Zorica B. NIKOLIĆ, Marko M. SMILIĆ

E-COMMERCE PHYSICAL LAYER SECURITY: PERFORMANCE ANALYSIS OF EAVESDROPPER ATTACK IN WIRELESS NETWORKS

Abstract: The evolution of technology and the internet led to the opening of infinite ways to engage with consumers worldwide. The idea of everything taking place online is now applicable for the finance and banking sector as well. The system of online wallets and e-transactions have become very common as a mode of payment. But handling money on a network is also dangerous as hackers may break into the firewall. The security wireless communication in e-commerce has received extensive attention recently. This paper offers an analytical framework to investigate the eavesdropping attacks over wireless communication link. Eavesdropping attack, as one of typical security threats in wireless communication systems, has attracted considerable attention. We will observe the physical layer security of an arbitrarily dimensioned wireless network in the presence of an unauthorized attacker. In this paper, we will explain different models of eavesdropping and attacks. Also, we will consider basic performance of the system such are secrecy outage probability (SOP), strictly positive secrecy capacity (SPSC) and average secrecy capacity (ASC) based on a probability density function (PDF) and specific cumulative distribution function (CDF).

Keywords: e-commerce; physical layer security; intercept probability; secrecy capacity

JEL Klasification: M1, M15, L86, H56

1. INTRODUCTION

The development of the Internet, smartphones and applications has significantly influenced the change in people’s consciousness. In order to get the desired information, schedule a vacation, make a purchase or access entertainment content, it only takes one click. Large IT companies and internet providers have enabled us to get everything immediately, without thinking about the potential risks and problems we might encounter[1]. Although from the point of view of end users the use of services seems fast and simple, IT companies and Internet providers face various challenges every day that they have to solve in order to provide the best quality of service[2].

The development of IT technologies has also changed the way companies operate. The possibility of paying by card, electronic transfer of money from account to account, shopping and paying over the Internet are just some of the advantages made possible by using IT technologies. This especially applies to e-commerce,
where online transactions are carried out between the customers and vendors on a daily basis[3].

The biggest challenge that e-commerce faces is the problem of security. When conducting transactions, exchanging data between customers and vendors, there is a risk of potential attack. For example, the eBay database hack – in which personal details belonging to 145 million users were stolen – is probably one of the biggest attack on e-commerce system. In order to ensure security during e-commerce, special attention is focused on threat analysis and threat protection. The first step in protection against threats is the analysis of hardware, software, networks, but also employees of companies who have access to sensitive data[4], [5].

Hardware devices do not mean only devices that access e-commerce applications (mobile devices, client computers, etc.), but also devices that are used for network traffic routing (routers, switches, servers). The development of various web and mobile applications used by both customers and vendors is also part of e-commerce protection. Licensed operating systems, licensed software, reliable web servers software are excellent choices for avoiding attacks. As data exchange and transactions are carried over the network, it is very important to monitor who is accessing those networks. Company employees have access that they can abuse or simply, due to carelessness, they can compromise sensitive data. Although the term network most often refers only to the Internet and/or communication between client and employer and/or communication between software when collecting and storing data in a database, communication and data transmission via wireless networks is often overlooked[6]–[9].

In this paper, we will consider the physical layer security of wireless network in the presence of an unauthorized attacker. We will present various scheduling schemes in order to enhance the secure transmission of reliable links impaired by generalized fading channels. Also, we will consider basic performance of the system such are secrecy outage probability (SOP), strictly positive secrecy capacity (SPSC) and average secrecy capacity (ASC) based on a probability density function (PDF) specific cumulative distribution function (CDF) and well knowns definitions from theory of information.

The work is organized in the following way. In Introduction section importance of IT technologies in e-commerce is presented. A basic analysis of threats and protection against threats is given. The motivation and results that will be discussed are highlighted.

In Literature review section, an overview of published scientific works dealing with the analysis of security in e-commerce is given. Models of protection against threats and attacks are presented in more detail.

In the System model section, different models of wireless communication systems and eavesdropping attack models are explained.

In the Performance analysis section, basic performance measures such as secrecy outage probability (SOP), strictly positive secrecy capacity (SPSC) and average secrecy capacity (ASC), are theoretically explained and mathematically defined.

In the Results section, the results obtained in the previous section are graphically presented.

2. LITERATURE REVIEW

In this chapter, we will present different studies related to different types of protection against threats, attacks and eavesdropping.

In his study, Singh [10]primarily emphasized the protection of applications through authentication, integrity, non-repudiation, access control and availability. Furthermore, in his study he presented basic security threats. Table 1 presents the security functions and their purpose.

Badotra and Sundas[11]in their study show how to ensure security. They proposed several ways such as encryption, digital signature and digital certificates. They paid special attention to cyber-attack where they singled out: Financial fraud attack, Brute force attack, Bot
attack, Spam attack, Cross-site scripting (XSS) attack, Trojan horses attack, Malware attack, Phishing attack, DDoS attack and SQL injection attack.

<table>
<thead>
<tr>
<th>No</th>
<th>Function</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Authentication</td>
<td>Aims to detect masquerade. Provides assurance that a communicating entity is the one that it claims to be.</td>
</tr>
<tr>
<td>2</td>
<td>Integrity</td>
<td>Aims to detect modification and replay. Provides assurance that data received are exactly as sent by the sender.</td>
</tr>
<tr>
<td>3</td>
<td>Non repudiation</td>
<td>Provides protection against denial by one entity involved in a communication of having participated in all or part of the communication. Two basic types: non-repudiation of origin and non-repudiation of delivery.</td>
</tr>
<tr>
<td>4</td>
<td>Access control</td>
<td>Aims to prevent unauthorized access to resources.</td>
</tr>
<tr>
<td>5</td>
<td>Availability</td>
<td>Should be available to authorized user whenever they need it over the network.</td>
</tr>
</tbody>
</table>

Dijesh, Babu and Vijayalakshmi[12] based their study on enhancement of e-commerce security through asymmetric key algorithm. They are represented two different algorithms: Fernet cipher algorithm and RSA algorithm. Both of these algorithms are based on encryption and decryption with the help of private and public key of receiver and sender.

The security of the physical layer is also very important in e-commerce because data is most often transmitted via wireless networks. As data is transmitted through the medium, it is exposed to various effects that can affect its quality, reliability and security [13]. The influence of fading, shadow effect, scattering, signal blocking, atmospheric conditions degrade the transmitted information and thus enable attackers and eavesdroppers to intercept it. In order to make the transmission of information safe, various measures have been proposed that indicate the security of the system, such as ASC, SPSC and SOP which have been investigated in [14]–[17].

By considering these performances, attacks can be proactively prevented. The attack can be active or passive. In case of passive attack, attacker attempts to learn or make use of information from the system but does not affect system resources. In case of active attack, attacker attempts to alter system resources or affect their operation.

Various data transmission systems have been investigated in the literature. Traditional radio frequency (RF) systems are investigated in [18]–[21], while modern Free Space Optic (FSO) systems are investigated in [22]–[29].

3. SYSTEM MODEL

Analysis of physical layer security performance depends on the system model we are considering. If we consider a system model where information is transmitted by an RF signal that is influenced by fading, scattering and the shadow effect, the system model can be shown as in Figure 1[16].

On the other hand, we can consider the system model shown in [25] where we have three different scenarios depending on the position of the eavesdroppers shown in Figure 2. As you can see from the picture, the first scenario (A) considers the case when the eavesdropper is near the legitimate receiver. The second
scenario (B) considers the case when the eavesdropper is near the legitimate transmitter. The third scenario (C) considers the case when the eavesdropper is far from both the legitimate transmitter and the legitimate receiver. For all three cases, information is transmitted through the FSO signal.

\[ y_D = h_D x + z_D \]
\[ y_E = h_E x + z_E \]  

where \( x \) represents transmitted signal, \( h_D \) and \( h_E \) represents fading channel of direct link and eavesdropper link and \( z_D \) and \( z_E \) represents AWGN for direct link and eavesdropper link, respectively. Various statistical fading distributions can be used for channel modeling. In this paper, we use the general Málaga distribution described in [30], [31].

### 4. PERFORMANCE ANALYSIS

Insight into the measures of the system performance enables us to analyze and predict the behavior of that system.

We have already said that safe and secure transmission of information is of great importance for e-commerce. If the information is transmitted from the transmitter to the legitimate receiver and the eavesdropper does not have access to that information, then we define a measure called average secrecy capacity defined as [24], [25], [32]:

\[ C_S(\gamma_D, \gamma_E) = \left[ \ln (1 + \gamma_D) - \ln (1 + \gamma_E), 0 \right] \]  

where \( \gamma_D \) and \( \gamma_E \) represents instantaneous received SNR of legitimate receiver and eavesdropper, respectively. To calculate ASC, equation (2) can be written:

\[ C_S = \int_0^{\infty} \ln (1 + \gamma_D) f_{\gamma_D}(\gamma_D) F_{\gamma_D}(\gamma_D) d\gamma_D \]
\[ + \int_0^{\infty} \ln (1 + \gamma_E) f_{\gamma_E}(\gamma_E) F_{\gamma_D}(\gamma_E) d\gamma_E \]
\[ - \int_0^{\infty} \ln (1 + \gamma_E) f_{\gamma_E}(\gamma_E) d\gamma_E \]  

\( f_{\gamma_D}(\gamma_D) \) and \( f_{\gamma_E}(\gamma_E) \) represents PDF of fading channel for direct link and eavesdropper link and \( F_{\gamma_D}(\gamma_D) \) and \( F_{\gamma_E}(\gamma_D) \) represents CDF for direct link and eavesdropper link, respectively.

Probability that the instantaneous secrecy capacity is below given threshold rate \( R_s \) represents secrecy outage probability and can be defined as [33]:
The strictly positive secrecy capacity (SPSC) is the probability that the secrecy capacity is always greater than the zero [34].

\[
SPSC = \Pr[C_S(\gamma_D, \gamma_E) > 0] \tag{6}
\]

or

\[
SPSC = \int_{0}^{\infty} \int_{0}^{\infty} f_{\gamma_D}(\gamma_D) f_{\gamma_E}(\gamma_E) d\gamma_D d\gamma_E \tag{7}
\]

5. RESULTS

In this section we present graphically results obtained from equations (3), (5) and (7). The parameter values used to obtain the results are defined in the paper [31] for the case when we consider moderate atmospheric turbulence for the Málaga model and the pointing error between the transmitter and the receiver is negligible.

Figure 4 depicts average secrecy capacity versus electrical SNR of legitimate receiver for different values of electrical SNR of eavesdropper.

![Fig. 4. Average secrecy capacity](image)

With the increase in the electrical SNR level of the legitimate receiver \(\mu_D\), the secret capacity of the channel also increases. Also, with a decrease in the level of the electrical SNR of the eavesdropper \(\mu_E\), the secret capacity of the channel increases. As the electrical SNR represents the level between signal and noise, it is logical that a lower level of the electrical SNR of the eavesdropper automatically means a greater secret capacity. For example, if we consider an electrical SNR level of a legitimate receiver \(\mu_5 = 12\, \text{dB}\), we achieve a secrecy capacity of 12 [bits/s/Hz] for \(\mu_E = 5\, \text{dB}\), 1.75 [bits/s/Hz] for \(\mu_E = 7\, \text{dB}\), and 1.5 [bits/s/Hz] for \(\mu_E = 10\, \text{dB}\).

Figure 5 depicts secrecy outage probability versus electrical SNR of legitimate receiver for different values of electrical SNR of eavesdropper.

![Fig. 5. Secrecy outage probability](image)

Similar conclusions can be made from Figure 5. With the increase in the electrical SNR level of the legitimate receiver \(\mu_D\), the secret outage probability of the channel decreases. Also, with a decrease in the level of the electrical SNR of the eavesdropper \(\mu_E\), the secret capacity of the channel decreases. The probability that the instantaneous secrecy capacity is below the threshold rate decreases with the increase in the signal quality of the legitimate receiver.

Figure 6 shows strictly positive secrecy capacity versus electrical SNR of legitimate receiver for different values of electrical SNR of eavesdropper.

![Fig. 6. Strictly positive secrecy capacity](image)

With the increase in the electrical SNR level of the legitimate receiver \(\mu_D\), strictly positive secrecy capacity also increases. Also, with a decrease in the level of the electrical SNR of
the eavesdropper $\mu_D$, strictly positive secrecy capacity increases.

Fig. 6. Strictly positive secrecy capacity

6. CONCLUSION

The development of IT technologies led to the development of e-commerce. The exchange of sensitive data and money that takes place is subject to various threats and attacks.

The paper reviews the most common methods of attacks on software, hardware and networks used in e-commerce, as well as solutions to protect against these threats.

The main goal of this work was the security of the physical layer when exchanging information using wireless communication systems in presence of eavesdropper. Performance measures have been considered for such a system, through which we can prevent potential attacks and threats. From the obtained results, we saw that the average secrecy capacity, strictly positive secrecy capacity and secrecy outage probability have better performance with the increase in the quality of the received signal on the legitimate receiver.

The influence of the quality of the received eavesdropping signal is also shown. If the eavesdropper has a better received signal quality, there are greater chances of intercepting the information being transmitted.

ACKNOWLEDGMENT

This research was supported by Ministry of Education, Science and Technological Development of the Republic of Serbia, under project III-44006.

REFERENCES


