A_{nj} = \binom{n}{j} \left( \frac{1}{L} \right)^j \left( 1 - \frac{1}{L} \right)^{n-j}
\]

From total probability theory, the probability that \( j \) attacking noise packets are transmitted to the same slot is

\[
A_j = \sum_{n=j}^{\infty} \frac{p^n}{n!} e^{-J} \left( \frac{1}{L} \right)^j \left( 1 - \frac{1}{L} \right)^{n-j} = \frac{(J/L)^j}{\beta} e^{-J/L}
\]

If the base station can receive only one message packet per time slot in the presence of interfering packets from other networks and attacking noise packets, then the slot is considered as successful. Let a maximum of \( r \) retransmission trials be allowed. Assume the retransmitted packets are also Poisson arrival [33]. Thus, the aggregate message packet arrival rate is \( G \) packet per time slot. If any message packet also selects \( L \) channels by random selection, the aggregate message packet arrival rate per time slot is \( G/L \). The system model and assumptions is presented in Fig. 1.

\[ m = \frac{p^m}{m!} e^{-l} \]

\[ I_{jk} = \binom{m}{i} \left( \frac{1}{L} \right)^i \left( 1 - \frac{1}{L} \right)^{m-i} \]

\[ I_j = \sum_{m=j}^{\infty} \frac{p^m}{m!} e^{-l} \left( \frac{1}{L} \right)^i \left( 1 - \frac{1}{L} \right)^{m-i} = \frac{(J/L)^i}{\beta} e^{-J/L} \]
Probability of success

The radio channel is characterized by fading of the receiving signal, resulting from vector addition of several reflected, scattered or diffracted multi-paths. The fading is assumed to be slow, affecting all bits in a packet in the same way, and flat, implying sufficiently low bit rates. With these assumptions the received signal envelop \( r \) is constant over each packet and approximately Rayleigh distributed [34]

\[
f(r) = \frac{2r}{P_0} \exp\left(-\frac{r^2}{P_0}\right) \quad r \geq 0
\]  

(7)

\[
P(Su) = P(\text{the selected packet will be a message packet})
\]

\[
= P(\text{a message packet is captured in the presence of interfering packets from other networks}) + P(\text{a message packet is captured in the presence of attacking noise packets}) + P(\text{the message packet is captured in the presence of other interfering message packets})
\]

\[
= P_M \cdot P_{CI} \cdot P_{CA} \cdot P_{CM}
\]  

(10)

where \( P_0 \) is the average power of the received packets. The corresponding instantaneous power distribution (i.e., power distribution of the packets) can easily been shown to be [34]

\[
f(p) = \frac{1}{P_0} \exp\left(-\frac{p}{P_0}\right) \quad p \geq 0
\]  

(8)

In the following analysis it is assumed that packet collision in a slot is the sole cause of packet loss. This, of course, is not strictly true since deep fades also contribute to packet loss, due to an increase error rate, even without packet collision. In a well-designed system, the probability of such events is generally of order of magnitude smaller than that of packet collision.

In a Rayleigh fading channel the probability that the power of a message packet is higher than that of the power of an attacking packet is \( \frac{1}{2} \) [32]. In the same way, it can be shown that the probability that the power of an attacking packet is higher than that of the power of a message packet is also \( \frac{1}{2} \).

The probability that a test message packet will be selected from all three types of packets is the ratio of the total number of message packets per time slot and the total number of interfering packets per time slot plus the total number of interfering packets from other networks per time slot and plus the total number of attacking noise packets per time slot. Therefore, the probability that a selected test packet is a message packet is

\[
P_M = P(\text{the selected packet is a message packet}) = \frac{\text{Total number of message packets}}{\text{Total number of message packets} + \text{Total number of interfering packets from other networks} + \text{Total number of attacking packets}}
\]

\[
= \frac{\sum_{n=0}^{\infty} a^n (G/L)^n e^{-G/L} + \sum_{b=0}^{\infty} b^n (I/L)^b e^{-I/L} + \sum_{c=0}^{\infty} c^n (J/L)^c e^{-J/L}}{G/L + I/L + J/L} = \frac{G}{G + I + J}
\]  

(9)

A message packet is successfully received in a time slot, if four conditions are fulfilled. First, the receiver will select a message packet in the presence of message packets from the same network, interfering packets from other networks and attacking noise packets. Second, there exists the probability that the message packet is captured in the presence of interfering packets from other networks. Third, there exists the probability that the message packet is captured in the presence of other attacking noise packets. Fourth, the probability that the message packet is captured in the presence of other interfering message packets from the same network exists. Therefore, the probability that a message packet is successfully transmitted can be written as

\[
P_{Su} = \exp\left(-\frac{J/L}{G + I + J}\right)
\]  

(11)

According to our assumption, the power distribution of a message packet, the power distribution of an interfering packet from other networks and the power distribution of an attacking packet are the same. The capture effect of a message packet in the presence of interfering packets from other networks is defined in the following way. In case of a message packet collision with interfering packets from other networks, a message test packet is captured if its power is \( z_f \) times higher than the combined power of all interfering packets from other networks transmitted on the same slot as message (selected by receiver) packet is being transmitted, during a 'certain section of time slot’, to lock the receiver. Note that, capture ratio \( z_f \) and ‘certain section of time slot’ both are affected by modulation and coding technique [34]. Using the procedure presented in Sarker and Mouftah [32], it can be shown that the probability of a message packet is captured against all interfering packets from other network transmitted to the same slot is

\[
P_{CA} = \exp\left(-\frac{J/L}{1 + 1/z_f}\right)
\]  

(12)

The capture effect of a message packet in the presence of attacking packets is defined in the following way. In case of a message packet collision with attacking packets, a message test packet is captured if its power is \( z_a \) times higher than that of all attacking interfering packets transmitted on the same slot as message (selected by receiver) packet is being transmitted, defined as the attacking packet capture ratio, during a
The evaluation procedure of "z_m" is presented in Sarker and Mouftah [32]. At the same way, a message test packet is captured, if its power is z_m times higher than that of all other interfering packets transmitted from the same network defined as the attacking packet capture ratio, during a 'certain section of time slot', to lock the receiver. The probability that a message packet is captured against all interfering packets transmitted from the same network is [32,34]

\[ P_{CM} = \exp\left( -\frac{G/L}{1 + 1/z_m} \right) \] (13)

Finally the probability of success of a message packet in the presence of interfering packets transmitted from the same network, attacking noise packets and interfering packets transmitted from the same network is

\[ P(Su) = P_M * P_{CL} * P_{CA} * P_{CM} = \frac{G}{G + I + J} \exp\left( -\frac{I/L}{1 + 1/z_f} \right) \times \exp\left( -\frac{J/L}{1 + 1/z_m} \right) \] (14)

The probability of failure of any message packet is \( 1 - P(Su) \). This unsuccessful part \( \frac{I}{L}(1 - z_f)(1 - P(Su)) \) will be transmitted during first retransmission time. The probability of two successive failures is \( (1 - P(Su))^2 \). So the second time retransmission part is \( \frac{I}{L}(1 - z_f)(1 - P(Su))^2 \), and so on. In general, kth time retransmission part is \( \frac{I}{L}(1 - z_f)(1 - P(Su))^k \). Let the total number of retransmissions of a packet be \( r \) (one transmission followed \( r \) retransmission trials). The total mean offered traffic from all active users is then given by

\[ \frac{G}{L} = \sum_{k=0}^{\infty} \frac{\hat{I}}{L}(1 - z_f)[1 - (1 - P(Su))^k] \] (15)

Simplifying Eq. (15) and combining with Eq. (14), we can write

\[ \frac{G}{L}P(Su) = \frac{\hat{I}}{L}(1 - z_f)[1 - (1 - P(Su))^{1+r}] \Rightarrow \frac{G}{L} = \frac{G}{G + I + J} \times \exp\left( -\frac{I/L}{1 + 1/z_f} \right) \exp\left( -\frac{J/L}{1 + 1/z_m} \right) \times \exp\left( -\frac{I/L + J}{1 + 1/z_f} \right) \exp\left( -\frac{J/L}{1 + 1/z_m} \right) \times \frac{\hat{I}}{L} \exp\left( -\frac{I/L + J}{1 + 1/z_f} \right) \exp\left( -\frac{J/L}{1 + 1/z_m} \right) \] (16)

Eq. (16) is the basic equation of retransmission cut-off and new packet rejection algorithm of multiple L-channels Slotted ALOHA in the presence of interfering packets transmitted from other networks and attacking noise packets. The probability of success of L-channel Slotted ALOHA system in the presence of interfering packets transmitted from other networks and attacking noise packets is derived in Eq. (14). The throughput per slot of L-channel Slotted ALOHA system is defined as the multiplication of average traffic arrival rate per time slot and the probability of success in the presence of interfering packets transmitted from other networks and attacking noise packets. Thus, the throughput is

\[ S = \frac{G}{L}P(Su) = \frac{G^2}{L(G + I + J)} \exp\left( -\frac{I/L}{1 + 1/z_f} \right) \exp\left( -\frac{J/L}{1 + 1/z_m} \right) \times \exp\left( -\frac{G}{G + I + J} \right) \left(1 - \frac{1 - G}{G + I + J} \right)^{\frac{I}{L} + J} \] (17)

Eq. (17) is the basic equation for the throughput of a message packet. Articulately, the new packet generation rate \( \hat{I} \), number of channels \( L \), new packet rejection probability \( z_f \), capture ratios, \( z_m \), interfering packets from other networks' generation rate, \( I \), attacking signal generation rate, \( J \), and number of retransmission trials, \( r \), play important role in this equation.

Fig. 2 shows the throughput of Slotted ALOHA in the presence of interfering packets from other networks and attacking signals. But in this section, we will limit our discussion only to the effect of L-channels and capture ratios. Therefore, we will consider only the first two methods of secured transmission in Slotted ALOHA. The first method is to use multiple channels and the second method is to lower the capture ratios.

Fig. 2 shows the throughput per slot, \( S \) with the variation of aggregate message packet arrival rate, \( G \) for different values of attacking packets rates of \( J \). From Fig. 2 we can make the following conclusions:

1. The throughput per slot \( S \) of 1-channel without capture effects, \( z_m = \infty, z_f = \infty, z_m = \infty \), Slotted ALOHA system is very low in the presence of interfering signals from other networks and attacking noise packet signal (Fig. 2a). Because of that the current 1-channel without capture effects Slotted ALOHA based networks [9–17] can be shut down very easily. A lower message capture ratio, \( z_m = 1 \), can increase the channel throughput significantly at all traffic load (Fig. 2c).

2. A lower interfering capture ratio, \( z_f = 1 \), can increase the channel throughput slightly. A lower interfering capture ratio is only effective, if the interfering signals rate from other networks, \( I \) is high (Fig. 2d comparing with Fig. 2c).

3. Similarly, a lower attacking capture ratio, \( z_f = 1 \), can increase the channel throughput slightly. If the attacking signals rate, \( J \) is high only then a lower attacking capture ratio is effective (Fig. 2e comparing with Fig. 2d).

4. If 5-channels are used instead of 1-channel then the throughput per slot increases significantly, even under the high interfering signals from other networks and attacking signals (Fig. 2f comparing with Fig. 2b).

5. Since the throughput per slot, \( S \), does not collapse even with a high interfering signals rate from other networks, \( I \) and attacking noise packet generation rate, \( J \), with a lower message capture ratio, \( z_m = 1 \), the security of Slotted ALOHA system can be enhanced by lowering the capture ratios Fig. 2c–e.

6. Since the throughput per slot, \( S \), does not collapse with a high message packet arrival rate, \( G \), even with a high interfering signal rate from other networks, \( I \) and a high attacking noise packet generation rate, \( J \), with a higher number of channels, \( L \), the security of Slotted ALOHA system can be enhanced using multiple L-Slotted ALOHA channels.
Differentiating Eq. (17) with respect to attacking noise packet generation rate, $J$, we obtain

$$\frac{dS}{dJ} = \exp\left(-\frac{J}{1+1/z_J}\right) \exp\left(-\frac{G/L}{1+1/z_m}\right) \left[ -\frac{1}{L(G+J+I)} \left( \frac{G}{G+J+I} \exp\left(-\frac{J}{1+1/z_a}\right) - \frac{G^4}{L(G+J+I)} \exp\left(-\frac{J}{1+1/z_a}\right) \right) \right]$$

It is clear from Eq. (18) that for any positive value of message packet generation rate, $G$, and interfering packets arrival rate from other networks, $I$, the throughput, $S$, decreases with the increase of attacking noise packet generation rate, $J$. Exactly in the same way, it can be shown that for any positive value of message packet generation rate, $G$, and the attacking noise packet generation rate, $J$, the throughput, $S$, decreases with the increase of interfering packets arrival rate from other networks, $I$. However, the numerical results of these two results have already been depicted in Fig. 2.

Differentiating Eq. (17) with respect to message packet generation rate, $G$, we get

$$\frac{dS}{dG} = \frac{1}{L} \exp\left(-\frac{J}{1+1/z_m}\right) \exp\left(-\frac{1}{1+1/z_a}\right) \left[ -\frac{1}{G+J+I} \left( \frac{G}{G+J+I} \exp\left(-\frac{1}{1+1/z_m}\right) + \frac{(G+J+I)(2G^2)}{(G+J+I)^2} \exp\left(-\frac{G}{1+1/z_m}\right) \right) \right]$$

$$\frac{dS}{dG} = \frac{1}{L} \exp\left(-\frac{J}{1+1/z_m}\right) \exp\left(-\frac{1}{1+1/z_a}\right) \left[ -\frac{1}{G+J+I} \left( \frac{G}{G+J+I} \exp\left(-\frac{1}{1+1/z_m}\right) + \frac{(G+J+I)(2G^2)}{(G+J+I)^2} \exp\left(-\frac{G}{1+1/z_m}\right) \right) \right]$$

7. There exists an optimum point where throughput per time slot, $S$, is maximum for given values of message packet generation rate, $G$, interfering signals rate from other networks, $I$, and attacking packet generation rate, $J$. 

- (a) 1-channel, without interference, without capture

- (b) $I=0.3$

- (c) message packet capture $z_m=1$

- (d) interfering packet capture $z_f=1$

- (e) attacking packet capture $z_a=1$

- (f) 5-channel, without capture

Fig. 2 Throughput per slot with the variation of message packet arrival rate.
Now putting the differentiation result Eq. (19) equal to zero, we obtain the optimum value of the message packet arrival rate from all active mobile nodes,

\[ G_{\text{opt}} = \frac{L(1 + 1/z_m) - (J + I)}{2} \]

Using the value of optimum message packet arrival rate, \( G_{\text{opt}} \) in Eq. (17), we can obtain the optimum throughput per time slot as

\[ \frac{S_{\text{opt}}}{L(G_{\text{opt}} + J + I)} \exp \left( -\frac{J}{1 + 1/z_m} \right) \exp \left( -\frac{I}{1 + 1/z_m} \right) \exp \left( -\frac{G_{\text{opt}}/L}{1 + 1/z_m} \right) \]

\[ = \frac{\left[ L(1 + 1/z_m) - (J + I) \right] + \sqrt{\left[ L(1 + 1/z_m) - (J + I) \right]^2 + 8L(J + I)(1 + 1/z_m)}^2}{2L \left( L(1 + 1/z_m) + (J + I) + \sqrt{\left[ L(1 + 1/z_m) - (J + I) \right]^2 + 8L(J + I)(1 + 1/z_m)} \right)} \]

\[ \times \exp \left( -\frac{J}{1 + 1/z_m} \right) \exp \left( -\frac{I}{1 + 1/z_m} \right) \exp \left( -\frac{G_{\text{opt}}/L}{1 + 1/z_m} \right) \]

\[ \frac{\left[ L(1 + 1/z_m) - (J + I) \right] + \sqrt{\left[ L(1 + 1/z_m) - (J + I) \right]^2 + 8L(J + I)(1 + 1/z_m)}}{2L(1 + 1/z_m)} \]  

\[ (20) \]

The optimum throughput per time slot is shown in Figs. 3 and 4 using Eq. (21). Figs. 3 and 4 show that the optimum throughput can be increased significantly using lower capture ratios and multiple channels. The conclusions of Figs. 3 and 4 are almost same as the conclusions drawn from Fig. 2.

---

![Fig. 3](image-url)  
The maximum throughput, \( S_{\text{opt}} \) with the variation of number of channels \( L \).
Now the question that may arise is: what is the optimum number of channels, $L$, that provides maximum throughput. To answer this question, the optimum $L$ can be obtained by setting Eq. (19) is equal to zero. Therefore, the optimum number of channels is

$$L_{\text{opt}} = \frac{G(G + J + I)}{(1 + 1/z_m)(G + 2J + 2I)} (22)$$

The optimum number of channels, $L_{\text{opt}}$, increases further with the increase of aggregate message traffic arrival rate, $G$. The $L_{\text{opt}}$, increases further with the increase of

$$P_{\text{opt}}(\text{Su}) = \frac{S_{\text{opt}}}{G_{\text{opt}}} = \frac{G_{\text{opt}}}{G_{\text{opt}} + J + I} \exp \left( -\frac{J/L}{1 + 1/z_m} \right) \exp \left( -\frac{I/L}{1 + 1/z_f} \right) \exp \left( -\frac{G_{\text{opt}}/L}{1 + 1/z_m} \right)$$

$$= \frac{L(1 + 1/z_m) - (J + I) + \sqrt{L(1 + 1/z_m) - (J + I)^2 + 8L(J + I)(1 + 1/z_m)}}{L(1 + 1/z_m) + (J + I) + \sqrt{L(1 + 1/z_m) - (J + I)^2 + 8L(J + I)(1 + 1/z_m)}} \times \exp \left( -\frac{J/L}{1 + 1/z_m} \right) \exp \left( -\frac{I/L}{1 + 1/z_f} \right) \exp \left( -\frac{G_{\text{opt}}/L}{1 + 1/z_m} \right)$$

$$= \frac{\{L(1 + 1/z_m) - (J + I)\} + \sqrt{\{L(1 + 1/z_m) - (J + I)^2 + 8L(J + I)(1 + 1/z_m)\}}}{2L(1 + 1/z_m)}$$

$$= \frac{\{L(1 + 1/z_m) - (J + I)\} + \sqrt{\{L(1 + 1/z_m) - (J + I)^2 + 8L(J + I)(1 + 1/z_m)\}}}{2L(1 + 1/z_m)}$$

$$= \frac{\{L(1 + 1/z_m) - (J + I)\} + \sqrt{\{L(1 + 1/z_m) - (J + I)^2 + 8L(J + I)(1 + 1/z_m)\}}}{2L(1 + 1/z_m)}$$

$$= \frac{\{L(1 + 1/z_m) - (J + I)\} + \sqrt{\{L(1 + 1/z_m) - (J + I)^2 + 8L(J + I)(1 + 1/z_m)\}}}{2L(1 + 1/z_m)}$$

message packet capture ratio, $z_m$. However, the same decreases with the increase of interfering packet arrival rate from other networks, $I$, or/and attacking packet arrival rate, $J$.

**Security improvement by limiting the number of retransmission trials**

In a normal data transmission system, every packet must be transmitted successfully. On the other hand, in the case of contention based access protocol or for real-time data transmission, we can cut the retransmission number, which will avoid the undesirable stability or security problem of Slotted ALOHA [35]. Over a long time period, the total offered traffic load $G$ will have an optimum value $G_{\text{opt}}$ depending on the other parameters like new packet generation rate per time slot and the number of retransmission trials. In the case of access or real-time traffic transmission packets are identical in nature for each user and the access procedure is limited by time. For a secured operation of $L$-channels Slotted ALOHA type system, with a higher value of new packet generation rate per time slot, the retransmission trials should be controlled. The purpose of the retransmission trial control is to get the optimum value of offered traffic load from all users $G_{\text{opt}}$, which will make the system secured or stable. Here, in this paper a simplified assumption is considered: if the traffic generation rate from all active users in a given time slot is less than or equal to the optimum packet arrival per time slot, the system is secured. This assumption is reasonable for Slotted ALOHA system [33].

The optimum throughput per slot of $L$-channels Slotted ALOHA system with and without limiting the number of retransmission trials can be obtained from Eqs. (18 and 21) as

$$S_{\text{opt}} = \frac{S_{\text{opt}}}{L} \left[ 1 - \{1 - P_{\text{opt}}(\text{Su})\}^{e+1} \right]$$

where the values of $S_{\text{opt}}$ and $P_{\text{opt}}(\text{Su})$ are given in Eqs. (23) and (24), respectively. The main purpose of our system model is to maximize the throughput per slot, $S$ by adjusting the transmission trials, $r$ and the new packet generation rate per slot, $\lambda/L$, for a given interfering packet arrival rate from other networks, $I$, and attacking packet arrival rate, $J$. We have already derived the maximum throughput of $L$-channels Slotted ALOHA system $S_{\text{opt}}$ in Eq. (23). And it occurs when the aggregate traffic generation rate, $G_{\text{opt}}$, which is shown in Eq. (20).

Eq. (25) is the basic equation for the secured transmission method. The secured transmission method can be stated as follows: For a call establishment system design or for a real-time traffic transmission, the time out is the most important parameter. This time out is the time to transmit the access information from mobile to base station plus the switching time. From the value of the time to transmit the access information or real-time transmission plus the propagation delay, we can find the maximum allowable retransmission trials, $r$, i.e., how many
retransmission trials are possible for a given time. From this value of \( r, L, I, J, z_m, z_f \) and \( z_m \) we can find the optimum new packet generation rate per time slot, \( \lambda_{\text{opt}}/L \)per time slot using Eqs. (23)–(25). Fig. 5 shows the variation of optimum new packet generation rate per time slot, \( \lambda_{\text{opt}}/L \), with the variation of number of channels, \( L \), using Eqs. (23)–(25).

Without any retransmission attempts \( (r \to 0) \) the optimum new packet generation rate per time slot can be obtained using Eq. (25) as

\[
\left( \frac{\lambda_{\text{opt}}}{L} \right)_{r \to 0} = \frac{S_{\text{opt}}}{P_{\text{opt}}(\text{Su})} = \frac{L(1 + 1/z_m) - (J + I) + \sqrt{[L(1 + 1/z_m) - (J + I)]^2 + 8L(J + I)(1 + 1/z_m)}}{2L}
\]

Eq. (26) shows the limit of the proposed solution with retransmission cut-off scenario.

In the other extreme, without any retransmission cut-off \( (r \to \infty) \) the optimum new packet generation rate per time slot can be obtained using Eq. (25) as

\[
\left( \frac{\lambda_{\text{opt}}}{L} \right)_{r \to \infty} = S_{\text{opt}}
\]

where the value of \( S_{\text{opt}} \) is given in Eq. (23). Therefore, the security improvement area by limiting the number of retransmission trials, \( r \) is

\[
Ar = \left( \frac{\lambda_{\text{opt}}}{L} \right)_{r \to 0} - \left( \frac{\lambda_{\text{opt}}}{L} \right)_{r \to \infty} = \frac{L(1 + 1/z_m) - (J + I) + \sqrt{[L(1 + 1/z_m) - (J + I)]^2 + 8L(J + I)(1 + 1/z_m)}}{2L} - S_{\text{opt}}
\]

The shaded parts indicated in Fig. 5 show the secured region by limiting the number of retransmission trials, \( r \). The lower most parts of the figures show the secured transmission region without limiting the number of retransmission trials. Increasing the number of channel, \( L \) or/and reducing the capture ratios, \( z_m, z_f \) and \( z_m \) are not enough to obtain a higher secured transmission operating region. Limiting the number of retransmission trials can increase the secured transmission operating region significantly.

**Security improvement by new packet rejection**

The main purpose of this paper is to obtain the secured transmission of L-channel Slotted ALOHA system. It is already shown that if L-channel Slotted ALOHA system provides maximum throughput then the system is secured. If limiting the retransmission trials is not sufficient for obtaining a secured stabilized L-channel Slotted ALOHA system, then it can be achieved by the expense of newly generated packet rejection.

The maximum throughput per slot of a L-channel Slotted ALOHA is \( S_{\text{opt}} \) is derived in Eq. (23), and it occurs when the aggregate traffic generation rate, \( G_{\text{opt}} \), which is shown in Eq. (20). The aggregate message packet generation rate per time slot \( G/L \), by limiting the number of retransmission trials and new packet rejection is shown in Eq. (16). Combining Eqs. (16 and 17) and after simplification we can write

\[
\frac{\lambda_{\text{opt}}}{L} = \left( \frac{1}{1 - z} \right) \frac{S_{\text{opt}}}{1 - \{1 - P_{\text{opt}}(\text{Su})\}^{1/r}}
\]

The secured operating region of L-channel Slotted ALOHA system with and without limiting the retransmission trials is depicted in Fig. 6. Please note that here the y-axis should be multiplied by \( X = \frac{G_{\text{opt}}}{1 - z} \). The value of \( L_{\text{opt}} \) is given in Eq. (20).

Fig. 6 shows clearly that by increasing the value of \( z \) (new packet rejection probability), the secured operating regions with and without retransmission cut-off can be increased significantly.

From Fig. 6, it can be said that the maximum value of the new packet generation rate per slot, \( \lambda_{\text{opt}}/L \) with new packet rejection is

\[
LR = \frac{S_{\text{opt}}}{1 - z}
\]

Comparing Eqs. (26) and (30), the upper limit of the new packet generation rate per slot with new packet rejection is \( 1/(1 - z) \) times higher than that of the without new packet rejection.

On the other hand the new packet generation rate per slot, without limiting the number of retransmission trials with new packet rejection is

\[
\left( \frac{\lambda_{\text{opt}}}{L} \right)_{r \to \infty} = \frac{L(1 + 1/z_m) - (J + I) + \sqrt{[L(1 + 1/z_m) - (J + I)]^2 + 8L(J + I)(1 + 1/z_m)}}{2L} - S_{\text{opt}}
\]

It can be said that the new packet generation rate per slot without limiting the number of retransmission trials with new packet rejection is \( 1/(1 - z) \) times higher than that of the without new packet rejection, by comparing Eqs. (27) and (31).

From Fig. 6, we can conclude that, the aggregate message packet generation rate, \( G \), never reaches its optimum point, if the new packet generation rate per slot, \( \lambda_{\text{opt}}/L \), is less than \( LR \) packet per time slot. The reason is that, we started to get the result of Eq. (31) with the aggregate message packet generation rate, \( G_{\text{opt}} \). So, it is unnecessary to control the retransmission attempt for a secured operation of L-channels Slotted ALOHA, if the new packet generation rate per slot, \( \lambda_{\text{opt}}/L \), is less than \( LR \) packet per time slot, where \( z \) is the newly generated packet rejection probability.

**Conclusions**

In this paper, an analytical approach for secured operating regions of Slotted ALOHA in the presence of interfering signals from other networks and DoS attacking signals has been
The performance evaluations presented in this paper are based on the numerical analysis.

The security improvement of $L$-channels Slotted ALOHA in the presence of interfering signals from other networks and random attacking noise packets signals is studied in this paper. The current security protected measures such as encryption makes the packets unreadable by unauthorized users. The authentication technique is used to protect the system from illegal users and authorization separates the legal users. However, in a Slotted ALOHA based network, the interfering signals from other networks and the random packet destruction DoS attacking noise packets may collide with message packets and reduces the secured transmission. Therefore, the current security measures such as encryption, authentication and authorization cannot prevent those types of attack. One of the main drawbacks of Slotted ALOHA protocol is its excessive collisions.

In this paper, we have used four different techniques for security improvement of Slotted ALOHA by reducing the collisions. Since the interfering signals from other networks and the random packet destruction DoS attacking noise packet increase the collision, we intend to use multiple channels in the Slotted ALOHA protocol to reduce the collisions in the first technique. The use of multiple channels in the Slotted ALOHA protocol reduces three types of packet collisions. First type of collision is the collision between two or more message packets. The second type of collision is the collision between a message packet and one or more interfering packets from other networks. The third type of collision is the collision between a message packet and one or more other attacking noise packets.

In the second security improvement technique, we have shown the effects of capture ratios in the presence of interfering signals from other networks and the random packet destruction DoS attacking noise packet. A lower message capture ratio can increase the throughput and maximum throughput significantly. A lower interfering capture ratio can increase the throughput and maximum throughput only if the rate of interfering signals from other networks’ packets rate is high. Exactly same conclusion is applied for a lower attacking capture ratio.

In the third technique, we have used retransmissions cut-off by limiting the number of retransmission trials. The retransmissions cut-off technique can limit the aggregate packet flow and form the optimum message packet flow in the presence of interfering signals from other networks and the attacking noise packet. It is possible that the third technique called retransmissions cut-off technique is not enough to control the flow of message packets. Because of that the fourth technique called new packet rejection probability is introduced. The secured
operating regions can be increased $1/(1 - \alpha)$ times by using this fourth technique. Where $\alpha$ is the new packet rejection probability.

Fig. 5  Security improvement by limiting the retransmission trials.

Fig. 6  Secured and unsecured operating regions of multichannel L-Slotted ALOHA in the presence of interfering signals from other networks and attacking signals.

References

[33] Sarker JH. Stable and unstable operating regions of Slotted ALOHA with number of retransmission trials and number of power levels. IEE proceedings, communications 2006;153(3): 355–65.