ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

A Lightweight Network Code based Authentication Scheme to thwart Pollution attacks in H.264/AVC Video Streaming

C. Sunitha [1], A. Abdul Faiz[2]

HOD, Department of BCA, Sri Krishna College of Arts and Science, Coimbatore, Tamil Nadu, India[1]

M.Phil. Scholar, Department of Computer Science, Sri Krishna College of Arts and Science, Coimbatore, Tamil Nadu, India[2]

ABSTRACT: Wireless communication channels are grown tremendously. Multimedia applications are using different wireless communication channels. Multimedia content verification and endorsement has become a rising issue for continuous video streaming. Especially this is a major issue over lossy/congested networks, which refers the network gives a lot of Timeout errors when packets are transmitted over it. Even though, several video coding standards are introduced to reduce the data size on the communication channel, the dependency of coding created new challenges and issues. Such video coding standards such as H.261, CCIR 723, MPEG-1 and MPEG-2 H.264/AVC has several challenges in inventing effective authentication scheme. In this proposal, we propose a lightweight authentication scheme against pollution attacks that integrates authentication into source and channel coding components such as coderate, conventional length, which helps to efficiently address the coding reliance and to design the optimal rate allocation scheme for the sake of end-to-end video quality. The proposed lightweight authentication framework is able to authenticate the video streaming with low communication overhead. In general, the quality will get affected by the noise in wireless channel and unsuccessful authentication. We proposed a new channel, source and receiver authentication scheme named as VSA (Video streaming Authentication). VSA provides continuous authentication with H.264 coding and channel rate allocation schemes. The experimental results on H.264/AVC video streaming confirm the effectiveness of this VSA and demonstrates that comparison with other video authentication schemes.

KEYWORDS: Lightweight authentication, Multimedia authentication, digital signature, stream authentication, wireless media communication, H.264 video streaming.

I. INTRODUCTION

The current Internet scenarios dominated by several video related applications, these applications are endorsed by the prompt growth of the network technologies, social networks and media coding standards. For example, YouTube has over a billion users worldwide and almost 55% internet traffic spent for those video streaming servers. With the growth of mobile devices, several applications are running on the mobile ends. The number of hours people spend watching videos on YouTube is up 60%. Due to this popular nature on video related applications, several Security issues arise [1]. In specific wireless media are more vulnerable to illegitimate and unauthorized access. The following fig 1.0 shows the continuous authentication process on video streaming.

The key goal of our work is to utilize the spaces available in standard random Network Coding to design a secure media streaming architecture that is inherently resilient to pollution attack in multimedia video streaming. When comparing with the existing works, most of the implementations focus either on identification and isolation of the malicious nodes or on designing ad-hoc data verification techniques. But those systems finds very critical to identify the malicious uploader and that techniques are very limited with network regions and thus increased computational complexity and/or communication overhead.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

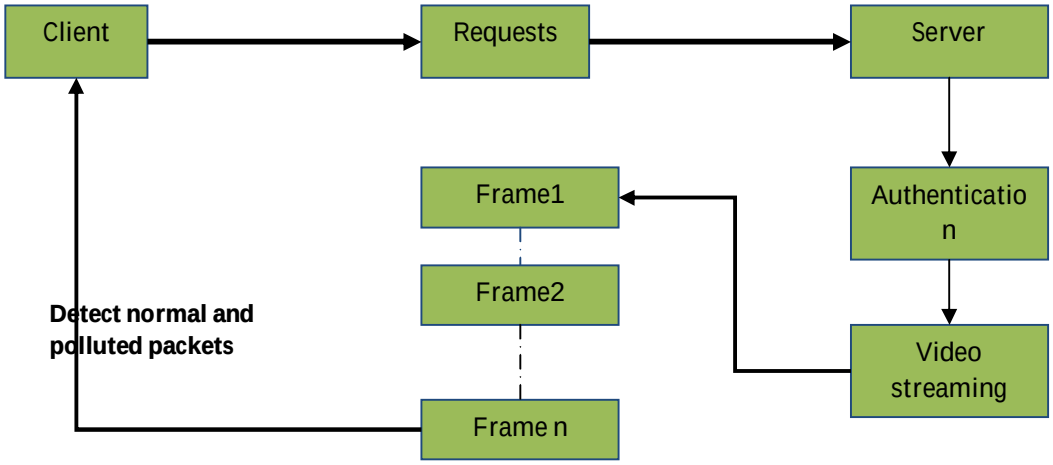

Fig 1.0 Video streaming process

In this paper, we focus on the issue of authenticating and securing video streaming without degrading the performance and quality. The authentication refers the source authentication, receiver authentication and integrity oriented. In integrity process, the data security is verifying the data and confirming that the data is not maliciously changed in streaming. The next process is Source authenticity, which refers to that the media content is indeed sent by the claimed sender. Non negation refers that the sender could not deny the fact of sending the media content. If received media cannot be verified by the beneficiary it should not be consumed and therefore the quality of consumable media is impaired. Additionally receiver authentication is performed.

II. PROBLEM DEFINITION

Recent multimedia applications will make continuous media stream on internet. It is very essential to thwart the data from Hackers and eavesdroppers. These types of threads technically called as potential threats from corrupting or stealing the valuable information that is being passed through the network communication [2][3]. The main Aim of Secured Video streaming is to offer: content tracking, copy control, authentication, conditional access, confidentiality. Conventional video stream authentication schemes build authentication graphs on transmission units or packets, in which the directed edge in the graph corresponds to hash appending and the cluster head is signed using digital signature, which has been proven to be an effective solution to the strict data authentication issues. To empower video content, several approached used digital signature concepts to avoid the unauthenticated access and failure in data transmission. This discussion empowers authentication graph and maximizes the verification probability of the transaction.

To efficiently utilize the power of digital signature while avoid the undesired authentication failure due to the packet loss in transmission, the authentication graph[4] has to be carefully designed to maximize the verification probability of the transmission units, which requires to increase the number of hashes appended. On another hand, to reduce the overhead generated by authentication, it requires to reduce the number of hashes. These two requirements are intrinsic contradictive and the design target of graph based algorithm is to find a proper balance between them. End-to-end quality is another important design target for multimedia transmission, in particular when channel is lossy and the transmission rate is limited. To achieve high end-to-end quality, it is common to apply channel coding on media. However most existing authentication schemes consider channel coding separately from authentication and simply treat channel coding as a method to reduce packet loss rate. Although low authentication overhead is a design target, how to optimally allocate rate for authentication, source coding and channel coding is not considered in most authentication schemes at all.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

a. Problems in video transmission:

1. In traditional video transmission process, we should tolerate some data content loss, but the data content is not changed. This content loss happens at the time of lossy compression process and lossy transmission. This type of problems increases the vulnerability and malicious attacks.
2. The end-to-end quality could achieve only on the high important data units, not the whole.
3. There are coding reliance relationships between the authentication scheme and the encoded units should be reliable with the coding dependency.
4. In terms of secure video authentication, the channel coding is generally applied. Those authentication schemes may create high authentication overhead. To reduce the authentication overhead, the authentications scheme should coherent with the error protection scheme.

The video authentication has the following additional challenges the following two challenges prohibit the direct application of the layered joint design framework on H.264/AVC. First, the unique coding dependency structure in H.264/AVC has to be considered. The coding dependency relationship between the compressed H.264/AVC video units is fundamentally different from the scalable coding structure in JPEG-2000 image [5].

III. RELATED WORKS

In recent scenario video streaming authentication is emerged with new techniques and schemes. Such techniques providing authentication of different video encoding techniques referred as H.264/AVC. Several works concentrates on content authentication, which is based on watermarking schemes [6][7]. Invisible watermarking is embedded into the video content and that will be used to authenticate. This invisible watermarked content will be verified by the receiver in order to identify malicious attacks. Some authors [8] proposed stream level scheme, which follows a hop by hop verification strategy. While comparing with the content based authentication schemes, the stream level authentication produces false alarms.

But the content based schemes utilize pattern recognition like techniques to detect features. And this has probability of false negative and false positive errors. Additionally the content based schemes consider the channel errors and this will not utilize channel information at all. Authors of [9] [10] has extended efficient stream authentication scheme, which extended H.264/SVC scheme along with hybrid authentication technique. But only a few stream level authentication works on AVC. A hash generation and signature based scheme is proposed to authenticate each set of videos in the streaming server [11]. In [12] a feature based fingerprint is first generated and then signed, in which security relies on the robustness of the fingerprint. It is necessary to further develop efficient stream level authentication schemes for H.264/AVC to achieve the goals of high authentication possibility and this provides low authentication overhead and high end-to-end quality.

IV. PROPOSED SYSTEM

We have proposed a lightweight authentication framework called Video Streaming Authentication (VSA). The lightweight authentication considers the verification and transmission of video streaming on lossy network and reducing verification overhead on lossless networks. So VSA provides both high verification probability and low authentication overhead in continuous video streaming environment. Our proposed lightweight Layered authentication is an identity and access management process that is implemented in the secure video streaming, which has a high exposure to risk and fraud. This is typically used to authenticate individuals before granting access to a particular system and requires more evidences and verifications of identity for authentication. The layered lightweight authentication-based video streaming requires two or more identity credentials for authentication.

The security of the proposed scheme only relies on the underlying cryptographic algorithms for hashing and signature generation. In the proposed system, SHA-2 is used for hashing and RSA is used for signature generation. So the system security is the same as other data stream authentication schemes. In this paper we presented an efficient authentication scheme for wireless video streaming on H.264/AVC. With the help of H.264 channel and source information VSA simultaneously handles several media quality issues. Our work also guarantees end-to-end video streaming quality. Our proposed scheme is able to achieve 100% effective verification probability of source, receiver and hop-by-hop authentications and this has achieved with low authentication over-head.

Contributions

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

In this paper we present a lightweight authentication scheme named as VSA, which need more verification properties in H.264/AVC video coding, this utilizes the channel information and characteristics of the video coding standard. Based on these approaches, we develop a lightweight scheme based on video source coding dependency and wireless channel condition. To overcome the several security and quality issues, we present a new technique named as VSA , which protects, authenticates and streams the H.264/AVC video effectively. Our proposed technique concentrates on source, channel and destination authentication in lossy network. The original contributions of this lightweight adaptive scheme are as follows.

1) Our proposal improves the detection of polluted packets in live video streaming.
2) We enhance the existing joint source-channel adaptive scheme method along with network code authentication scheme which makes suitable for the H.264/AVC video streaming. This is the first work trying to address the source, channel and destination authentication problem in the live video streaming over lossy network.
3) We recognized several security issues in H.264/AVC video streaming, channel authentication with video coding information.
4) We enhance and accelerate the H.264/AVC video streaming with source, channel and integrity verification.
5) We perform the above authentication and pollution detection methods in hybrid content delivery networks such as CDN and P2P. For that we proposed a new scheme named as video streaming_ H.264/AVC [13].

V. PROPOSED SYSTEM FRAMEWORK

The proposed adaptive authentication strategy, Multi factor (Video Streaming Authentication) is shown in Figure2.0. The existing standard streaming authentication schemes usually consider transmission packet as the basic authentication unit and authentication information is appended after packetization. After transmission over lossy channel, packets are first verified before they are transmitted. Untested packets are then discarded without further accumulation and utilization.

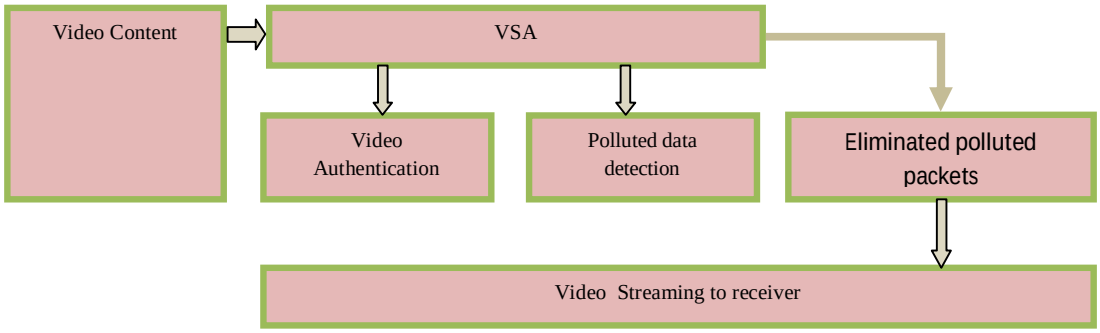

Fig 2.0 VSA process at sender side

The above fig 2.0 shows the process of VSA, which utilizes source and channel authentication along with adaptive rate allocation while streaming H.264/AVC videos. The fig 3.0 shows the receiver side process of proposed VSA. This process has receiver authentication with existing video streaming process and the reconstructed video will be transmitted to the receiver.

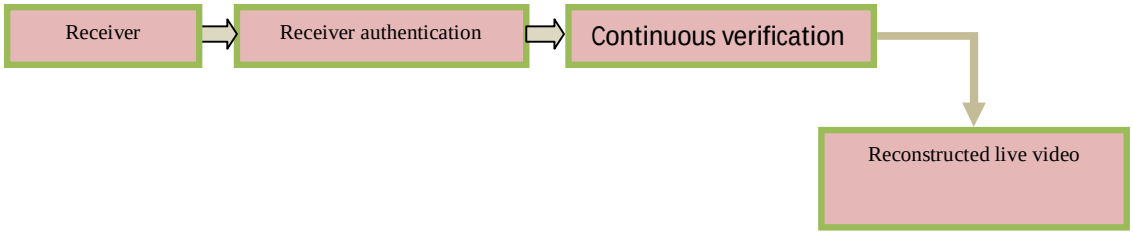

Fig 3.0 VSA process at Receiver side

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

The proposed source-channel adaptive authentication scheme hews out a new path by shifting authentication backward to consider the source coding, authentication, and channel coding jointly. The joint layered design module takes the video content as input and carries out coding dependency analysis on the encoded NAL units and makes decision on the layer division on the NAL units, so that the NAL units are assigned to NAL sets that will be protected on different levels. The joint design scheme further carries out the rate distortion analysis on the encoded video content and allocates the source rate, authentication rate and channel coding rate optimally. The optimal decision process is an iterative process that gradually approaches the optimal rate assignment**.**

VI. RESULTS AND DISCUSSION

We use H.264 coding standard and the number of frame is 60 per minute. For each second, the number of transmission packet is set to 10. The hash function is SHA-2 with hash size 224 bits. A signature of length 1024 bits is generated by RSA for each video segment. Two types stream authentication schemes are selected for comparison with proposed VSA . One is JMEAP and Low overhead SVC Authentication (LSVCA) [14], the performance metrics are listed in Table 1.0.

Metrics
Verification delay
authentication delay
Communication and Computation overhead

Table 1.0: performance metrics

The above metrics such as computation overhead refers the number of hash operations and signature process done at source and receiver. The communication overhead has been calculated for every packet at the time of streaming. This includes the number of extra bits carried by every packet for the validation. Using this verification delay calculated. Additionally the sender authentication and receiver authentication delay is compared.

Metrics	VSA	LSVCA	JMEAP
Reduced % of verification delay	12.3%-13.1%	2.1%-2.4%	11%-12.4%

Table2.0 Comparison table

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

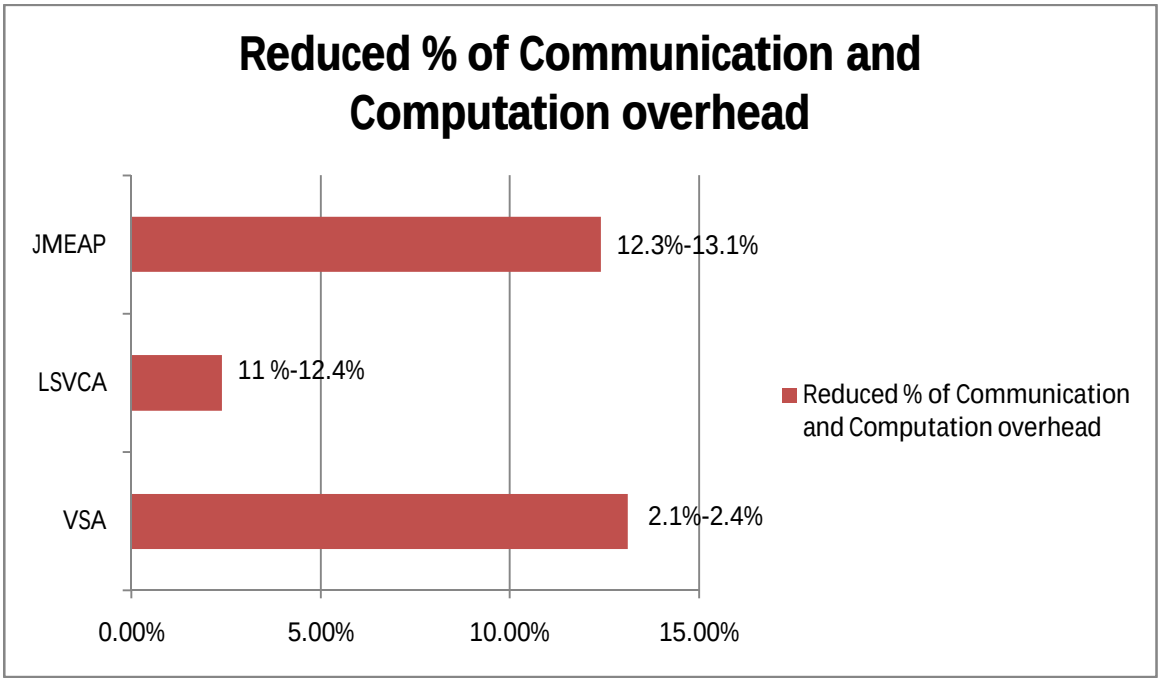

Fig 4.0 comparison study between different video authentication techniques

The above table2.0 and fig 4.0 shows the comparison of existing and proposed system with the respective of reduced communication overhead. The LSVCA scheme reduces the overhead by 2.1 % , in JMEAP 11% overhead are reduced from the total overhead. In the proposed work it is 12.3%.

VII. CONCLUSION

In this paper we presented an efficient lightweight authentication scheme for lossy network wireless H.264/AVC video streaming. The proposed system completely utilizes the H.264 source and channel components simultaneously. This resolves many issues, which are related to the video streaming. This extensively extends the existing video streaming framework for source and receiver authentication and introduces a network code authentication for channel authentication named as VSA . We combined the dependency of video encoding and the channel components with effective hashing technique. These processes are integrated in lossy or congested networks. We integrate the coding dependency relationship into the lightweight authentication framework, together with the hash embedding. The proposed scheme is able to achieve 100% effective verification probability while maintaining low authentication over-head. The results and analysis shows the proposed work reduces the communication and computation overhead up to 13% from the existing system.

REFERENCES

1. [Online]. Available: https://www.youtube.com/yt/press/statistics.html
2. Zhu, Xiaoqing, and Bernd Girod. "Video streaming over wireless networks."*Proceedings of the European Signal Processing Conference, EUSIPCO-07, Poznan, Poland*. 2007.
   A. Perrig, R. Canetti, J. D. Tygar, and D. Song, "Efficient authentication and signing of multicast streams over lossy channels," in *Proc. IEEE Symp. Secur. Privacy*, May 2000, pp. 56–73.
3. Z. Zhang, Q. Sun, W.-C. Wong, J. Apostolopoulos, and S. Wee, "An optimized content-aware authentication scheme for streaming JPEG-2000 images over lossy networks," *IEEE Trans. Multimedia*, vol. 9, no. 2, pp. 320–331, Feb. 2007.
4. X. Zhu and C. W. Chen, "A joint source-channel adaptive scheme for wireless H.264 video authentication," in *Proc. IEEE Int. Conf. Multimedia Expo (ICME)*, pp. 13–18, Jul. 2010.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

5. G. Qiu, P. Marziliano, A. T. S. Ho, D. He, and Q. Sun, "A hybrid watermarking scheme for H.264/AVC video," in *Proc. 17th Int. Conf.Pattern Recognit.*, vol. 4. Cambridge, U.K., Aug. 2004, pp. 865–868.
6. D. Pröfrock, H. Richter, M. Schlauweg, and E. Müller, "H.264/AVC video authentication using skipped macroblocks for an erasable watermark," in *Proc. (VCIP)*, Beijing, China, Jun. 2005.
7. U. Shintaro, S. Hiroshi, and O. Ken-Ichi, "NAL level stream authentication of H.264/AVC," *IPSJ Digital Courier*, vol. 3, pp. 55–63, 2007.
8. K. Mokhtarian and M. Hefeeda, "Authentication of scalable video streams with low communication overhead," *IEEE Trans. Multimedia*, vol. 12, no. 7, pp. 730–742, Nov. 2010.
9. Y. Zhao, S.-W. Lo, R. H. Deng, and X. Ding, "Technique for authenticating H.264/SVC and its performance evaluation over wireless mobile networks," *J. Comput. Syst. Sci.*, vol. 80, no. 3, pp. 520–532, 2014.
10. N. Ramaswamy and K. R. Rao, "Video authentication for H.264/AVC using digital signature standard and secure hash algorithm," in *Proc. Int. Workshop (NOSSDAV)*, Newport, RI, USA, May 2006.
11. Y. J. Ren, L. O'Gorman, L. J. Wu, F. Chang, T. L. Wood, and J. R. Zhang, "Authenticating lossy surveillance video," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 10, pp. 1678–1687, Oct. 2013.