New VoIP Traffic Security Scheme with Digital Watermarking

Wojciech Mazurczyk[1] and Zbigniew Kotulski[1,2]

[1] Warsaw University of Technology, Faculty of Electronics and Information
Technology, Institute of Telecommunications 15/19 Nowowiejska Str.
00-665 Warszawa, Poland
{W.Mazurczyk, Z.Kotulski}@tele.pw.edu.pl
[2] Polish Academy of Sciences, Institute of Fundamental Technological Research
zkotulsk@ippt.gov.pl

Abstract. In this paper we propose a new, lightweight, no bandwidth consuming authentication and integrity scheme for VoIP service based on SIP as a signalling protocol. It is shared password mechanism and this solution exploits digital watermarking. Nowadays, there are many applications of this technique, such as solving copyright protection problems, but we propose to use it to secure the transmitted audio and signalling protocol that IP Telephony is based on simultaneously. This solution can be the potential answer to the problem VoIP faces today: finding a scalable and universal mechanism for securing VoIP traffic (voice and the signalling protocol messages) at the same time. It can greatly improve, if we combine it with existing security mechanisms, overall IP Telephony system's security.

1   VoIP Security Problems

Securing IP Telephony is a complex process. This not only means the ability to make secure conversation between two communicating parties, but also the security of signalling messages used to make this call possible at all. The need to provide certain QoS (Quality of Service) parameters values often results with not enough or no security mechanisms for VoIP service. This is mainly because security mechanisms can be responsible for the increased latency. If latency is too high, it can be the most degenerating constrain for the quality of the VoIP call. So, nowadays we are often facing the necessity of the trade off between providing security and the low latency for real-time service.

That is why our motivation in finding alternative way to handle IP Telephony security (with special emphasize on the authentication and integrity security services) is based on the following facts:

- There is no universal solution for protecting both: audio and signalling messages for IP Telephony systems [8],
- There are drawbacks of SRTP protocol which are discussed in [3]; SRTP is the most popular mechanism to provide authentication and integrity for the data stream,

- The speed of embedding/extracting digital watermark into/from audio is suitable for real-time services,
- Authentication based on digital watermarking scheme is inseparably bound to the data stream content,
– VoIP security is still evolving and still it is time for new solutions and ideas.

That's why, in this paper, we are proposing a novel approach to the IP Telephony security based on digital watermarking. This solution is suitable for the protection of both the audio content and signalling messages simultaneously.

2   Digital Watermarking

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). From typical applications for digital watermarks, described in [1] and [2], most important application, which can really improve VoIP security, is the ability of embedding the **authentication and integrity watermark.** Authors can embed data, which is similar to a cryptographic hash, into their digital work. This hash is invisible and inseparable from the data. This way we can achieve the copyright protection by watermarking data with the author's identifier (owner authentication) and we can ensure the authentication and integrity of the data, which allows us to recognize all later data manipulations (a general term in literature is the data authentication [9], [10]).

   The watermark that will be used in the authentication and integrity scheme we propose, must possess certain properties like: robustness, security, transparency, complexity, capacity, verification and invertibility. The mentioned properties are described in details in [1] and [2]. The optimization of these properties for real-time audio system is crucial. They are often mutually competitive; that is why there is always a compromise necessary to construct an efficient system. For our purpose the embedded watermark, that we will use, must be characterized by **high robustness** (but only until the semantics of the data is destroyed), **high security** and must be **non-perceptual**. IP Telephony is a demanding, real-time service, so we need the watermarking schemes that deal with the real-time services. The number of such solutions is not high, however, they already exist. Such watermarking algorithms are described, e.g., in [2], [3] and [5].

   The general audio watermarking scheme for VoIP traffic consists of two functions: embedding and extractions of the watermark. As soon as the conversation begins, certain information is embedding into the voice samples (as a watermark) and it is sent through the communication channel. After reaching a called party the watermark is extracted, the information is retrieved and verified. If the received watermarked data and extracted parameters are correct, the conversation can be continued.

   Most digital watermarking algorithms for the real-time communication are designed to survive typical non-malicious IP Telephony operations like: low bit rate audio compression, codec changes, DA/AD conversion and packet loss. For example, in [2] the watermarking scheme developed at the Fraunhofer IPSI and the Fraunhofer IIS were tested for different compression methods. Those results revealed that the large simultaneous capacity and robustness depend on the scale of the codec compression. When

the compression rate is high (1:53), the watermark is robust only when we embed about 1 bit/s. With a lower compression rate we can obtain about 30 bit/s, whereas the highest data rate was 48 bit/s with good robust, transparent and complexity properties. For the monophonic audio signal, which is a default type for IP Telephony, the watermark embedding algorithm appeared around 14 times faster and the watermark detector almost 6 times faster than the real-time.

3   VoIP Security Services

As stated in [16] the security services for system's information security are: authentication (and identification), integrity, authorization (logical access control), confidentiality and non-repudiation/non-denial. But if we take into consideration securing IP telephony systems, the three most crucial security services are: authentication, integrity and confidentiality. The first two can be provided with the use of the watermarking techniques. The third one should be guaranteed in a different manner, e.g., with the use of the security mechanisms (encryption) from the set defined for each VoIP standard.

In particular, the proposed here scheme provides the following security services:

- **Authentication of the data source** (one can be sure of the identity of the caller),
- **Authentication of the signalling messages** (one can prove that the caller is the source of the signalling messages that were exchanged during the signalling phase of the call),
- **Signalling messages integrity** (one knows that the signalling messages were not modified during the transmission through the communication channel)
- **Data authentication** – integrity (one can be sure that the audio comes from the caller and it has not been tampered).

Furthermore, making a call in IP Telephony systems consists of two phases: the initial **signalling phase,** in which certain signalling messages are exchanged between the parties, and the **conversation phase**. Each phase has its disjunctive set of security mechanisms (although, the secure signalling sometimes includes a secure key-setup for the media channels). Nowadays, in SIP and H.323 we can implement different security mechanisms designated for securing the data stream (audio) and other that cover signalling protocols security. Additionally, the security model for the protocols: SIP and H.323 is also different, which means that they use almost disjunctive set of the security mechanisms. What we are proposing in this paper 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. This is a first scheme that is using this method. What is characteristic the act of checking the security of the signalling protocol is made after the signalling phase is finished. Such a solution has disadvantages: the most serious one is that a potential attack on the signalling protocol is detected some time after the beginning of the conversation. But on the other hand, this approach has certain advantages:

- It provides one, unified solution for the audio and signalling protocol security,
- It is low-power computing as stated in [2] and no bandwidth consuming mechanism, because we use a channel created in media streams,

- It is signalling protocol independent solution,
- It prevents doubling latency and excessive consuming of the processing time,
- It also reduces complexity (and cost!) of the network equipment on the communication path,
- It is capable of solving the security mechanisms compatibility for various IP Telephony systems that are based on different signalling protocols.

Moreover, it can also help to protect the audio and signalling protocol on the interface between VoIP systems and PSTN (since the watermark is robust, it will survive AD/DA operations).

Unlike the existing security mechanisms for IP Telephony, it provides also real end-to-end security. No network equipment on the communication path will be aware of the embedded watermark, unless it is designed to do so.

Thus, we think that the proposed solution can be an important step in providing authentication and integrity for VoIP traffic.

4   Proposition of Authentication and Integrity Scheme

We assume that proposed mechanism is independent of the watermarking algorithm. It means that it does not depend on watermark embedding and extraction technique. No matter which algorithm for real-time communication is used, the output watermark, if created, has the best properties allowed for the communication environment used. Such an assumption gives this solution flexibility and it will be capable of supporting future ideas of digital watermarking algorithms. Another assumption is that both sides of communication share a secret password (in this paper we do not cover the algorithm used for password exchanging).

4.1   Scenarios for Digital Watermarking in VoIP Security and Related Work

We can point out three possible scenarios, in which we can take advantage of using the digital watermarking to provide authentication and integrity for IP Telephony:

> I. We can secure the media stream (audio),
> II. We can secure the signalling messages,
> III. We can secure both: the audio and signalling protocols at the same time.

Working algorithms for **I** are presented, i.e., in [2], [3] and [5]. We do not fully benefit from the solution **II**, because in this case we still have a disjunction set of the security mechanisms for securing the media stream and a signalling protocol. This is a novel approach and there are no known algorithms that use this approach. As we said at the beginning of Section 3, we want to combine two phases of VoIP call to achieve, mainly, less significant delay. That is why we will focus on the third possible scenario: the simultaneous authentication and integrity protection of audio and signalling messages. All the following considerations, figures and schemes apply to the scenario No. **III**.

4.2   General Digital Watermarking Scheme Modifications

The scheme presented here requires modifications to the general audio watermarking system. First, we are proposing to add a new functional block called Pre-processing Stage (**PPS**). It will be responsible for preparing data before the watermark embedding stage. The modified scheme, with this new block, is shown in the Fig. 1 below:
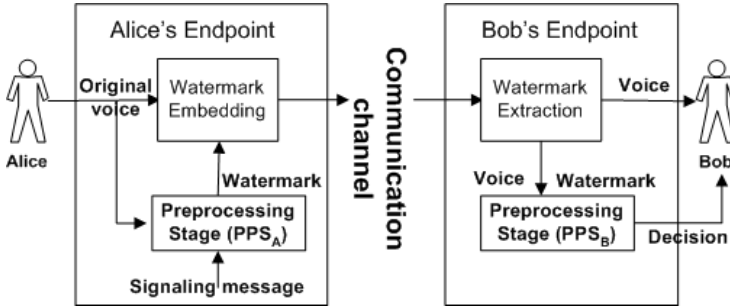

Fig. 1. Modified watermarking scheme with the new Pre-processing Stage (PPS)

As we see in the Fig. 1 we provide a signalling message and a sample of the caller's original voice, as an input to the PPS block in the transmitter. How the PPS block process information will be covered later in the Section 4.4. After the digital watermark is embedded and sent through the communication channel, the information in the receiver is retrieved and verified in an analogous block on the other communication side. If the retrieved information is correct, the connection will continue. We must also consider the problems connected with the call quality degeneration parameters, such as the packet loss and jitter (characteristic for IP networks). The connection cannot break down if the watermark is not retrieved correctly in few samples. The problem will be addressed in the Section 4.5.

The next important thing for this scheme is how much information we are able to embed into the original voice data. This will influence the speed of the authentication and integrity process throughout the conversation. This parameter, in our solution, is expected to be high but it is not crucial. However, the lowest payload watermarks (about 1 bit/s) cannot be accepted in our scheme because, in this case, the conversation would have to last enormously long to work correctly.

4.3   Pre-processing Block (PPS) Description

In this section we will describe how the Pre-processing Stage (PPS) block (presented in Fig.1) is built, in greater details. It consists of functional blocks shown in Fig. 2, which are described below.

The blocks constituting PPS have the following functions:

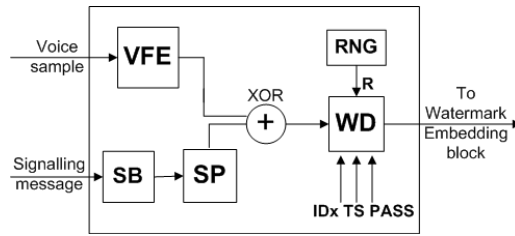**SB** (Signalling Message Buffer): stores the signalling messages from the first phase of the call.

Fig. 2. Architecture of Pre-processing stage block (PPS)

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, even if the rest of information provided will be the same again (e.g., all the signalling messages were verified, so in this case we use the last one that was sent). It produces a random value R, which is included later in the watermark.

WD (Watermarking Data): in this block the input data is concatenated with the obligatory R parameter (the randomizer value) and other parameters: IDX (unique, global identifier of one side of the connection; X means caller or callee), PASS (the password, which is shared and known to both sides of the conversation) and TS (time stamp). The last parameter can be optional, because it requires tightly synchronized clocks. However, it is useful since it can protect against the replay attacks.

VFE (Voice Feature Extractor): provides characteristic features (VF) of the original voice that we want to protect. Afterwards, a hash is also performed on this value.

As we can see in the Fig. 2, all the sent signalling messages from the first phase of the call are stored in a special buffer (SB). When the voice sample enters the VFE block, the first signalling message is send to the SP block where a hash function is performed. Simultaneously, the same function is performed over the voice sample in VFE. Then, both values are XORed bit by bit and the results enter WD block. The input value is concatenated with the randomizer value (R), the global identifier of caller (IDX), a shared password (PASS) and, eventually, the time stamp (TS). After that, the hash function is performed again. The result, which we will call a **token,** is send to the embedding function and will become a **watermark**. Next, the watermarking process continues for the other signalling messages in the SB buffer. Before the caller's voice reaches the callee, the token from the watermark must be retrieved and verified. This can be done because the callee computes locally the same token, and then the two tokens are being compared.

4.4 The Authentication and Integrity Scheme

The general idea of the proposed scheme is to compare the received token with a locally calculated, appropriate one. Fig. 3 shows how the algorithm works (the inverse communication is analogous).
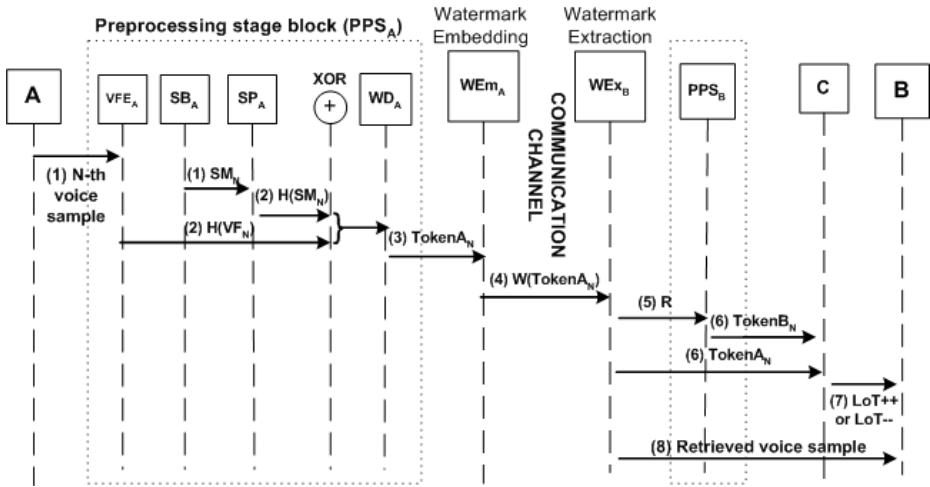
Fig. 3. Architecture of Pre-processing stage block (PPS)

In this situation the values of the tokens A_N and B_N are:

$$\mathbf{TokenA_N = TokenB_N = H}\left((H(SM_N) \oplus H(VF_N)) \, \| \begin{pmatrix} \mathbf{TS} \\ \mathbf{PASS} \\ \mathbf{ID_A} \end{pmatrix} \| \mathbf{R} \right) \| \mathbf{R}$$

PPS_B block is functioning analogously to PPS_A. That is why it is not shown above in details. Additionally, we assume that in the signalling phase some of the signalling messages (SM_N means N-th Signalling Message) were exchanged (and they are stored in SB). Now, in the second phase, they will be verified. **H** stands for the hash function and **W** for the embedding of the digital watermark into audio. The algorithm works as described below:

(1) When the conversation begins, the first voice sample enters VFE_A block and, simultaneously, the first signalling message (SM) is send from the buffer (SB_A) to the SP_A block. In the VFE_A the feature of the voice sample (VF_N) is extracted (for the data integrity) and then the hash function is performed on the result. At the same time, the hash function is performed on the signalling message in SP_A.

(2) The result values from SP_A and VFE_A are, then, XORed (they have the same length). Afterwards, the result is sent to WD_A block, in which **TokenA** is created, together with the other parameters like: the randomizer value (R), the shared password (PASS), the global identifier of A (ID_A) and, optionally, the time stamp (TS).

(3) TokenA is sent to the watermark embedding function and the information, that it contains, is saved there in the caller's voice. Then, the data stream, formed this way, is sent through the communication channel.

(4) Before the voice from A reaches the callee B, the watermark is extracted and send to the comparator (C) on the receiver side.

(5) From the extracted token, the randomizer value (R) is sent to the analogous PPS_B block. In this block some pre-processing had taken place (e.g., the hash function from signalling message was performed). If we have the R-value, then we can compute **TokenB**. It should be equal to TokenA, if the transmission had not been tampered. The result is sent to the comparator (C).

(6) In the comparator (C) both token values are compared.

(7) If TokenA=TokenB, the special parameter LoT (Level of Trust) value (its function will be covered in the Section 4.5) is increased. In any other situation it is decreased. Then, basing on LoT value, the decision is made whether the call should be continued or broken down.

(8) If the call continues, the voice sample finally reaches the callee B.

4.5 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 will update special parameter named LoT (Level of Trust), during a conversation. As we said, if tokens are equal, the LoT parameter increases. In any other situation its value decreases. If A sends to B a token to compare, the algorithm of handling the LoT parameter (on B side) works as described below in a pseudo-code:

```
/*CL - Critical Level, LoT - Level of Trust, T-timer*/
START
CL = a; LoTA = x; TA = 0; /* Initiating values */
StartTimer(TA);
FOR (i = 0; i++; i< End of Transmission)  /* i - Time
slot */
  {
  IF (TokenA_A = TokenA_B) THEN
    {
    LoTA ++;
    ResetTimer(TA);
    }
  ELSE (LoTA --);
 IF (LoTA <= CL) OR (TA > k) THEN STOP; (1)
 IF (LoTA = a*x) THEN LoT = x; (2)
}
```

As we can see, the breakage of the call will take place if the value of the LoT parameter is equal or below the given threshold (CL value) or if the timer TA expires (1). If the communication continues and every signalling message that was sent is verified, embedding of the digital watermark does not stop. It is a continuous process: to calculate information to be sent, as soon as all the signalling messages are verified, we take the last signalling message. The LoT value changes during the conversation time. If every signalling message is successfully verified the LoT value rises. To prevent its increase from reaching the infinity, we lower it, as soon as it reaches the value of the critical level multiplied by the start value of LoT (2).

This way of decreasing the LoT value has one serious disadvantage: it allows an attacker to wait until LoT= (a*x)-1. However, we must assume that he is able to possess information about its value and then safely spoof ((a*x) - 1 – (CL + 1)) audio packets without LoT's falling below the threshold (CL). To prevent it, one must choose the initiating values (a and x) carefully. Their values should depend on network's parameters e.g. the packet loss and possible delays. So it can be, for example, a function (F) of the following parameters:

$$LoT = F (Packet\_loss\_ratio, Delay, Bit\_Error\_Rate, …)$$

If the network does not suffer heavily from the packet loss, those values must be low. In the other case, they must be set to a higher level. For example, the network administrator or service provider can circumscribe those parameters for a certain network/user.

5   Implementation of the Scheme for VoIP Based on SIP

SIP is one of the most popular application-layer (TCP/IP model) signaling protocols for IP Telephony that can establish, modify, and terminate multimedia sessions, such as VoIP calls. It is text-based and simple. SIP specification [14] defines only six main methods: REGISTER for registering contact information, INVITE, ACK, and CANCEL for setting up sessions, BYE for terminating sessions and OPTIONS for querying servers about their capabilities. SIP uses network elements called proxy or redirect servers to help route requests to the user's current location, authenticate and authorize users for services, implement provider's call-routing policies, and provide features to users. Our scheme for this signaling protocol is described below. Our mechanism will be integrated with SIP UA and in case of interconnection scenarios also with Media Gateways (MGs). We will show scenario for basic call flow for VoIP based on SIP, which are taken from [15]. In this scenario, Alice completes a call to Bob directly:

Both sides know what signaling messages were exchanged during the signaling phase of the call. The tokens flow for this call is the following:
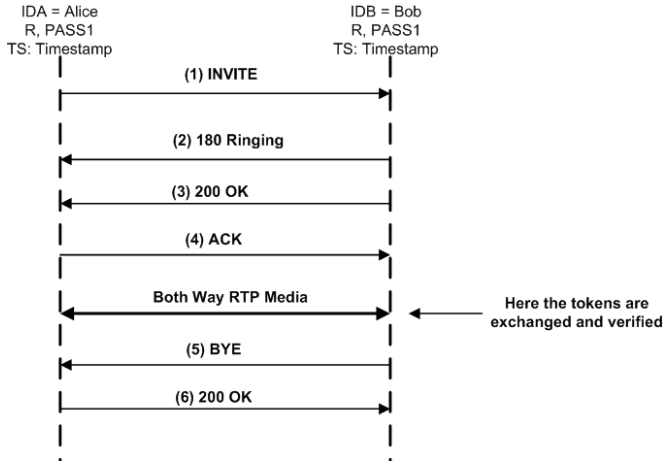
Fig. 4. Connection stages and signalling messages exchanged for SIP

Alice sends to Bob:

(1)
$$\textbf{TokenA}_1 = \textbf{H}\left((\textbf{H(INVITE)} \oplus \textbf{H(VF}_{A1})) \parallel \textbf{TS}_1 \parallel \textbf{PASS}_1 \parallel \textbf{ALICE} \parallel \textbf{R}_1 \right) \parallel \textbf{R}_1$$

(4)
$$\textbf{TokenB}_2 = \textbf{H}\left((\textbf{H(180RINGING)} \oplus \textbf{H(VFB}_{B1})) \parallel \textbf{TS}_1 \parallel \textbf{PASS}_1 \parallel \textbf{BOB} \parallel \textbf{R}_3 \right) \parallel \textbf{R}_3$$

Bob sends to Alice:

(2)
$$\textbf{TokenA}_4 = \textbf{H}\left((\textbf{H(ACK)} \oplus \textbf{H(VF}_{A2})) \parallel \textbf{TS}_2 \parallel \textbf{PASS}_1 \parallel \textbf{ALICE} \parallel \textbf{R}_2 \right) \parallel \textbf{R}_2$$

(3)
$$\textbf{TokenB}_3 = \textbf{H}\left((\textbf{H(200OK)} \oplus \textbf{H(VFB}_{B2})) \parallel \textbf{TS}_2 \parallel \textbf{PASS}_1 \parallel \textbf{BOB} \parallel \textbf{R}_4 \right) \parallel \textbf{R}_4$$

If any new message is exchanged during the connection, for example, for nego-tiation of any parameter of the call, then it does not influence the call until its au-thentication and integrity is checked. The tokens are analogous as it is shown above.Authentication of BYE (or CANCEL) messages, which is used to terminate a VoIP conversation, has to be treated the same as normal messages that come during the call. Normally, the media channels are terminated, upon receiving this message. In our scheme, it is vital to retain RTP flow until those messages are authenticated. So, the authentication and integrity check of messages BYE and the OK are as follows:

Bob sends to Alice (for N-th exchange of the tokens):

$$\textbf{(5)} \quad TokenB_5 = H\left((H(BYE) \oplus H(VFB_{BN})) \parallel TS_N \parallel PASS_1 \parallel BOB \parallel R_N \right) \parallel R_N$$

Alice sends to Bob (for (N+1)-th exchange of the tokens):

$$\textbf{(6)} \quad TokenA_6 = H\left((H(200OK) \oplus H(VFB_{A(N+1)})) \parallel TS_{(N+1)} \parallel PASS_1 \parallel ALICE \parallel R_{N+1} \right) \parallel R_{N+1}$$

Only after those messages are authenticated and their integrity is verified, the flow of RTP packets is stopped and conversation is over. The schemes for other scenarios are analogous. If network servers of SIP functional architecture are used (proxy or redirect), then only certain fields of signalling messages can be used. Some fields must be left free for routing purposes.

6 Conclusions and Remarks

In this paper the new, lightweight authentication and integrity scheme for VoIP, based on the digital watermarking, has been proposed. It is a new approach that combines securing the signalling protocol's messages and audio, which are exchanged between calling parties at the same. The scheme was described for any VoIP system, in general. The new functional blocks and algorithms were also defined. We showed, how this solution works and how it could be implemented for VoIP based on SIP (Session Initiation Protocol) signalling protocol, for a basic call flow.

The presented solution is a *post factum* method because it works some time after the phase of exchanging the signalling messages took place. So, this mechanism can be used only if the connection was previously established. Nevertheless, we find it useful and flexible because this algorithm does not depend on the signaling protocol, gives new potential possibilities for securing and providing compatibility of IP Telephony. Moreover, it does not consume any additional bandwidth because it uses watermarking technique. As proved in [17], there is a need for using lightweight authentication mechanisms, especially for transmissions that depend on certain values of QoS parameters and VoIP service is the best example of that. Implementing such a solution can greatly reduce number of possible attacks (but it will not eliminate them completely) and improve overall system's security.

References

1. J. Dittmann, A. Mukherjee, M. Steinebach: Media-independent Watermarking Classification and the need for combining digital video and audio watermarking for media authentication, Proceedings of the International Conference on Information Technology: Coding and Computing, IEEE Computer Science Society, Las Vegas, Nevada, USA (2000) 62-67.
2. M. Steinebach, F. Siebenhaar, C. Neubauer, R. Ackermann, U. Roedig, J. Dittmann: Intrusion Detection Systems for IP Telephony Networks, Real time intrusion detection symposium, Estoril, Portugal (2002).

3. S. Yuan, S. Huss: Audio Watermarking Algorithm for Real-time Speech Integrity and Authentication, International Multimedia Conference Proceedings of the 2004 Multimedia and security workshop on Multimedia and security, Magdeburg, Germany (2004) 220 - 226

4. M. Sienebach, A. Lang, J. Dittmann, Ch. Neubauer: Audio Watermarking Quality Evaluation: Robustness to DA/AD Processes, Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC '02), Las Vegas (2002) 100-105.

5. T. Mizrahi, E. Borenstein, G. Leifman, Y. Cassuto, M. Lustig, S. Mizrachi, N. Peleg: Real-Time Implementation for Digital Watermarking in Audio Signals Using Perceptual Masking, 3rd European DSP Education and Research Conference, ESIEE, Noisy Le Grand, Paris (2000).

6. C. Lu, H. Liao, L. Chen: Multipurpose Audio Watermarking, Proceedings of 15th International Conference on Pattern Recognition, Barcelona, Spain, pp. 282-285 (2000).

7. M. Arnold: Attacks on Digital Audio Watermarks and Countermeasures, Third International Conference on WEB Delivering of Music (WEDELMUSIC'03), Leeds, United Kingdom (2003).

8. D.R. Kuhn, T.J. Walsh, S. Fries: Security Considerations for Voice Over IP Systems, Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology Special Publication 800-58, January 2005.

9. J. Dittmann, P. Wohlmacher, K. Nahrstedt: Using Cryptographic and Watermarking Algorithms. IEEE MultiMedia 8(4): 54-65 (2001).

10. M. Steinebach; J. Dittmann: Watermarking-based digital audio data authentication, EURASIP Journal on Applied Signal Processing, No. 10, September; Hindawi Publishing Corporation, pp 1001 - 1015, ISBN ISSN 1110-8657, 2003.

11. J. Dittmann, F. Nack, A. Steinmetz, R. Steinmetz: Interactive Watermarking Environments, Proceedings of International Conference on Multimedia Computing and Systems, Austin, USA 1998, pp. 286-294.

12. J.D. Gordy, L.T Brutin: Performance evaluation of digital audio watermarking algorithms, in Proc. 43rd IEEE Midwest Symposium on Circuit and Systems (MWSCAS '00), pp. 456-459, Lansing, USA, August 2000.

13. M. Arnold: Audio watermarking: Features, applications and algorithms, in Proc. IEEE International Conference on Multimedia Expo (ICME '00), pp. 1013-1016, New York, USA, July-August 2000.

14. J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, RFC 3261 - SIP: Session Initiation Protocol, IETF, June 2002.

15. A. Johnston, S. Donovan, R. Sparks, C. Cunningham, K. Summers, RFC 3665 - Session Initiation Protocol (SIP) Basic Call Flow Examples, IETF, December 2003.

16. ISO 7498. International Standards Organisation (ISO). Information processing systems - Open systems interconnection - Basic reference model - Part 2: Security architecture (ISO/IEC 7498-2). 1989.

17. H. Johnson, Toward Adjustable Lightweight Authentication for Network Access Control, PhD thesis, Blekinge Institute of Technology, December 2005.