Optik 125 (2014) 5647–5650

Contents lists available at ScienceDirect

Optik

journal homepage: www.elsevier.de/ijleo

A secure transmission scheme on link level for optical fiber communication systems

Shaojing Su, Jing Zhou, Zhiping Huang*, Yimeng Zhang, Zhen Zuo

College of Mechatronic Engineering and Automation, National University of Defense Technology, Changsha 410073, Hunan Province, PR China

ARTICLE INFO

Article history:
Received 23 September 2013
Accepted 25 May 2014

Keywords:
Optical fiber communications
Blind frame synchronizations
Forward error-correction (FEC)
Military communications

ABSTRACT

In secure communication systems, a very important problem is how to prevent wiretapping. Lots of researches on cryptography give good solutions on secure communications. But if a wire tapper can detect the existence of the transmitted information and get enough eavesdropped frames, cryptanalysis techniques can help to blindly recover the frame structures, error-control coding parameters and passwords. In this paper we propose a novel secure transmission scheme on the link level for optical fiber communication systems. Based on the blind frame synchronization technique, we propose to drop the traditionally strict frame structures in fiber communications and conceal the error-correcting-encoded blocks among random data, so that wire tappers cannot get enough coded packets to analyze and recover the transmitted information. Therefore, the proposed method is very suitable for secure communications and military communications.

© 2014 Elsevier GmbH. All rights reserved.

1. Introduction

In secure communication systems, legal users hope to conceal the transmitted information to avoid wiretapping. The developing of cryptology on communications increases the difficulty of understanding the information for an eavesdropper [1–4]. However, the cryptanalysis is always bringing challenges to secure communications [5,6]. In traditional fiber communication systems, the transmitted data stream always has strict structures, so a wire tapper can easily detects the existence of the transmitted information and get enough eavesdropped frames. Based on the eavesdropped data, cryptanalysis techniques can help to blindly recover the frame structures, error-control coding parameters and passwords. But if the packets is hidden into a random noise sequence and the frame synchronization word is removed, it is difficult for the eavesdropper to discover the existence of one's interested information and hard to synchronize to the transmitter. Without synchronization words, legal receivers must synchronize the transmitted packets blindly. In this paper we propose a valid transmission scheme to make the legal receiver can blindly synchronize the transmitted packets and bring extreme difficulties to wire tappers on detecting the existence of the transmitted information and obtaining enough valid frames. And in this paper we assume that the optical fiber is a binary symmetry channel.

The remaining of the paper is organized as follows. In Section 2 we list the safety risks of traditional communication systems. According to the safety risks, we propose a new secure transmission scheme in Section 3. Section 4 shows the simulation results of the proposed methods. Finally we give the conclusions in Section 5.

2. Safety risks of traditional fiber communications

Fig. 1 depicts a typical frame structure in optical transport network (OTN) [7]. The data stream is transmitted packet-by-packet with the frame structure in Fig. 1. The frame alignment signal (FAS) in Fig. 1 is a synchronization word (SW), which repeats in each frame. The overhead includes frame counters, service information and parity bits of error-control codes applied in the frames. Payload is the information to be transmitted.

This kind of frame structure is convenient for synchronizations between receivers and transmitters. But the strict format is also convenient for a wire tapper to eavesdrop the transmitted information. Even the forward-error-correction (FEC) parameters also might be blindly recognized and the wire tappers can get the low error rate data. Generally, the frame structure has following safety risks which are easily to be attacked.

(1) The FAS repeats periodically, which can betray the frame length and the starting positions of the eavesdropped streams [8–10].

* Corresponding author.
E-mail address: h.zhiping@hotmail.com (Z. Huang).

http://dx.doi.org/10.1016/j.ijleo.2014.06.061
0030-4026/© 2014 Elsevier GmbH. All rights reserved.

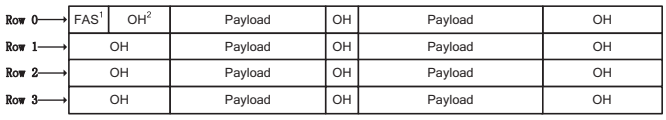

Fig. 1. A typical OTN frame structure.

(2) According to the FAS and frame length, if the data is coded by an error-correction code, a wire tapper can blindly recover the coding parameters, including type of codes, parity check matrix and positions of payload data and OH data in the frame structure [11–16]. According to the recovered coding parameters, the wire tapper can obtain error-corrected payload information.
(3) Finally, the payload data, which is usually not protected by effective interleaving, may be eavesdropped by illegal users. Although the payload data might be encrypted, the cryptogram parameters can also be attacked if the wire tapper gets enough payload data [5,6].

3. A secure transmission scheme on link level

3.1. General design

We have analyzed the safety risks of the frame structures of traditional optical communications in Section 2. In this section, we propose a secure transmission scheme on the link level to solve the problem of safety risks in order to avoid wire tapping. Aiming at the mentioned safety risks, we propose the following modifications to improve the security of transmission.

(1) We drop the FAS in the frame structure and propose a blind synchronization method. This modification makes sure that the recognitions of frame length and frame starting positions are more difficult to wire tappers, while the legal users can achieve synchronizations by employing the relationship between payload bits and parity bits.
(2) We do not transmit frames packet-by-packet. Instead, we insert random data among packets. The length of inserted random data is also selected randomly. According to the blind coding parameter recognition algorithms [11–16], a basic condition of recovering the coding parameters is by obtaining lots of valid codewords. Taking this modification, it is more difficult for a wire tapper to get enough codewords to analyze the coding parameters.
(3) We propose an effective interleaving scheme on the payload bits and parity bits to puzzle wire tappers.

3.2. Blind frame synchronization method

We propose to drop FAS, so we have to employ a blind frame synchronization method. To realize the blind fame synchronizations and reduce errors introduced in transmission, we can use error-correction codes to encode the transmitted information bits. The code length, interleaving approach and parity check matrices of the codes are known by legal receivers. Therefore, a legal receiver can firstly set an initial receiving position t and obtain all the codewords in the sequence from t to $t+l-1$, where l is the length of frames. We fill the codewords into an $n \times M$ matrix $\mathbf{C}$ column by column, where n is the length of the codewords and M is the number of codewords in a frame. Let $\mathbf{C}_i (1 \le i \le M)$ be a column of matrix $\mathbf{C}$ and $\mathbf{H}$ be the parity check matrix of the code. If the assumed frame starting position t is correct and no error occurs during transmission, $\mathbf{C}_i$ is a valid codeword and we have

$$\mathbf{H} \times \mathbf{C}_i = 0 \tag{1}$$

If the assumed starting position t is not correct, any column of $\mathbf{C}$ cannot form a valid codeword so the relationship $\mathbf{H} \times \mathbf{C}_i = 0$ is always not true. Let $\mathbf{h}_j (1 \le j \le n-k)$ be a row of $\mathbf{H}$, which has n–k rows and n columns and k is the dimension of the error-correction code, the probabilities of $\mathbf{h}_j \times \mathbf{C}_i = 0$ in correct and incorrect frame starting positions are different in a noisy channel. When the assumed starting position t is not correct, the bits in codewords have no constraint relation, so $\mathbf{h}_j \times \mathbf{C}_i$ can be considered to follow a binomial distribution with the parameter $p = 0.5$. So the mathematical expectation of the probability of $\mathbf{h}_j \times \mathbf{C}_i = 0$ is about 0.5 [17,18]. And if the starting position t is estimated correctly, that expectation is $[1-(1-2\tau)^w]/2$ [17,18], where τ is the cross-over probability of the channel and w is the Hamming weight of $\mathbf{h}_j$. It is clear that $[1-(1-2\tau)^w]/2 < 1/2$. And because the mean value is the unbiased estimation of the mathematical expectation, we can traverse all the probable starting positions and find the one as the true estimation of synchronization position that minimizes the mean value of $\mathbf{h}_j \times \mathbf{C}_i$ as follows

$$\frac{1}{(n-k)M} \sum_{i=1}^{M} \sum_{j=1}^{n-k} \mathbf{h}_j \times \mathbf{C}_i \tag{2}$$

We let

$$P_r = 1 - \frac{1}{(n-k)M} \sum_{i=1}^{M} \sum_{j=1}^{n-k} \mathbf{h}_j \times \mathbf{C}_i \tag{3}$$

and find the synchronization positions by maximizing P_r. To distinguish the values of P_r on different starting positions, we use $P_r(t)$ to depict the P_r calculated when the matrix $\mathbf{MT}$ is filled with the assumption that t is the synchronization position. In Eqs. (2) and (3), the product operation is defined in Galois Field GF(2) and the sum in real field.

To improve the synchronization performances, we need to select property coding parameters based on the following principles.

(1) Selection of code type

Firstly we discuss witch kinds of error-correction codes are suitable for the blind frame synchronizations. We can analyze the mathematical expectation and variances of P_r and find out which variables have impact on the distinction of P_r on correct and incorrect synchronization positions. According to the binomial distribution theories, we have the expectation EI and variance DI of P_r based on incorrect synchronizations as follows:

$$\begin{cases} EI = \dfrac{1}{2} \\ DI = \dfrac{1}{4(n-k)M} \end{cases} \tag{4}$$

And in correct synchronization cases, we denote the expectation and variance by EC and DC which can be calculated as follows:

$$\begin{cases} EC = \dfrac{1+(1-2\tau)^w}{2} \\ DC = \dfrac{1-(1-2\tau)^{2w}}{4(n-k)M} \end{cases} \tag{5}$$

As the value of w rising, DI and DC also raise, i.e. the variance of P_r rises. And EC descends when w rises, which reduces the distance between the values of P_r on correct and incorrect synchronizations. So we hope that w is low. A lower w means that we have a higher EC to make the distance between EC and EI be larger. And a low w can reduce DI and DC to make the distribution of P_r be more concentrated so we have less superposition area between the distributions of P_r in correct and incorrect synchronization situations.

Download English Version:

https://daneshyari.com/en/article/848473

Download Persian Version:

https://daneshyari.com/article/848473

Daneshyari.com