

Covert channel for improving VoIP security

ACS 2006, October 18-20, 2006

Wojciech Mazurczyk, Zbigniew Kotulski
{wmazurczyk, zkotulsk}@tele.pw.edu.pl

Warsaw University of Technology
Faculty of Electronics and Information Technology
Institute of Telecommunications

Outline

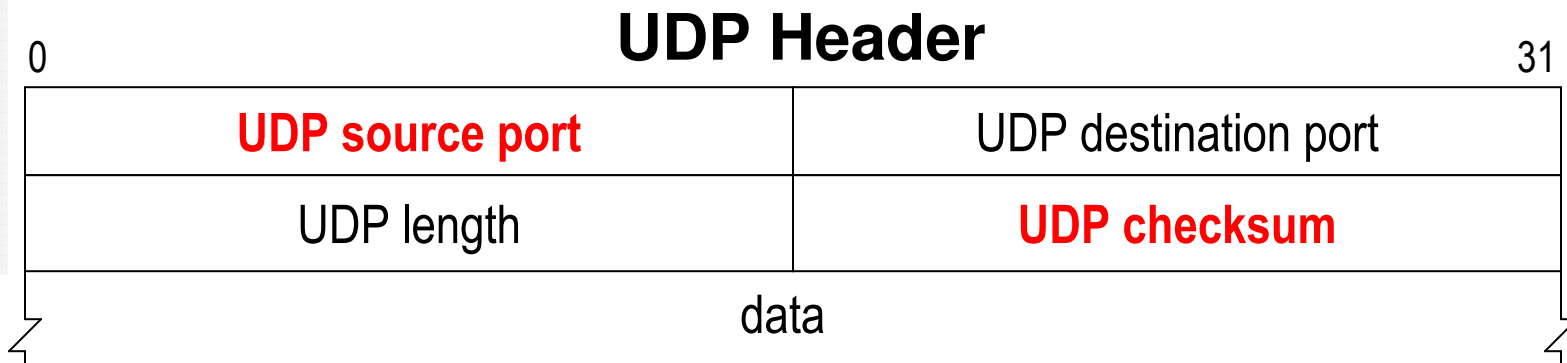
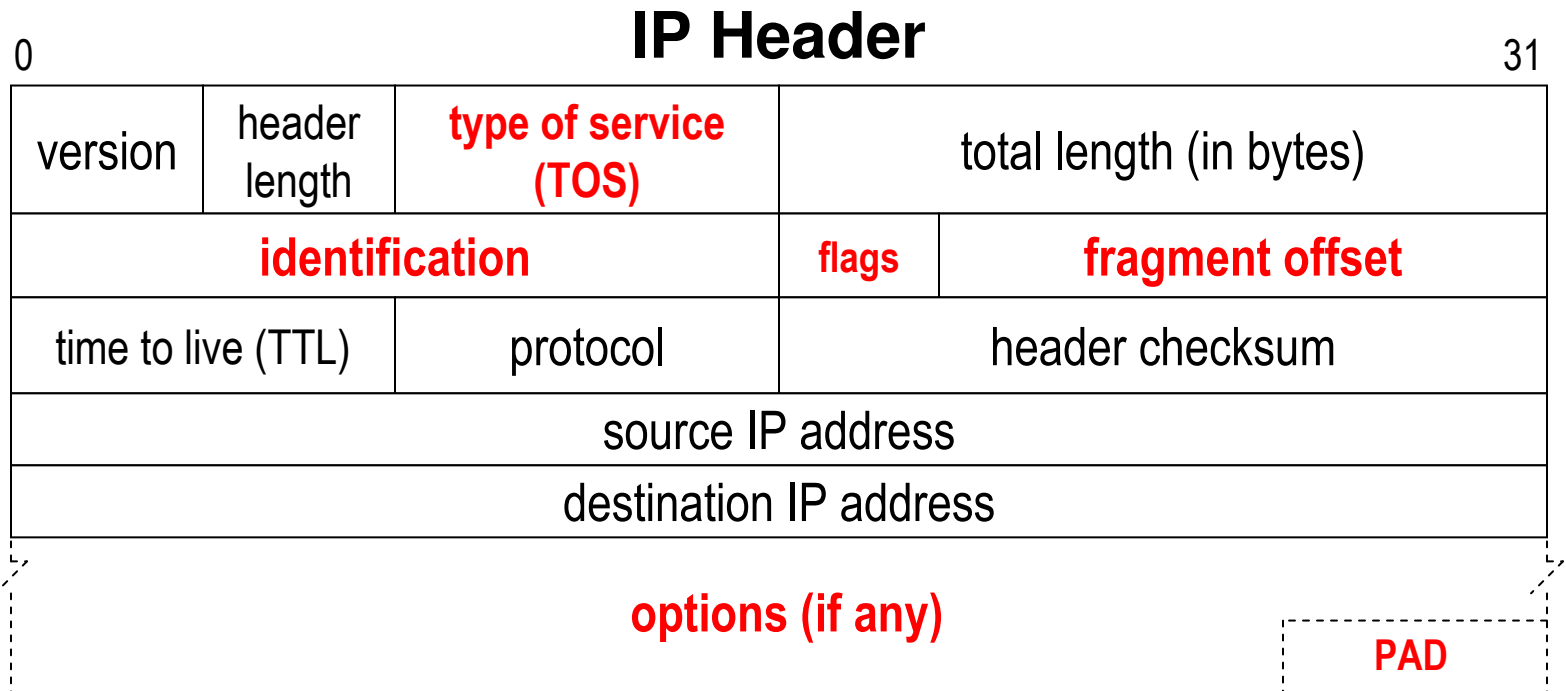
- Introduction
- Information Hiding Techniques
 - Network Steganography
 - Digital Watermarking
- Multipurpose covert channel for VoIP
- PDU Description
- Improving VoIP security
- Summary

Introduction

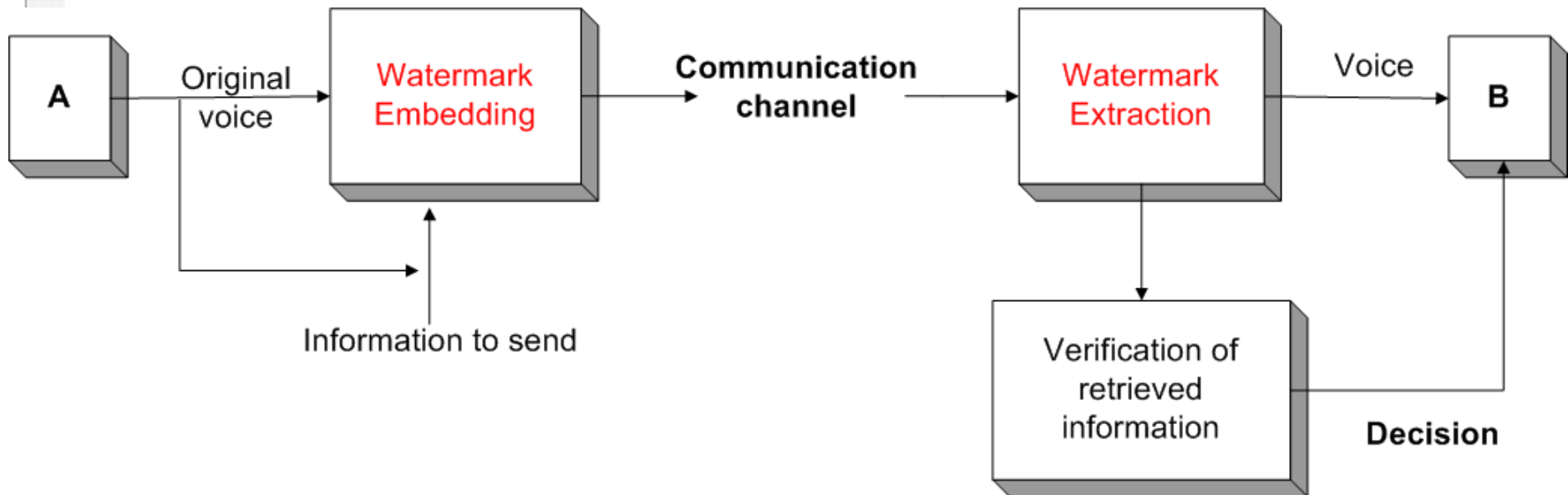
- Voice over IP problems
 - Providing QoS (Quality of Service) parameters (low latency, packet loss etc.)
 - Security issues – problems with existing mechanisms
 - Seeking for new approaches

- Covert channel in VoIP with Information Hiding techniques:
 - Network steganography
 - Digital watermarking

Network Steganography – IP/UDP/RTP



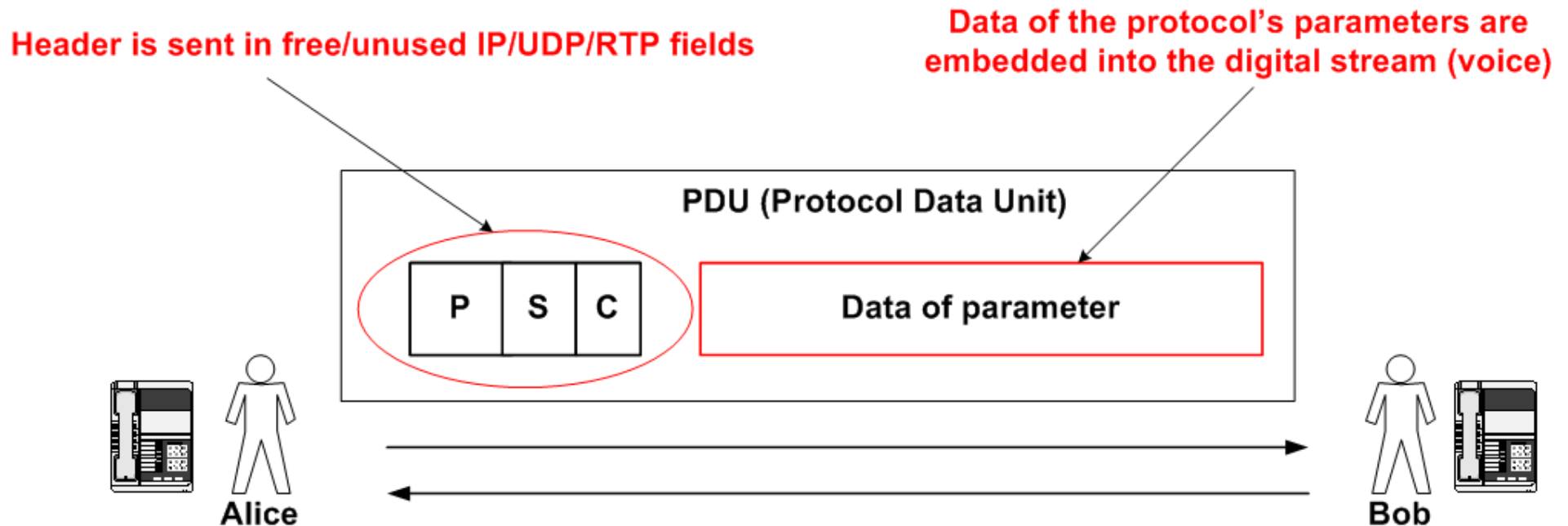
Digital Watermarking



- Marking digital content (images, video, **audio** or text)
- Two main functions:
 - Watermark Embedding Function
 - Watermark Extraction Function

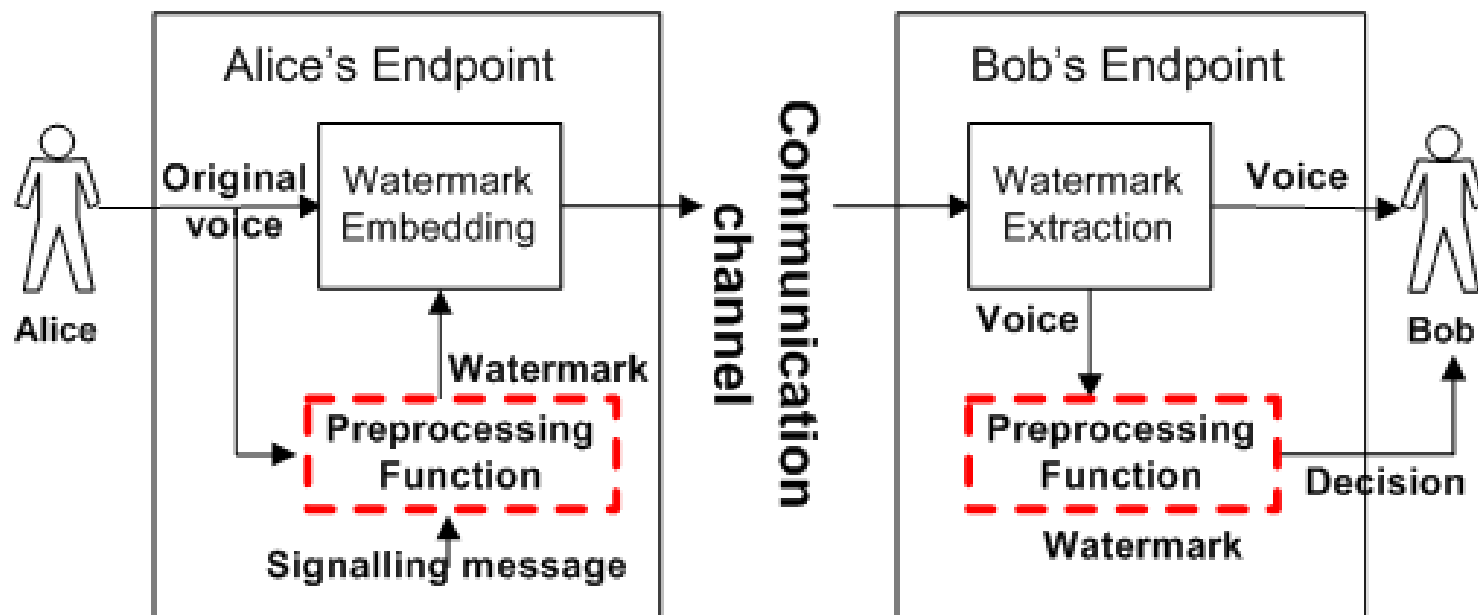
Multipurpose Covert Channel - protocol

- PDU's (Protocol Data Unit) size must be kept to minimum. It consists of:
 - The header/control fields are transmitted in unused/optional fields of IP/UDP/RTP protocol's headers
 - Actual value of the data is embedded into voice as a watermark



Multipurpose Covert Channel - details

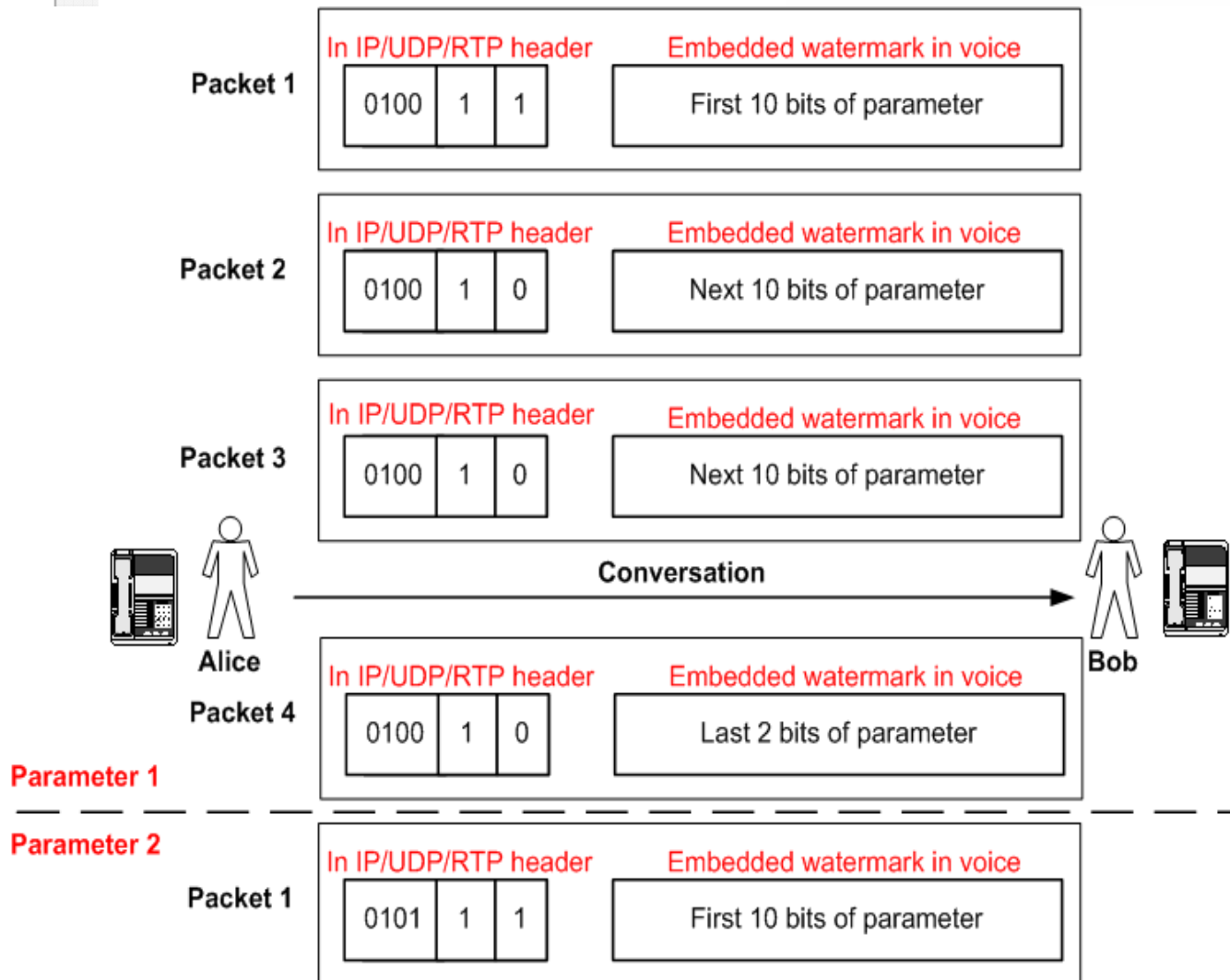
- General characteristic
 - Proposed mechanism is independent of the watermarking algorithm
 - The data that forms the watermark are prepared with **Preprocessing function**



PDU Description

Type of field	No. of bits	Function
P (Parameter)	4	Indicates parameter that is transmitted inside the watermark
S (Side)	1	Indicates the side of the communication (1 - sender, 0 – receiver)
C (Continuity)	1	Describes if a packet contains the beginning or continuation of the parameter indicated in the field P (1 – beginning of new parameter, 0 – continuation of the last parameter)

EXAMPLE



Types of parameters:

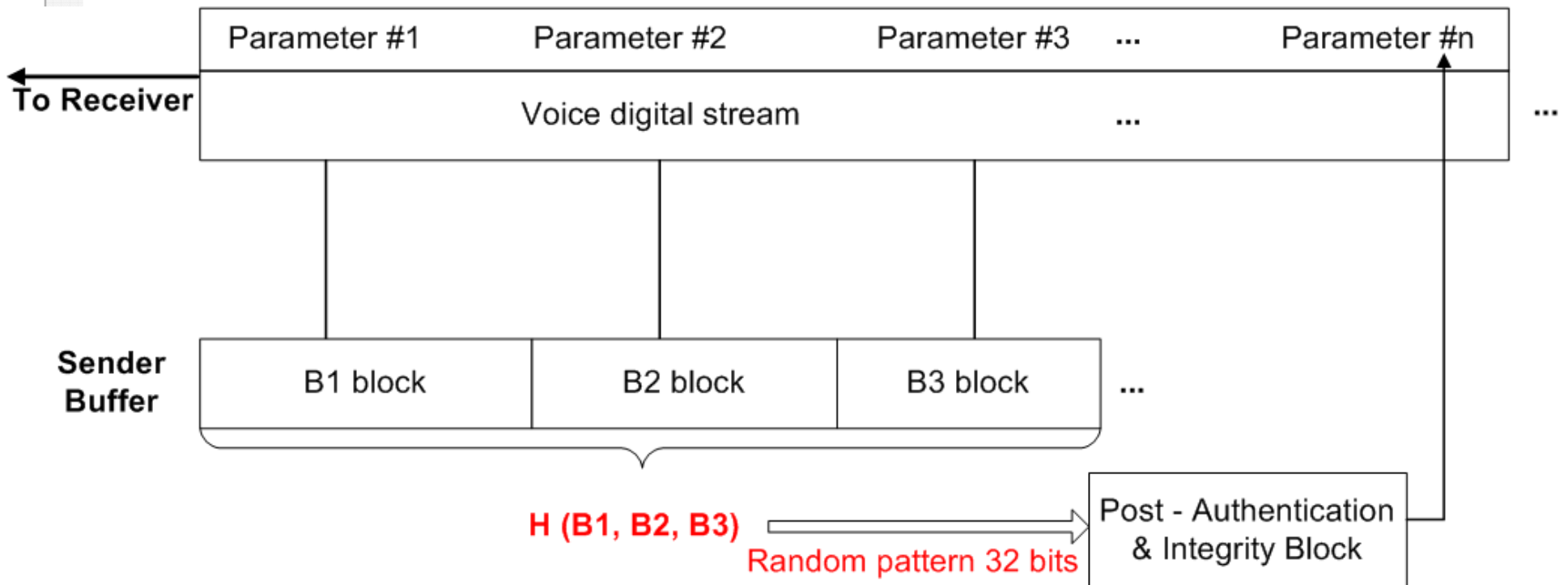
- Informational
- Security (authentication and integrity)
- Postauthentication and integrity

Improving VoIP Security

Security Token Calculation

$$TokenA_N = H \left(H(VF_N) \parallel H(SM_N) \parallel \begin{pmatrix} TS \\ PASS \parallel R \\ ID_A \end{pmatrix} \parallel R \right)$$

Post Authentication



Summary

- ❑ **Lightweight, low-power computing** and **no bandwidth consuming** solution, that uses a covert channel created in media streams
- ❑ Useful to improve **IP Telephony security** - able to protect both: voice and signalling protocol
- ❑ **Multipurpose channel** – can be used to carry any information e.g. QoS parameters
- ❑ **Capacity** of the channel depends on the **watermarking technique** used and **codec bit rate**
- ❑ **Constant exchange** of data during whole conversation

Covert channel for improving VoIP security

ACS 2006, October 18-20, 2006

Wojciech Mazurczyk, Zbigniew Kotulski
{wmazurczyk, zkotulsk}@tele.pw.edu.pl

Warsaw University of Technology
Faculty of Electronics and Information Technology
Institute of Telecommunications