Live Video Streaming Authentication for Vehicle Multimedia based on Merkle Tree

Dongqi Han[1], Jindong Zhang[1.2, 3, a)], Yang Liu[1], Peibin Wu[1,] Yiding Sun[1]

[1] *College of Computer Science and Technology, Jilin University, Changchun, 130012, China*
[2]*Key Laboratory of Symbol Computation and Knowledge Engineering of the Ministry of Education, Jilin University, Changchun,130012, China*
[3]*State Key Laboratory of Automobile Simulation and Control, Jilin University, Changchun 130025, China*

[a)] Corresponding author: zhangjindong_100@163.Com

Abstract. Merkle tree has been widely applied in the field of P2P transmission. In this paper, an efficient authentication scheme is proposed in the integrity check module for vehicle live video streaming system by optimizing the construction and verification of the Merkle tree. It can create and check nodes at the same time in a shorter time without trusted channel. At the same time, in order to prevent the oversensitivity of hash algorithm, this paper uses the perceptual hash algorithm to generate the hash value of nodes in the Merkle tree. After performance evaluation and analysis, our algorithm can build a Merkle tree with 2N-1 nodes only after the N+log2N times hash calculation. It has better time performance than the traditional tree, whether receiving attacks or not. And it is proved that the scheme is secure under the condition that the vehicle live video streaming system is safe.

Key words: vehicle streaming media system; Merkle tree; P2P-streaming; integrity authentication; perceptual hash algorithm..

INTRODUCTION

Nowadays, the needs of audio-visual multimedia system are presented for vehicular network, especially with the combination of emerging technologies such as live video and video conferencing. Facing the severe network security situation, it is necessary to verify the transmitted video stream to ensure that the video content is not tampered maliciously.

Merkle tree is a hash method for distributed environment. In recent years, there have been many related studies. The paper [1] describes how it applies to distributed web environment. There is an application for live video streaming in VANETs environment in [3].An integrity verification scheme for data streaming is proposed in [2] to solve the one-wayness problem of Merkle tree. There is an instance of perceptual hash for authentication in [4].

In summary, if the conventional Merkle tree is applied to the vehicle live video streaming system based on P2P streaming media technology, the following problems will appear: waiting for all nodes of live video streaming system to be completed will bring multiple delays; checking integrity only through hash values requires the trusted live video streaming channel; common hash functions are very sensitive to the change of live video streaming information.

Based on these problems, we propose a new tree structure suitable for the vehicle live video streaming system by using the perceptual hash algorithm and optimizing the creation and verification of the Merkle tree.

THE PROPOSED AUTHENTICATION SCHEME BASED ON DYNAMIC MERKLE TREE

In this section, the proposed Merkle tree for integrity check module and the entire procedure using this tree to complete authentication for the vehicle live video streaming system will be introduced.

Integrity Check Module

First, the architecture of the vehicle live video streaming system is shown in Fig.1, and the location of the proposed integrity check module is marked in the system. It can be seen that integrity check is used on each kind of device.

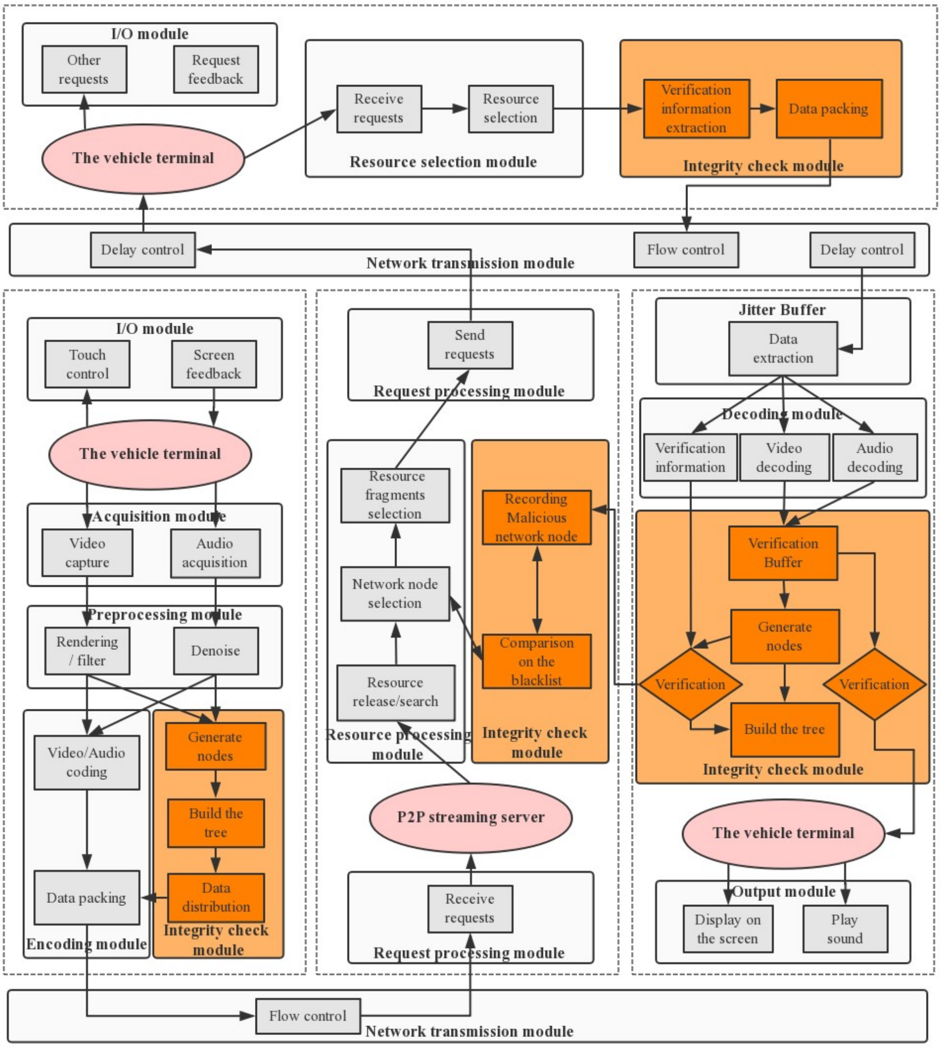

FIGURE 1. The architecture of the vehicle streaming media system with integrity check module

The Proposed Authentication Scheme

Now the authentication scheme based on the tree structure above will be introduced, the vehicle streaming media system can be divided into three categories during the transmission: the receiver, the sender and the video live publisher.

The Video Live Publisher

The workflow of the vehicle streaming media system's video live publisher is shown in Fig.2. We mark and classify the nodes for further description. The hash value of the node whose post-traversing number is *i*, is represented by $H_{(k,i)}$ during *k*-th transmission. $F_{(k,i)}$ is used to represent a video fragment or key frame, it is marked as "available" after two kinds of sets C_i and S_i are also defined, both of them have two elements represented by $c_{(i,0)}$/ $s_{(i,0)}$ and $c_{(i,1)}$/ $s_{(i,1)}$. The method of building the Merkle tree is similar to the traditional tree except that the perceptual hash algorithm is required when the leaf node is built. Each value of $c_{(i,1)}$ and $s_{(i,0)}$ need to be saved for subsequent verification.

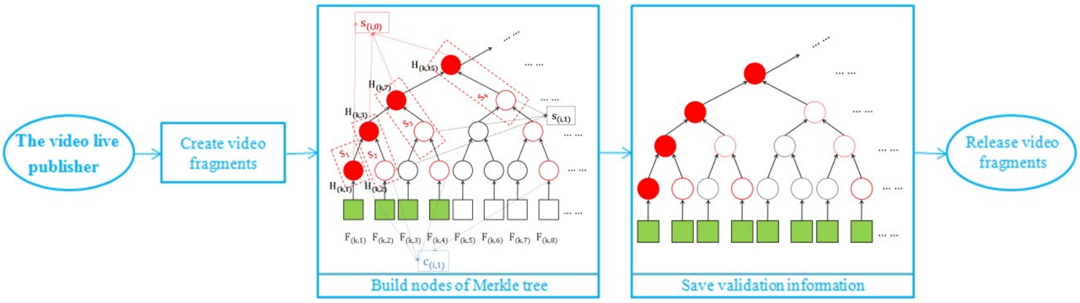

FIGURE 2. The workflow of the video live publisher

The Sender

As is shown in Fig.3, the sender of vehicle streaming media system needs to decide which verification information to transmit according to which set the requested fragment belongs to.

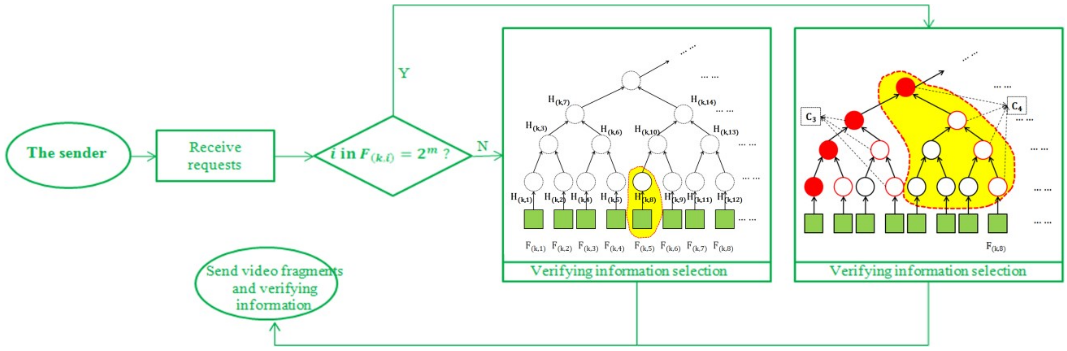
The sender
Receive requests
i in F(k,i) = 2^m ?
Y
N
H(k,7)
H(k,14)
H(k,3)
H(k,6)
H(k,10)
H(k,13)
H(k,1) H(k,2) H(k,4) H(k,5) H(k,8) H(k,9) H(k,11) H(k,12)
F(k,1) F(k,2) F(k,3) F(k,4) F(k,5) F(k,6) F(k,7) F(k,8)
Verifying information selection
C3
C4
F(k,8)
Verifying information selection
Send video fragments and verifying information

FIGURE 3. The workflow of the sender

The Receiver

The workflow of the vehicle streaming media system's receiver is shown in Fig.4.When the vehicle streaming media system receives $F_{(k,i)}$ and verification information, it is divided into two cases: if the leaf node corresponding to $F_{(k,i)}$ is not belong to *C*, the transferred nodes are temporarily used after hash value comparison; otherwise, The two comparison are made as shown in the figure, and the second one is the comparison between $H_{(k,2i-1)}$ in buffer and the hash value of the combination of $H_{(k,2i-2)}$ and $s_{(\log i+1,1)}$. The fragments are marked as "available" after verification.

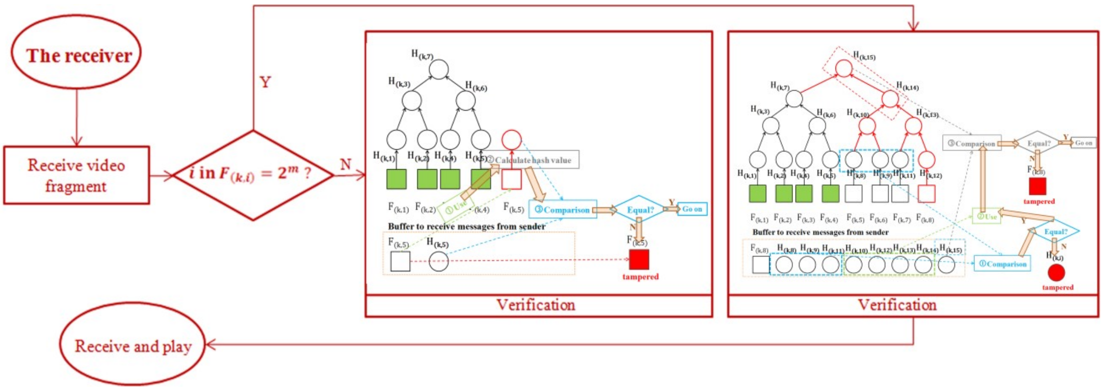

FIGURE 4. The workflow of the receiver

PERFORMANCE EVALUATION AND ANALYSIS

Experiments are performed on a laptop with Intel(R) Core(TM) i7-4710MQ CPU 2.50 GHz 8 GB RAM running on Windows 7 professional equipped with the MATLAB R2010b and python 3.6.3 environment. First, the definitions of video streaming authentication time parameters and their values measured by several experiments are shown in Table 1.

TABLE 1. The definitions and their values of video streaming authentication time parameters.

parameters	t_{ph}	t_h	t_c
meaning	The time for calculating a perceptual hash value	The time for calculating a secure hash value	The time for a comparison
value(s)	0.1622126511	0.01233765221	5.337013135e-06

Next, the proposed scheme is compare with the traditional Merkle tree used in video live in Fig.5. N is used to represent the total number of nodes in a finished tree. $T_1(i,N)$, $T_2(i)$ and $T_3(i,N)$ represent the time from request to play of $F_{(k,i)}$ without any attack, with the attack on images and with the attack on hash values. (a1) (b1) (c1) make comparisons and (a2) (b2) (c2) show the performance of our scheme. It can be seen that the time performance of our scheme is better than the other one in T_1, T_2 and T_3, and it becomes more and more obvious as the parameter increases.

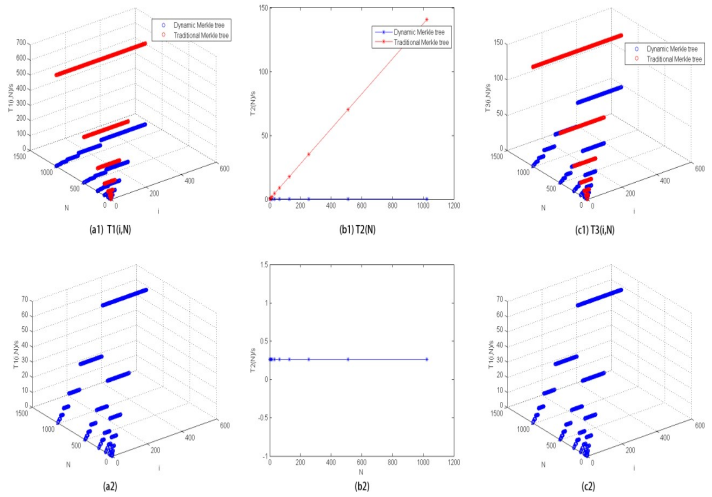

FIGURE 5. The time performance of two ways

CONCLUSION

In this paper, an authentication scheme based on Merkle tree is proposed for vehicle live video streaming system by redefining the nodes' verification and constitution. Through experiments and analysis, it is proved that the scheme is secure under the condition of live broadcast device security. And it has better time performance than the traditional tree, whether receiving attacks or not.

ACKNOWLEDGEMENTS

This work is supported in part by the National Key Research and Development Program of China (2017YFB0102500), Natural Science Foundation of Jilin province (20170101133JC), and Jilin University (5157050847, 2017XYB252, 2017A53216).

REFERENCES

1. Dias D., Benet J. (2016) Distributed Web Applications with IPFS, Tutorial. In: Bozzon A., Cudre-Maroux P., Pautasso C. (eds) Web Engineering. ICWE 2016. Lecture Notes in Computer Science, vol 9671. Springer, Cham.
2. Vinel, A., Belyaev, E., Bellalta, B., & Hu, H. (2014). Live Video Streaming in Vehicular Networks. Paper presented at the Communication Technologies for Vehicles, Cham.
3. Chen, C.-Y., Wu, H.-M., Wang, L., & Yu, C.-M. (2017). Practical integrity preservation for data streaming in cloud-assisted healthcare sensor systems. Computer Networks, 129, 472-480. doi:https://doi.org/10.1016/ j.comnet. 2017.05.032.
4. Zhang, Q.-y., Hu, W.-j., Huang, Y.-b., & Qiao, S.-b. (2018). An efficient perceptual hashing based on improved spectral entropy for speech authentication. Multimedia Tools and Applications, 77(2), 1555-1581. doi: 10.1007/s11042-017-4381-y.