
New VoIP traffic security scheme with digital watermarking

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

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

SafeComp 2006, Gdansk, 28.09.2006

Outline

- Introduction: securing IP Telephony problems
- Types of traffic in VoIP and most important security services
- Digital watermarking – a new approach
- Details of the proposed scheme and general mechanism operation
- Advantages and disadvantages of proposed solution and conclusions

Introduction: securing VoIP

- Securing VoIP (Voice over IP) is a **complex process** as it is a real-time service
- **A lot of aspects to consider:** network design, condition, delay...
- The need to provide certain QoS (Quality of Service) parameters values often results with **not enough** or **no security mechanisms** for VoIP service
- Total delay value for transmitting the media streams cannot exceed 150ms
- Security mechanisms can be responsible for the **increased latency**. It can be degenerating for the quality of the VoIP call
- Nowadays we are often facing the necessity of the **trade off between providing security and the low latency** for real-time service

Types of traffic in VoIP and security services

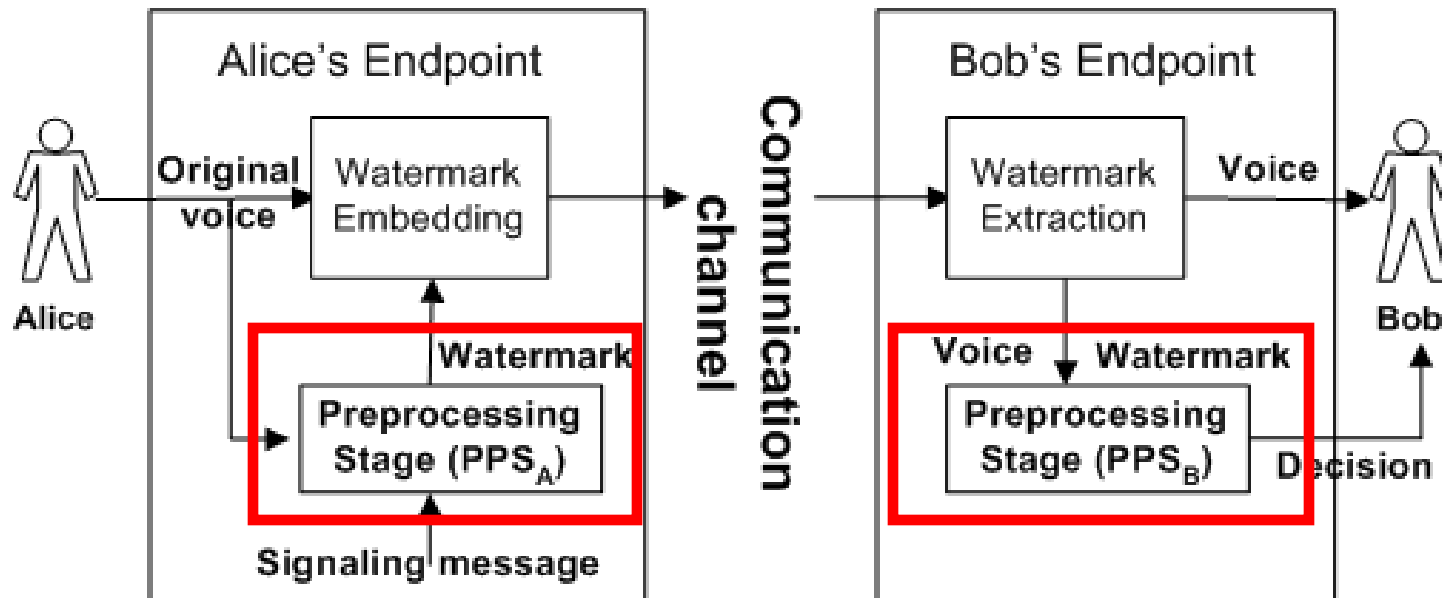
- **Two phases of the connection:**
 - 1) The initial **signalling phase**, in which certain signalling messages are exchanged between the parties
 - 2) **Conversation phase** (exchanging media streams)
- Each phase has its **disjunctive set of security mechanisms**
- Security mechanisms for the VoIP signalling protocols e.g. SIP and H.323 are also different
- **What we are proposing is to move providing the security of the signalling messages from the first phase to the second one (to the conversation phase)**
- **We called this method a *post factum* method**
- The three most crucial security services for IP telephony systems are: **authentication, integrity and confidentiality**. With proposed mechanism we can provide first two of them

Watermarking – a new approach

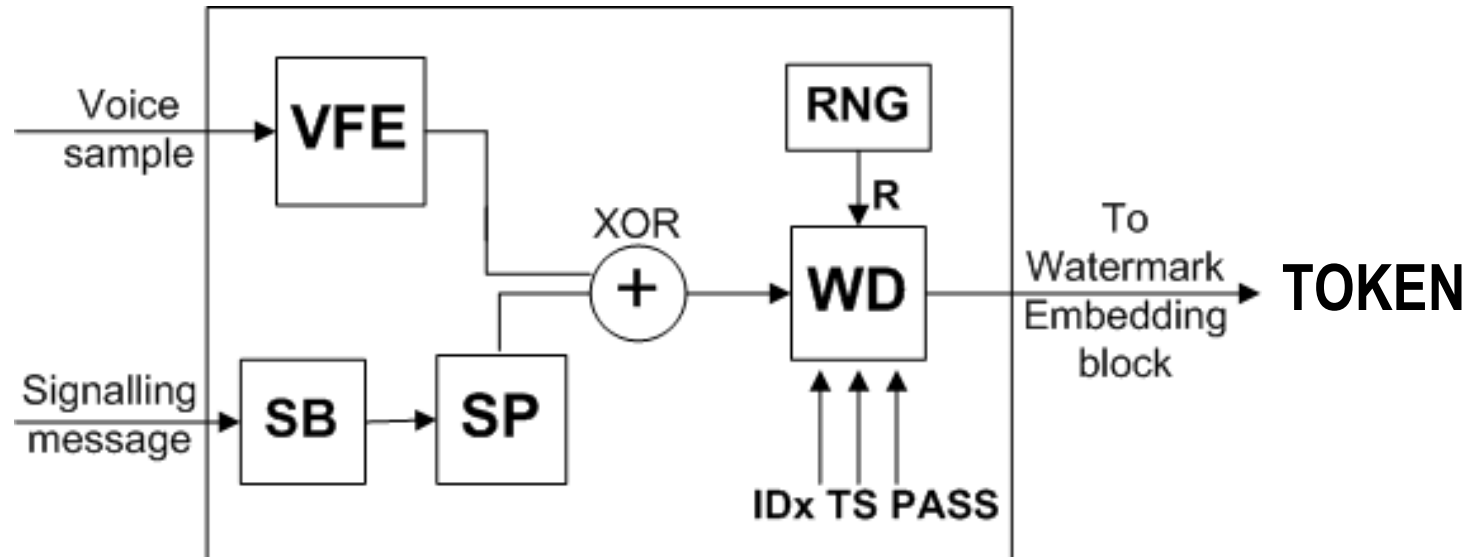
- **Digital watermarking** technique is gaining more and more attention these days. It covers a large field of various aspects, from cryptography to signal processing
- It is mainly **used for marking the digital data** (images, video, **audio** or text)
- Authors can embed data, which is similar to a cryptographic hash, into their digital work. This hash is **invisible** and **inseparable** from the data
- Properties of watermark: **robustness**, **security**, transparency, complexity, capacity, verification and invertibility are mutually competitive
- The most popular audio watermarking algorithms include: LSB, spread spectrum watermarking or watermarking the phase of the host signal

Details of the proposed scheme

- **Two general assumptions**
 - proposed mechanism is **independent of the watermarking algorithm** - the output watermark, if created, has the best properties allowed for the communication environment used
 - both sides of communication **share a secret password**



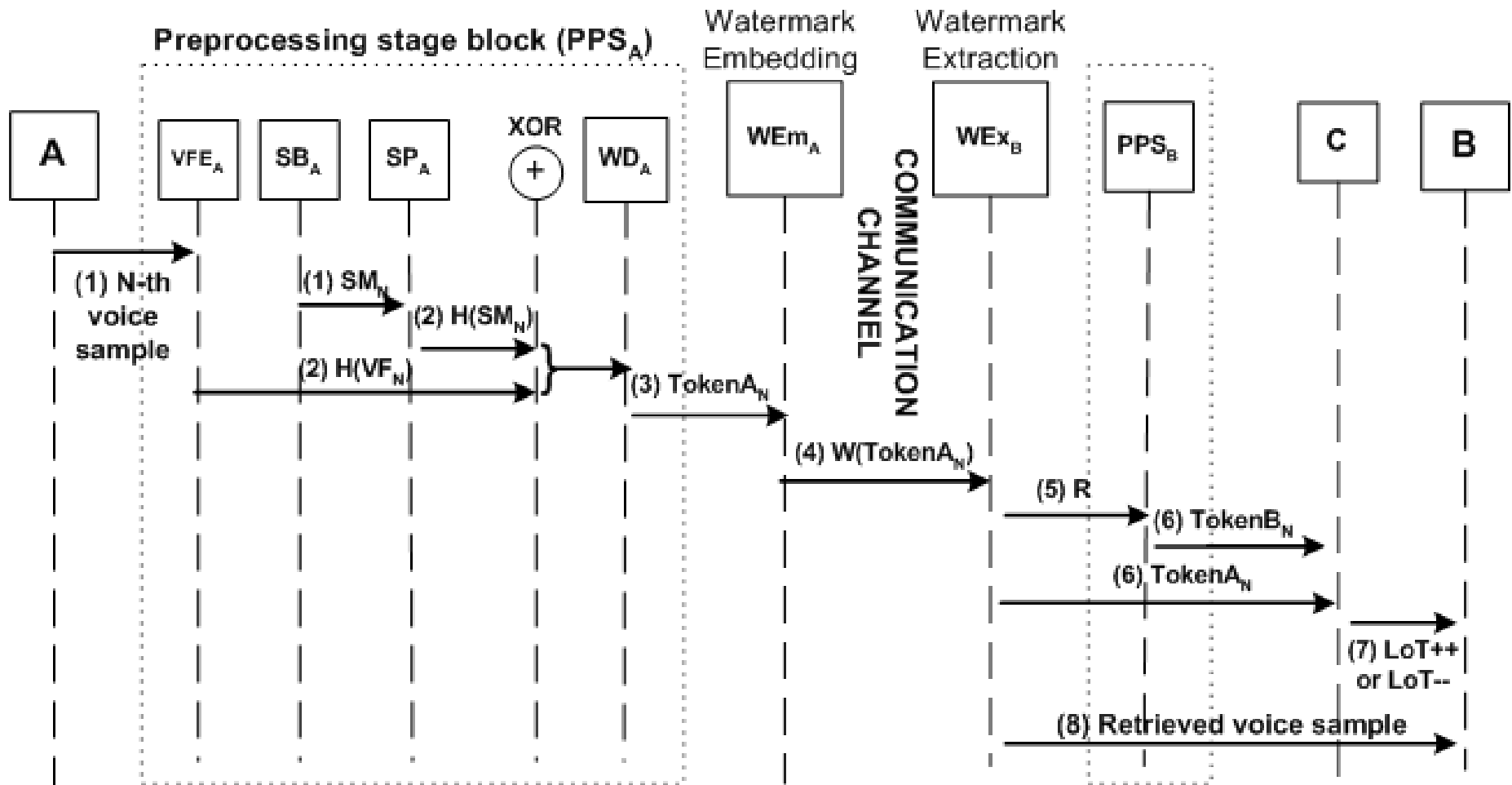
Preprocessing Stage Block



- **SB** (Signalling Message Buffer): stores the signalling messages from the first phase of the call
- **SP** (Signalling Messages Processing): in this block a hash function is performed on each signalling message
- **RNG** (Randomizer): we use it to provide a unique set of data for every embedded watermark
- **WD** (Watermarking Data): in this block all the input data is concatenated
- **VFE** (Voice Feature Extractor): provides characteristic features (VF) of the original voice that we want to protect

General mechanism operation

$$\text{TokenA}_N = \text{TokenB}_N = \text{H} \left((\text{H}(\text{SM}_N) \oplus \text{H}(\text{VF}_N)) \parallel \begin{pmatrix} \text{TS} \\ \text{PASS} \\ \text{ID}_A \end{pmatrix} \parallel \text{R} \right) \parallel \text{R}$$



Level Of Trust (LoT) parameter

- Still we can imagine a situation, in which **the retrieved token will be corrupted**, due to the packet loss (or some other reason). In this case, we cannot allow the call to be cancelled immediately
- That is why both sides update **special parameter named LoT** (Level of Trust), during a conversation. If the compared tokens are equal, the LoT parameter increases. In any other situation its value decreases
- LoT has initial value and the critical threshold set, so that if attack occurred it can be detected (but it will not be mistaken with poor network condition). Those initial values should be chosen carefully:

$$\text{LoT} = F(\text{Packet_loss_ratio}, \text{Delay}, \text{Bit_Error_Rate}, \dots)$$

Advantages and disadvantages of proposed solution

Advantages (+)	Disadvantages (-)
+ It is lightweight, low-power computing and no bandwidth consuming mechanism, because it uses a channel created in media streams	- Checking the security of the signalling protocol is made after the signalling phase is finished - late attacks detection on signalling protocol
+ It provides one, unified solution for the audio and signalling protocol security	- Provides authentication and integrity, so can be used only in combination with other security mechanisms
+ It prevents doubling latency and excessive consuming of the processing time for security mechanisms	
+ It is signalling protocol and digital watermarking algorithm independent solution	
+ It is capable of solving the security mechanisms incompatibility for various IP Telephony systems that are based on different signalling protocols	

New VoIP traffic security scheme with digital watermarking

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

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

SafeComp 2006, Gdansk, 28.09.2006