This invention relates to packet switching systems and to methods for preventing the unauthorised detection of the start and end of packets being transmitted in a packet switching system.

Data encryption is well known and has been in use for a number of years. A problem arises in packet switching networks in that whereas it is possible to encrypt the data contained within the packet, the packet itself, as it is transmitted between packet switching networks via interconnecting trunks, is defined by flag and header information. Hence, the encryption of the data is not as effective since the amount of data being encrypted is relatively small, and the probability of the encryption algorithm being broken is greatly increased. Indeed, the packet header information contains the logical channel number which allows the identification of which packets are associated with particular frames being transmitted between packet switching systems.

One such prior art packet switching system is disclosed in U. S. Patent 4,494,230, and is illustrated in FIG. 1. FIG. 2 illustrates the packet which would be transmitted in the packet switching system of FIG. 1 between customer 100 and customer 110. The data portion of the packet illustrated in FIG. 2 would be encrypted by customer 100 before transmission into the packet switching system, but the system adds flag information and the header information that consists of packet identifier, logical address, and time stamp fields. The packets in the above-cited U. S. patent are communicated via high-speed digital links across country via trunks such as trunk 118. These trunks could be microwave or satellite links. In the event that unauthorized personnel should gain access to trunk 118, the packets being communicated on trunk 118 would have the format illustrated in FIG. 2. Since the customer is only able to encrypt the data portion of the packet of FIG. 2, the unauthorized personnel could readily break the encryption algorithm.

From the foregoing, it can be seen that there exists the need for a method of not only encrypting the data within a packet, but for encrypting the entire transmission path over which the packets flow, thus also encrypting the flag and header information. Whereas the present public key encryption systems perform extremely well in absence of errors, these systems require a large amount of processing, and more efficient and less intense processing algorithms are desirable. In the presence of errors, packets are likely to be lost during periods of re-synchronization using a public key encryption system.

According to one aspect of this invention there is provided a packet switching system as claimed in claim 1.

According to another aspect of this invention there is provided a method as claimed in claim 7.

5

In an illustrative method and structural embodiment, a departure in the art is achieved by a packet switching system which encrypts the flags that define the start and end of packets being communicated on links such as high-speed data transmission trunks. Furthermore, a procedure is provided for synchronizing the encryption of the flag information at either end of the trunk by the trunk controllers that connect directly to the high-speed digital trunk.

Advantageously, the structural embodiment comprises a circuit for encrypting only the flags prior to transmission on a trunk and a circuit for decrypting the flags upon receipt from the trunk. The decrypting circuit has a subcircuit for detecting when the decrypting circuit is no longer in flag synchronization with respect to the encrypting circuit. Upon detecting that flag synchronization has been lost, the latter subcircuit initializes the encrypting circuit by transmitting a predetermined packet to the encrypting circuit.

Advantageously, the encrypting circuit has a subcircuit for detecting the predetermined packet and for generating an initialization signal. The encrypting circuit has another subcircuit responsive to the initialization signal for initializing the encrypting circuit to generate a predetermined sequence of encrypted flags.

Also, the decrypting circuit has a detection subcircuit for detecting the predetermined sequence of encrypted flags. The detection subcircuit is responsive to the predetermined sequence to place the decrypting circuit in flag synchronization with the encrypting circuit.

In addition, each flag has a plurality of bytes, and the decrypting circuit has a maintenance subcircuit for maintaining synchronization upon up to a predetermined number of the flag bytes being incorrect within any particular flag. Also, the maintenance subcircuit maintains flag synchronization upon up to a predetermined number of the bytes of the current flag appearing in the data of the current packet.

A method prevents an unauthorized detection of the start and end of packets being transmitted in a packet switching system which has packet switching networks that are interconnected by trunks. Each network terminates a trunk with trunk controller. The method has the steps of only encrypting flags separating packets upon transmission of the packet on a connected trunk and decrypting the encrypted flags upon receipt of the packets from the connected trunk. The decrypting step includes the step of synchronizing with encrypted

1983, published by American Telephone and Telegraph Company.

Consider in greater detail the functions performed by the blocks of FIG. 3. First, consider the transmission from trunk controller 131 to trunk controller 140. It is assumed at this point that the trunk controllers are in synchronization both with respect to the data stream and the flag encryption. When the trunk controller has a packet to send, it transfers the packet to the idle transmitter 301 via the data and write links of cable 310. Before the transfer, the trunk controller must be receiving the ready signal from idle transmitter 301 via cable 310. Idle transmitter 301 is responsive to the start of the data to transmit the data select signal via conductor 314 and data via conductor 313 to flag aliasor 303 if the hold signal is not being transmitted from block 303 to block 301 via conductor 315. Block 303 is responsive to previously received flag bits from random flag generator, RFG, 302 to perform a standard flag aliasing operation on the data being received via conductor 313 to assure that the start flag does not appear in the transmitted data. After the aliasing operation is performed, block 303 transfers the data via conductor 314 to the T1 subsystem 308 via OR gate 307. After the packet has been transmitted, block 303 detects this fact and transmits the new flag signal via conductor 341 to RFG 302. The latter block is responsive to the latter signal to transmit the end flag to T1 subsystem 308 via conductor 320 and OR gate 307. RFG 302 will continue to transmit flags to T1 subsystem 308 until the toggle signal is transmitted via conductor 319 from block 303. The transmission of the toggle signal indicates that block 303 has information to transmit to T1 subsystem 308. Block 303 does not commence transmission of this data until the load flag signal is received via conductor 318 from RFG 302. The latter block transmits the load flag signal after it has transmitted the last current flag via cable 317. The flags are variable and are being generated by random variable generator 302 in response to an initial seed as will be explained in greater detail with respect to FIG. 9.

At the receiving end, as illustrated in FIG. 4, as the data is being received via trunk 118 by T1 subsystem 328, the latter subsystem recovers the clock and transfers the data via conductor 348 to random flag receiver, RFR, 326. When RFR 326 detects a start flag indicating the start of a new packet, it transmits the flag valid signal via conductor 344, blocks 324, and 365, and transfers the flag bits via conductor 346 to block 325. The flag valid signal indicates that the flag bits transferred via conductor 346 represented the start flag of a new packet. After RFR 326 has received the start flag for that packet, it

Claims:

1. A packet switching system for the communication of a plurality of packets, said packet switching systems comprising a plurality of switching offices (102,104) interconnected by a plurality of trunks (117,118) with each trunk terminated on both ends by a pair of trunk controllers (131,140), and wherein flags are used to separate packets during communication on said trunks, each of said trunk controllers being CHARACTERIZED BY

a circuit (301,302,303) for randomly encrypting only said flags separating packets upon transmission of said packets and said flags; and

a circuit (304,305,306) for decrypting said randomly encrypted flags upon receipt of said packets and said flags.

2. A system as claimed in claim 1 wherein said decrypting circuit comprises a subcircuit (306) for synchronizing with said randomly encrypted flags.

3. A system as claimed in claim 2 wherein said encrypting circuit comprises a subcircuit (302) for generating a predetermined sequence of said randomly encrypted flags upon initialization; and

said synchronizing subcircuit comprises a subcircuit (600-604, 610-614, 620-624, 630-634) for detecting said predetermined sequence of said randomly encrypted flags thereby achieving flag synchronization.

4. A system as claimed in claim 3 wherein said synchronizing subcircuit comprises a subcircuit (600-604, 610-614, 620-624) for detecting the loss of said flag synchronization; and

a circuit (304) responsive to the detection of said loss of said flag synchronization for initializing said encrypting circuit.

5. A system as claimed in claim 4 wherein said initializing circuit comprises a subcircuit (504) for transmitting a predetermined packet to said encrypting circuit means; and

said encrypting circuit comprises a subcircuit (806) responsive to said predetermined packet for initializing said encrypting means.

6. A system as claimed in claim 5 wherein each of said flags comprises a plurality of bytes, and said synchronizing subcircuit comprises a subcircuit (627) for

maintaining synchronization upon up to a predetermined number of said bytes being incorrect within any particular one of said flags.

7. A method for preventing the unauthorized detection of the start and end of packets being transmitted in a packet switching system, wherein said packet switching system has packet switching networks (102,104) comprising communication controllers (131,140), said packet switching networks are interconnected by communication paths (117,118) between said networks, each end of said communications paths terminates on an inidividual one of said communication controllers, and flags are used to separate packets during communication on said communication paths, said method being CHARACTERIZED BY the steps of

only randomly encrypting (301,302,303) flags separating packets upon transmission of said packets and said flags; and

decrypting (304,305,306) said randomly encrypted flags upon receipt of said packets and said flags.

8. A method as claimed in claim 7 wherein said decrypting step comprises the step of synchronizing (306) with said encrypted flags.

9. A method as claimed in claim 8 wherein said encrypting step comprises the step of generating (302) a predetermined flag pattern upon initialization; and

said synchronizing step comprises the step of detecting (600-604, 610-614, 620-624, 630-634) said predetermined flag pattern thereby achieving flag synchronization.

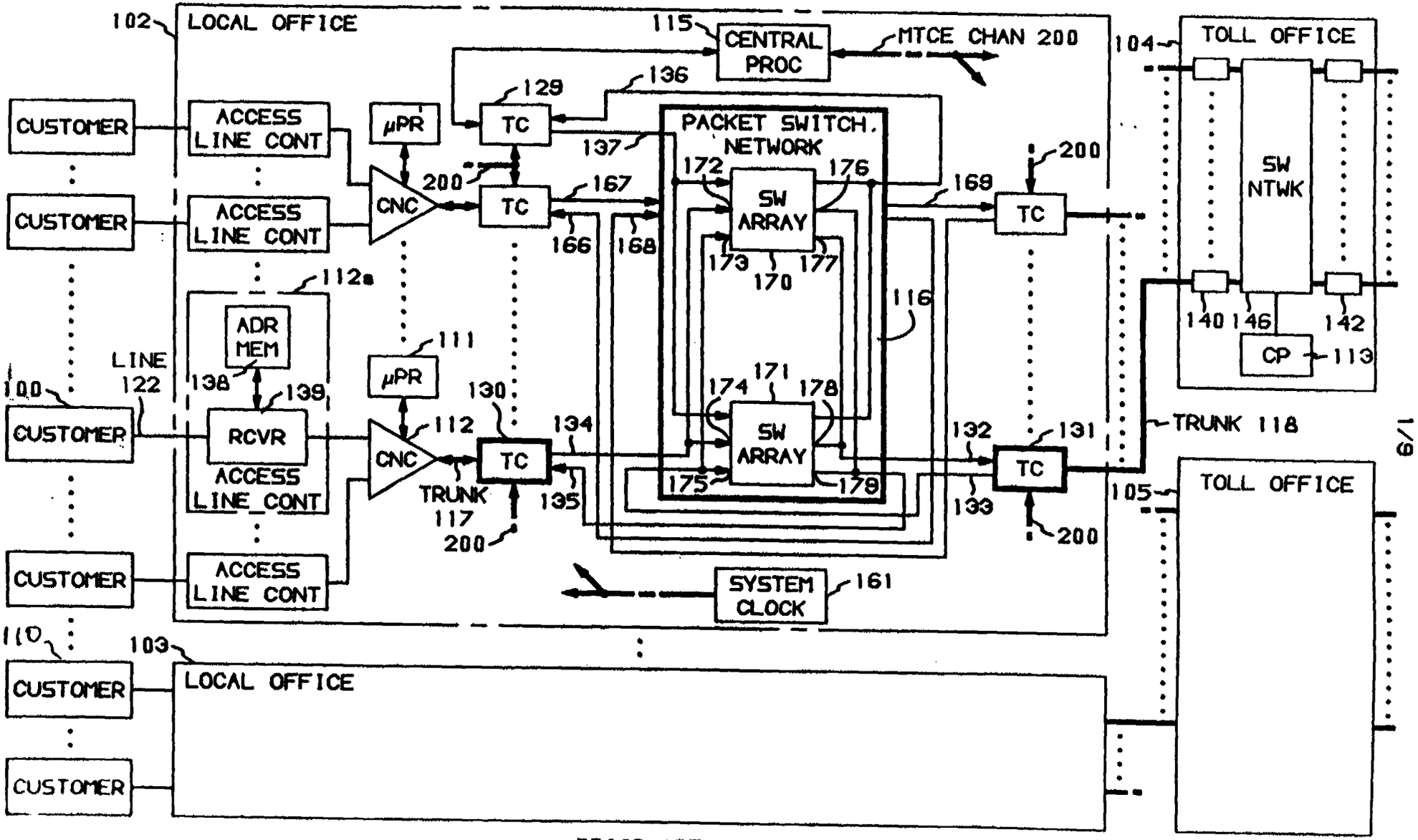
10. A method as claimed in claim 9 wherein said decrypting step comprises the steps of detecting (600-604, 610-614, 620-624) the loss of said flag synchronization; and

initializing (304) said encrypting step in response to the detection of the loss of said flag synchronization.

11. A method as claimed in claim 10 wherein said initializing step comprises the step of transmitting (504) a predetermined packet to said encrypting step; and

said encrypting step comprises the step of restarting (806) to initialize said encrypting step in response to said predetermined packet.

12. A method as claimed in claim 11 wherein each of said flags comprises a plurality of bytes, and said syncrhonizing step comprises the step of maintaining (627) synchronization upon up to a predetermined number of said bytes being incorrect within any particular one of said flags.



PRIOR ART

FIG. 1

1/9