Infocommunications Journal

A PUBLICATION OF THE SCIENTIFIC ASSOCIATION FOR INFOCOMMUNICATIONS (HTE)

December 2016 Volume VIII Number 4 ISSN 2061-2079

Technically Co-Sponsored by

IEEE ComSoc™ IEEE Communications Society

hte

IEEE HUNGARY SECTION

Editorial Board

Editor-in-Chief: ROLLAND VIDA, Budapest University of Technology and Economics (BME), Hungary
Associate Editor-in-Chief: ÁRPÁD HUSZÁK, Budapest University of Technology and Economics (BME), Hungary

ÖZGÜR B. AKAN
Koc University, Istanbul, Turkey
JAVIER ARACIL
Universidad Autónoma de Madrid, Spain
LUIGI ATZORI
University of Cagliari, Italy
LÁSZLÓ BACSÁRDI
University of West Hungary
JÓZSEF BÍRÓ
Budapest University of Technology and Economics, Hungary
STEFANO BREGNI
Politecnico di Milano, Italy
VESNA CRNOJEVIÇ-BENGIN
University of Novi Sad, Serbia
KÁROLY FARKAS
Budapest University of Technology and Economics, Hungary
VIKTORIA FODOR
Royal Technical University, Stockholm
EROL GELENBE
Imperial College London, UK
CHRISTIAN GÜTL
Graz University of Technology, Austria
ANDRÁS HAJDU
University of Debrecen, Hungary
LAJOS HANZO
University of Southampton, UK
THOMAS HEISTRACHER
Salzburg University of Applied Sciences, Austria
JUKKA HUHTAMÄKI
Tampere University of Technology, Finland
SÁNDOR IMRE
Budapest University of Technology and Economics, Hungary
ANDRZEJ JAJSZCZYK
AGH University of Science and Technology, Krakow, Poland
FRANTISEK JAKAB
Technical University Kosice, Slovakia
KLIMO MARTIN
University of Zilina, Slovakia
DUSAN KOCUR
Technical University Kosice, Slovakia
ANDREY KOUCHERYAVY
St. Petersburg State University of Telecommunications, Russia
LEVENTE KOVÁCS
Óbuda University, Budapest, Hungary
MAJA MATIJASEVIC
University of Zagreb, Croatia
VACLAV MATYAS
Masaryk University, Brno, Czech Republic
OSCAR MAYORA
Create-Net, Trento, Italy
MIKLÓS MOLNÁR
University of Montpellier, France
SZILVIA NAGY
Széchenyi István University of Győr, Hungary
PÉTER ODRY
VTS Subotica, Serbia
JAUDELICE DE OLIVEIRA
Drexel University, USA
MICHAL PIORO
Warsaw University of Technology, Poland
ROBERTO SARACCO
Trento Rise, Italy
GHEORGHE SEBESTYÉN
Technical University Cluj-Napoca, Romania
BURKHARD STILLER
University of Zürich, Switzerland
CSABA A. SZABÓ
Budapest University of Technology and Economics, Hungary
LÁSZLÓ ZSOLT SZABÓ
Sapientia University, Tirgu Mures, Romania
TAMÁS SZIRÁNYI
Institute for Computer Science and Control, Budapest, Hungary
JÁNOS SZTRIK
University of Debrecen, Hungary
DAMLA TURGUT
University of Central Florida, USA
ESZTER UDVARY
Budapest University of Technology and Economics, Hungary
SCOTT VALCOURT
University of New Hampshire, USA
JINSONG WU
Bell Labs Shanghai, China
GERGELY ZÁRUBA
University of Texas at Arlington, USA

Indexing information

Infocommunications Journal is covered by Inspec, Compendex and Scopus.
Infocommunications Journal is also included in the Thomson Reuters – Web of ScienceTM Core Collection, Emerging Sources Citation Index (ESCI)

Infocommunications Journal

Technically co-sponsored by IEEE Communications Society and IEEE Hungary Section

Supporters

FERENC VÁGUJHELYI – president, National Council for Telecommunications and Information Technology (NHIT)
GÁBOR MAGYAR – president, Scientic Association for Infocommunications (HTE)

Editorial Office (Subscription and Advertisements)**:**
Scientic Association for Infocommunications
H-1051 Budapest, Bajcsy-Zsilinszky str. 12, Room: 502
Phone: +36 1 353 1027
E-mail: info@hte.hu • Web: www.hte.hu

Subscription rates for foreign subscribers: 4 issues 10.000 HUF + postage

Publisher: PÉTER NAGY

HU ISSN 2061-2079 • Layout: PLAZMA DS • Printed by: FOM Media

A Highly Secure Image Watermarking Authentication Algorithm Based on MECDH and AECDSA

Run Zhang, Yong-Bin Wang, Jin-Yao Yan and Shuang Feng

***Abstract*—This paper proposes a highly secure DSWT (Discrete Stationary Wavelet Transform) domain image watermarking and digital signature algorithm. The algorithm is based on MECDH (Modified Elliptic Curve Diffie-Hellman) key exchange protocol with more secure elliptic curves and SHA-512 AECDSA (Advanced Elliptic Curve Digital Signature Algorithm), both of which are derived from ECC (Elliptic Curves Cryptography) [1] with ECDLP known to be very difficult to solve. Meanwhile, the algorithm run on MIRACL (Multiprecision Integer and Rational Arithmetic C/C++ Library) becomes stronger. Theoretical analyses and experimental results show that the proposed algorithm is more secure and practical to protect the copyrights of multimedia digital works.**

***Index Terms*—AECDSA, ECC, MECDH, MIRACL, Signature Authentication, Watermarking.**

I. INTRODUCTION

Watermarking technology with enough imperceptibility, robustness and security is honored as the last defense line of the digital copyright protection. The scheme can resist normal operation as well as malicious attacks, and protect the copyrights and authenticate data integrity. Therefore, digital watermarking technology and products are widely and deeply researched and used. [2] proposed a multiple watermarking technique and made digital assets secure and undetectable by dividing a host image into two regions. It used LSB to insert the owner information in DWT-DFT domain with a circular watermark. [3] proposed a hybrid algorithm combining encryption and digital watermarking techniques which embedded a cryptographic watermark and the users data in the carrier image to provide confidentiality in telemedicine images exchanging.

However, the security of traditional watermarking needs to be improved with currently powerful cryptography technology. Started in 1985, Neal Koblitz and Victor Miller put forward the concept of ECC scheme independently, without noticing the counterpart's existence. Since then, an extensive and deep research on its security and effectiveness has been carried out.

Manuscript submitted September 6, 2016. The work was supported by Research, Application and Demonstration of Key Technologies in National Sharing services of Public Digital Culture under Grant 2015BAK25B03.

Run Zhang, Yong-Bin Wang, Jin-Yao Yan and Shuang Feng, are with the Communication University of China, No.1 Dingfuzhuang East Street, Chaoyang District, Beijing, 100024, P.R. China(e-mail: zrun@cuc.edu.cn).

Compared to RSA and Diffie-Hellman scheme, ECC with ECDLP has more advantages like higher security, faster calculating speed, less storage space, narrower transmission bandwidth, and deeper mathematical basis and theoretical research. So ECC has become the most powerful public-key mechanism algorithm for its superior security and wider application environment. Meanwhile, ECC also has its disadvantages and may be attacked by the well-known Pollard Rho algorithm [1]. [4] proposed a new method for image tamper detection in the spatial domain. It used authentication encrypted with pseudo random sequence generated by Jacobian elliptic map and then the authentication was embedded in the image.

The problem with [2] is that it didn't use cryptography and authentication technology. Three verification tests were applied in [3].Firstly, ownership authentication with similarity between the extracted watermark and the original watermark. Secondly, integrity verification was employed by comparing the Hash value watermark and the Hash value of the received image's ROI. Finally, tamper location was computed by comparing the CRC-16 value with the extracted CRC-16 value of the same block. But no professional and specific cryptography and digital signature technology are seen. [4] completed a new authentication method based on Jacobian elliptic map with 160 bits key, which was lower robustness and small capacity and easily leaded to reducing the security of watermarking.

To solve the above problem better, our paper proposes more secure algorithms based on MECDH and AECDSA to enforce its security and improve the security of watermarking with the newly proposed algorithms.

The rest of the paper is organized as follows: Section II introduces public-key mechanism with new algorithm based on MECDH and AECDSA. Section III mainly describes the proposed highly secure image watermarking and digital signature with newly proposed scheme. Experimental results and performance analyses are shown in section IV. Finally, we draw some conclusions and discuss the future work.

II. PUBLIC-KEY CRYPTOGRAPHY SCHEME WITH NEW ALGORITHMS BASED ON MECDH AND AECDSA

ECC has been proved to be a more efficient and powerful public-key cryptography scheme, which is based on ECDLP [5]. No algorithm has been found so far with the sub exponential of

complexity [6]. However, with the deep and new application of ECC, some security problems such as ECDH key exchange protocol and Pollard Rho attack have been revealed gradually. Therefore, we put forward some more secure cryptography and signature algorithm based on MECDH and AECDSA implemented with MIRACL.

A. The Selection of More Secure Elliptic Curves

The security of ECC is on the basis of elliptic curve over finite fields. The elliptic curve with proper parameters is believed to be secure. The more difficult solution to ECDLP is, the more secure the elliptic curve is. The system parameters of secure elliptic curve are open in practice and the security of algorithm has nothing to do with the confidentiality of the parameters. So we'd better follow some essential rules so as to select more secure elliptic curves recommended by the National Institute of Standards and Technology (NIST)[7]. Because the ECC system in our paper studied at software level, the finite field is defined as a prime finite field, $GF(p)$ or F_p.

Let us explain how to choose system parameters for a secure elliptic curve by illustrating the $E(GF(p))$ formed by the points on an elliptic curve defined over a prime finite field.

1) The system parameters of the $E(GF(p))$ expressed as $y^2=x^3+ax+b(mod\ \ n)$ is commonly described as $D=(p,a,b,G,n,h)$, where $a,b \in GF(p)$, p from $GF(p)$ is a prime number, G is the base point of the curve and the prime n is the order of the point, h is a cofactor meeting the condition of $N=nh$, N is the order of the curve, $\#E(GF(p))$ determined by p, a and b. For being securer, all the parameters in an ECC application are open and required to satisfy the following conditions: The prime $p>3$.
2) $a<p$, $b<p$, $ab\neq 0$, $\triangle=4a^3+27b^2\neq 0$, $(4a^3+27b^2) \bmod p\neq 0$.
3) $n=\max(2^{191}, 4p^{1/2})$.
4) $h=[\#E(GF(p))]/n$, $1\leq h\leq 4$.
5) $\gcd[p,p+1-\#E(F_p)]=1$ (Non-supersingular).
6) $p+1-2p^{1/2} \leq \#E(F_p) \leq p+1+2p^{1/2}$ [9].
7) $\#E(F_p)\neq p$ (Non-anomalous).

Among all the above parameters, n is the most important, for cryptographically random number and private-key are both taken values from (1, n-1). Thus the length of the ciphers in ECC is normally defined as the binary length of n, which is recommended to be no less than 163 bits [10]. In this paper, for higher security and more receivable response, we choose 192 bits ciphers.

B. MIRACL

MIRACL is a big number library developed by Shamus Software Ltd., and is also the predecessor of the company with the same name as the library. The library not only implements all kinds of the primitives necessary to precisely arithmetical operations of big integer and fraction but also provides relevant algorithms of cryptography based on big number. With all its advantages, MIRACL is widely used in cryptography applications based on ECC. Furthermore, MIRACL runs at fast speed, because of some assembly code in its core.

Therefore, we make full use of the professional big number library to improve the security and the efficiency of highly secure watermarking and authentication resolution proposed in the paper.

C. MECDH (*Modified Elliptic Curve Diffie-Hellman*)

The ECDH (Elliptic Curve Diffie-Hellman) widely used in Cryptosystems is the key exchange protocol based on ECC and Diffie-Hellman algorithm, but it is vulnerable to Pollard Rho attack. For the purposes of more security, this paper has modified the ECDH and generated the MECDH (Modified ECDH) key exchange algorithm.

The scheme has been implemented in the following manner, which involves the uses of a more secure elliptic curve defined as $E(GF(p))$ with the parameters just like the form of $D=(p,a,b,G,n,h)$ and MIRACL above. The MECDH between two parties, A and B, has been accomplished as follows.

1) Initialization phase
   a) Initializing the MIRACL system for our application with the numbers of digits and the number base, here for 192 and 16 respectively.
   b) Initializing the system parameters, $D=(p,a,b,G,n,h)$, with $GF(\|p\|=192)$ based on secure elliptic curves recommended by NIST.
2) A randomly selects a big integer base on MIRACL, $d_A \in (1, n-1)$, as its private key. Then A computes the corresponding public key, $P_A=d_A\times(G \bmod n)$, which is a point on $E(GF(p))$. Finally A sends its public key, P_A, to B.
3) In the similar way, B randomly selects a big integer, $d_B \in (1,n-1)$, as its private key. Then B computes the corresponding public key, $P_B=d_B\times(G \bmod n)$, which is also a point on $E(GF(p))$. Finally B sends its public key, P_B, to A.
4) A generates the secret key, $K_1=d_A\times P_B \bmod n$. So does B, $K_2=d_B\times P_A \bmod n$, Thus $K=d_A\times d_B\times(G \bmod n)=K_1=K_2$.
5) A randomly selects a big integer as above, $d\in(1, n-1)$, computes $K^*=d\times K$ and sends it to B. So K^* acts as the session secret key.

Compared to the original ECDH key exchange algorithm, the MECDH above makes an attacker fail to get enough information to execute the Pollard Rho attack, and guarantees the new key exchange protocol to perform on unsecure channel.

D. Cryptography with MECDH

With MECDH key exchange protocol mentioned above, we can encrypt plaintext M to ciphertext. For simplicity, let's continue with step C.

1) B randomly selects a big integer as above, $e\in(1, n-1)$, and computes $C_1=e\times K$, $C_2=M+e\times K^*$, here M for plaintext, sends (C_1,C_2) to A.
2) A receives (C_1, C_2) and computes $M=C_2-e\times K^*=C_2-e\times(dK)=C_2-d\times(eK)=C_2-dC_1$.

Based on the MECDH key exchange protocol, the encryption and decryption processing above have improved the security of the original EC EIGamal[11] scheme, with which the Pollard Rho attack could be employed to reveal the private key, leading to potential safety loophole any further.

E. AECDSA (*Advanced Elliptic Curve Digital Signature Algorithm*)

AECDSA with 512 bits signature, implemented on ECC over E(GF(p)) with D=(p,a,b,G,n,h) above and on MIRACL, is the revised edition of the current ECDSA, but more secure with stronger elliptic curves and more efficient with the MIRACL library.

Let's suppose message m to be signed to (m,r,s,t), which is regarded as digital signature to be authenticated.

1) Initialization phase with MECDH above.

2) Signature stage
   a) Randomly choose a big integer $d\in(1, n-1)$, which meets the condition of $\gcd(d, n)=1$, as private key, then compute public key, $Q=d\times G$, and makes it public.
   b) Compute $e=SHA\text{-}512(m)$ and $w=H(e)$, where SHA-512 is a more secure hash function for 512 bits digest and e is the message digest in the form of MIRACL, w for Hamming weight of e and H for Hamming function.
   c) Select a big, random integer, $k\in(1, n-1)$, which meets the condition of $\gcd(d, n)=1$, then compute $kG=(x_1, y_1)$, $r=x_1 \bmod n$, $s=(wr+d-k) \bmod n$. If $r=0$ or $s=0$ then repeat this step.
   d) Select a big, random integer, $\lambda\in(1, n-1)$, which meets the condition of $\gcd(\lambda, n)=1$, then compute $t=\lambda\times m$, if $t=0$ then repeat the step.
   e) Generate the signature (m,r,s,t).

3) Authentication stage
   a) Judge the validity of the signature, (m,r,s,t). If $(r, s)\notin(1, n-1)$ then show that the signature is false.
   b) Compute $e=SHA\text{-}512(m)$ and Hamming weight of e, w, then repeat in the same way above.
   c) Compute $X=(s\text{-}wr\text{-}\lambda m+u)G+Q=kG=(x_2,y_2)$. If $X=O$ then the signature is false else $v=x_2 \bmod n$.
   d) If $v=r$ then the signature is validity else invalidity.

The AECDSA algorithm can not only resist kinds of attacks at the ECDSA scheme by forged signature like replacing message or random number, but also reduce the operating quantity.

III. SECURE WATERMARKING ALGORITHM WITH NEW ALGORITHM BASED ON MECDH AND AECDSA

Human Vision System (HVS) is playing an important role in image watermarking scheme. We use the HVS combined with newly proposed algorithms based on ECC and MIRACL to achieve our goal of ideal secure performance of the watermarking algorithm with better balance of invisibility and robustness.

A. Images Preprocessing

1) DSWT

The major weakness of the classical DWT is that it can't provide shift invariance on account of down-sampling of its sub-bands, which means DWT is not a time-invariant and leads to inaccurate extraction of the watermark embedded into a carrier image, possibly results in a poor extracted watermark.

In order to solve the problem, we introduce the DSWT algorithm to this paper. DSWT is designed to aim at overcoming the lack of shift invariance of DWT by removing down-sampling and up-sampling of coefficients during each filter-bank iteration and up-sampling the filter coefficients by a factor of 2^j in the j+1 level of the algorithm [12]. Since frame expansion increases robustness with respect to additive noise, images processing based on DSWT is more robust than that based on DWT [13].

In this paper, a selected carrier image and a selected watermark image with DSWT is implemented by *swt*2 function running on MATLAB R2012b, performing *swt*2 decomposition of the carrier image I at level 2 for higher PSNR and the watermark image W at level 1, generating $LL2$ for approximation coefficients of the carrier image and LL for approximation coefficients of the watermark image respectively.

2) SVD

SVD is used to extract algebraic features from images. Both DSTW and SVD do benefit to HVS in the proposed watermarking algorithm.

Let us suppose that A is a given gray-scale image represented in the form of $m\times n$ matrix with the data type of *single* in MATLAB environment, the result of SVD transformation is described as follows:

$$A=U\times\Sigma\times V^T \tag{1}$$

Here U is an $m\times m$ *single* unitary matrix, Σ is an $m\times n$ rectangular diagonal matrix with non-negative *single* values on the diagonal, and V^T is an $n\times n$ *single* unitary matrix. The diagonal entries $\Sigma_{i,i}$ of Σ are known as the singular values of A.

SVD transformation efficiently reveals intrinsic algebraic properties of an image, where singular values relate to brightness of an image and singular vectors reflect geometry characteristics of an image [14]. Because singular values concentrate the main energy of an image and singular vectors have good stability and rotation invariance, both of them are useful for invisibility and robustness of the proposed watermarking scheme.

In our paper, the image A in equation (1) is replaced by LL2 and LL subband respectively, both of the subband are transformed according to SVD operation mentioned above.

B. Embed Watermark and Generate Digital Signature

The newly proposed secure watermarking embedding algorithm based on MECDH and AECDSA is implemented with DSWT and SVD in MATLAB environment. The algorithm illustration is shown in Fig. 1.

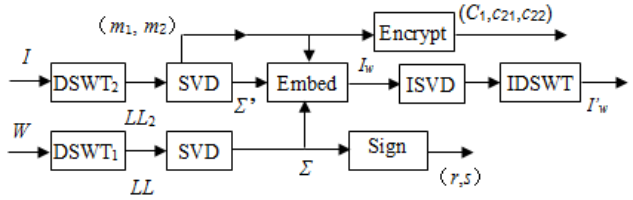

Fig. 1 Watermark Embedding Algorithm

The steps of watermark embedding and digital signature generating algorithm are described as follows:

1) Apply DSWT at level 2 to the carrier image to decompose it into LL_2, HL_2, LH_2, HH_2 sub-bands, and apply SVD transformation to LL_2 to generate its diagonal matrix Σ'.
2) Apply DSWT at level 1 to the watermark image to decompose it into LL, HL, LH, HH sub-bands, and apply SVD transformation to LL to generate its diagonal matrix Σ.
3) Modify the singular values of the carrier image with the singular values of watermark image based on the following expression:

$$I_w=\Sigma'+\sigma\Sigma \quad (2)$$

Where I_w stands for the watermarked image, σ for embedding intensity coefficient.

4) Encrypt position parameters with MECDH algorithm based on MIRACL.

$(m_1\|m_2)$ are encrypted to 192-bit (C_1, C_2) in the form of hexadecimal, where m_1 stands for the starting position and m_2 for number of embedding coefficients.

5) Generate 512-bit digital signature (m,r,s,t) based on the AECDSA.
6) Apply inverse SVD and DSWT to the transformed carrier image to reconstruct the watermark-embedded image.

C. Extract Watermark and Authenticate Digital Signature with MECDH and AECDSA

The proposed secure watermark extracting algorithm based on MECDH and AECDSA is implemented with DSWT and SVD in MATLAB environment. The algorithm illustration is shown in Fig. 2. The meanings of the parameters are listed above. As an exception, W'' stands for the extracted watermark image and W' for reconstructed watermark image based on W''.

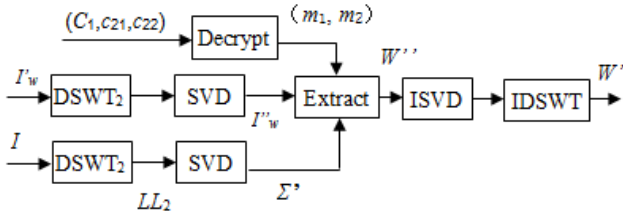

Fig. 2 Watermark Extracting Algorithm

The steps of watermark extracting and authenticating digital signature algorithm based on AECDSA are an inverse process B simply described as follows:

1) Apply $DSWT_2$ and SVD transformation to I'_w to generate I''_w.
2) Apply $DSWT_2$ and SVD transformation to I to generate Σ'.
3) Decrypt encrypted position parameters (C_1, C_2) to (m_1, m_2) based on the corresponding algorithm above.
4) Extract the singular values from the watermarked image according to the following formula:

$$W''=(I''_w - \Sigma') \quad (3)$$

5) Apply inverse SVD and DSWT to W'' to obtain the extracted watermark image, W'.
6) Authenticate the digital signature shown in Fig. 3.

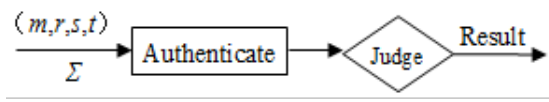

Fig. 3 Digital Signature Authenticate

IV. EXPERIMENTAL RESULTS AND PERFORMANCE ANALYSIS

This paper has proposed a more secure image watermarking algorithm based on MECDH and AECDSA, the algorithm has been implemented in MATLAB R2012b with DSWT and SVD, calling *DLL* (Dynamic Linked Library) generated in Microsoft Visual Studio 2010 with MIRACL. The main results of our applications to the new algorithm are illustrated as follows:

Fig. 4 (a) Original Image (b) Watermarked Image（σ=0.1, PSNR=45.17）

Fig. 5 (a) Original Image (b) Watermarked Image（σ=0.01, PSNR=64.80）

On the basis of the subjective evaluation, the original and watermarked images are shown in Fig. 4. Let us pay more attention to the objective evaluation criterion, PSNR, an approximation to human perception of reconstruction quality. A higher PSNR value normally means higher quality of reconstruction. The typical PSNR value for distorted images and videos are between 30 and 50 dB. Provided the bit depth is 8 bit, normally, the higher value of PSNR and the better performance for the algorithm.

Together with the subjective evaluation shown as Fig. 4&5, and PSNR values is 64.80 to 45.17 dB with $\sigma\in(0.01,0.1)$, by which the invisibility of the final image embedded with the watermark image is effective, and the similarity of the original carrier image and the watermarked image is high. So the result of the proposed algorithm is more robust, more secure and better than that of [4] with 44.12 dB, [2] didn't mentioned it, but lower than the PSNR in [3] without professional and specific cryptography and digital signature technology.

In this paper, with the subjective evaluation shown as Fig. 6&7, the correlation coefficient between the original watermark image and the extracted one is 0.9974 to 0.9917, which means the close correlation between them. [2~4] didn't mention the corresponding data.

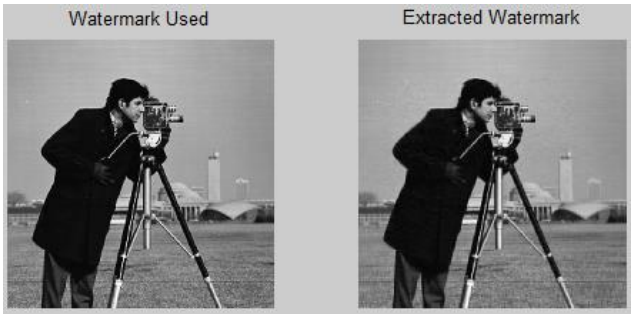

Fig. 5 (a) Original Watermark (b) Extracted Watermark（σ=0.1, correlation coefficient=0.9974）

Fig. 6 (a) Original Watermark (b) Extracted Watermark（σ=0.01, correlation coefficient=0.9917）

To verify the robustness of the newly-proposed algorithm, we only test median-filtering attack and 45°-rotation attack against the algorithm due to space limitations as Fig. 7. ~ 10. . The results of the algorithm have turned out to be robust despite some kinds of attacks.

Fig. 7 Median-filtering Attack（σ=0.1, correlation coefficient=0.9748）
(a) Original Watermark (b) Extracted Watermark

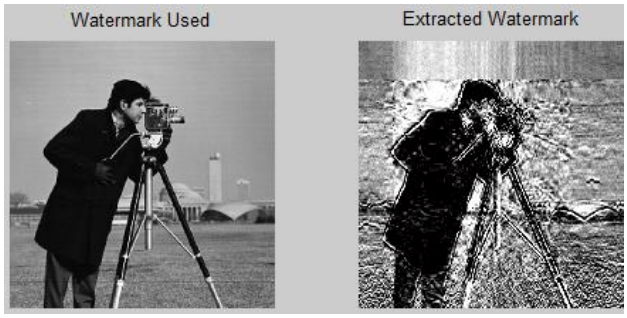

Fig. 8 Median-filtering Attack（σ=0.01, correlation coefficient=0.6134）
(a) Original Watermark (b) Extracted Watermark

Fig. 9 45°-Rotation Attack（σ=0. 1, correlation coefficient=0.3724）
(a) Original Watermark (b) Extracted Watermark

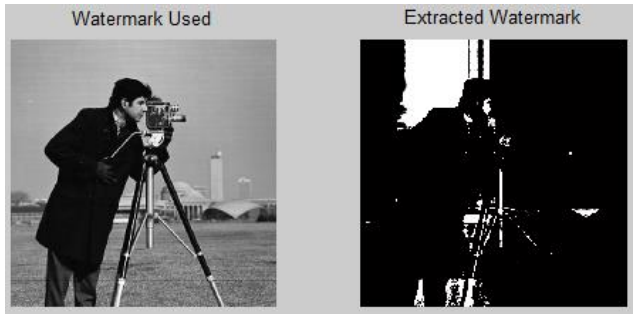

Fig. 10 45°-Rotation Attack（σ=0.01, correlation coefficient=0.3069）
(a) Original Watermark (b) Extracted Watermark

V. CONCLUSION

This paper presents a highly secure watermarking and digital signature authentication scheme with the improved MECDH and AECDSA algorithm running on MIRACL, which is implemented with DSWT and SVD. Both theoretical analyses and experimental results show that the proposed watermarking scheme with digital signature is more secure and efficient, authentic to protect digital copyrights, and is conforming to HVS with good invisibility and robustness. In next step we wish to implement quantitative analyses in the watermarking algorithm performances against all kinds of attacks, and to compute some elliptic curve with better performance over F_p.

REFERENCES

[1] D. Hankerson, A. Menezes, S. Vanstone, "APPENDIX B ECC Standards,", "Cryptographic Protocols," in *Guide to Elliptic Curve Cryptography*, New York: Springer, 2004, pp. 267–270. , pp. 153–204.
[2] Shalu Singh, Ranjan Kumar Arya, Harish Sharma, "Region based undetectable multiple image watermarking," in *ICCTICT*, 2016, pp. 141 -144.
[3] Ali Al-Haj, Noor Hussein, Gheith Abandah, "Combining cryptography and digital watermarking for secured transmission of medical images, " in *ICIM*, 2016, pp. 40-46.
[4] Milad Jafari Barani, Milad Yousefi Valandar, Peyman Ayubi, "A secure watermark embedding approach based on chaotic map for image tamper detection, " in *IKT*, 2015, pp. 1-5.
[5] Marco Indaco, Fabio Lauri, Andrea Miele, Pascal Trotta. "An Efficient Many-Core Architecture for Elliptic Curve Cryptography Security Assessment," in *FPL*, 2015, pp. 1-6.
[6] Songyuan Yan, "Public-Key Cryptography," in *Elliptic Curve*, CN:Dalian University of Technology Press, 2011, pp. 103-117.
[7] National Institute of Standards and Technology, Digital Signature Standard, FIPS Publication 186-2, February 2000.
[8] Ali Makki Sagheer, "Elliptic Curves Cryptographic Techniques," in *ICSPCS*, 2012, pp. 1-7.

[9] Joseph H. Silverman, "Elliptic Curves over Finite Fields," in *The Arithmetic of EllipticCurves*[M], New York:Springer-Verlag, 1986, pp. 130-145.
[10] Yong Ding, "Introduction to Elliptic Curve Cryptograpy," in *Fast Algorithm Theory of Elliptic Curve Crytography*, CN:Post & Telecom Press, 2012, pp. 1-14.
[11] Tafta Zani, Ari Moesriami Barmawi, "Securing Elliptic Curve based El-Gamal against Pollard Rho attack using Elliptic Curve based Diffie-Hellman Key Exchange, " in *ITST*, 2012, pp. 505-512.
[12] M.V. Tazebay and A.N. Akansu, "Adaptive Subband Transforms in Time-Frequency Excisers for DSSS Communications Systems, " *IEEE Transaction on Signal Processing*, vol 43, no. 11, pp. 2776-2782, Nov. 1995.
[13] Samira Lagzian, Mohsen Soryani, Mahmood Fathy. (2011, Mar.). "A New Robust Watermarking Scheme Based on RDWT-SVD: Embedding data in all subbands," International Journal of Intelligent Information Processing, 2 (1), pp. 48-52.
[14] Paul Bao, Xiaohu Ma. (2005). "Image Adaptive Watermarking Using Wavelet Domain Singular Value Decomposition," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 15, no. 1, pp. 96-102.

Run Zhang is an associate professor of Computer Science at Communication University of China and a member of ACM. His research interests include Information Safety, Machine vision and Machine learning, etc. He has joined several National High Technology Research and Development Programs of China (863 Program) and published several theoretical technological articles.

Yong-Bin Wang is a professor of Computer Science and director of Science and Technology Office at Communication University of China. He is the director of Academic Committee at Key Laboratory of Vision-Audition Technology and Intelligent System, Ministry of Culture and Beijing Laboratory of Modern Performing Arts Technology. He is also a member of Beijing Committee of the Chinese People's Political Consultative Conference. His research expertise is in the areas of media big data, social computing, and network new media. He gained 3rd class of S&T Achievements Granted with National Technology Invention Awards and 2nd class of Beijing Science and Technology Award. He has managed a variety research projects from Ministry of Science and Technology, Beijing Municipal Science & Technology commission. Prof. Yongbin Wang is the author of over 100 technical papers.

Jin-YaoYan received the B.S. degree from Tianjin University, the M.S. and Doctor (in engineering) degrees from Beijing Broadcasting Institute, the Ph.D (in science) degree from Swiss Federal Institute of Technology (ETH Zurich). Since 2010, he has been a Professor at Communication University of China, Beijing, P.R.China. He is a guest professor in communication system group at ETH Zurich. His research interests are in the areas of future network, multimedia communication, and cloud computing.

Shuang Feng is an associate professor of Computer Science at Communication University of China. Her research interests include Intelligence media processing, recommender systems and information retrieval. She joined the Department of Computer Science at the University of California, Santa Barbara as a visiting scholar in August 2013. She received her BSc and MSc from China Agriculture University, and her PhD from Communication University of China in 2013. She is a member of ACM. She managed more than 10 research projects from Ministry of Science and Technology, National High Technology Research and Development Program of China (863 Program), Beijing Municipal Science &Technology commission and obtained 2 national invention patents.

Privacy Preserving Data Aggregation over Multi-hop Networks

Szilvia Lestyán

***Abstract*—We present a novel privacy-preserving data aggregation protocol in wireless networks composed of short-range devices. These devices provide a collaborative service and conduct privacy-preserving computations to obtain the aggregated result of their secret inputs. Our solution uses secure multi-party primitives as well as a new distributed perturbation technique to guarantee strong differential privacy against untrustworthy aggregators.**

***Keywords*—Privacy Preserving Data Mining, Secure Multiparty Computation, Differential Privacy**

I. INTRODUCTION

Although Internet is the prevalent communication network today connecting billions of different devices worldwide, there are still several practical cases where Internet connectivity is scarce and expensive, such as surveillance and monitoring of rural areas. In such applications, multi-hop wireless networks using short-range communications still provide a cheaper and compelling alternative to a global networking infrastructure. For example, wireless sensor networks are deployed for the purpose of monitoring agricultural areas in order to facilitate more responsive intervention and to optimise maintenance tasks with the aim to increase productivity [1]. However, different producers can compete with each other, and hence security, and in particular, confidentiality is of primary concern.

As a motivational scenario, consider vineyards[1] where sensors measure different regional characteristics such as the pH of the soil or its mineral composition. Across a large territory, there are several wineries, where winemakers use different types of fertilisers for their field. The composition of fertilisers is considered as trade secret among winemakers, thus revealing some characteristics of the soil can also reveal this confidential information. Moreover, for geological surveys as well as various consultancy services, different organizations periodically collect statistics about a larger territory over multiple vineyards, belonging to different producers, e.g., in order to measure soil contamination. Such monitoring service can also be beneficial for the producers as they may lack of expertise to deeply analyze the quality of the soil. Importantly, these organizations are only interested in aggregate measurements over multiple vineyards, and less concerned with sensor readings of a single producer. To this end, organizations can use mobile base stations, which move along the perimeter of multiple vineyards without approaching the fields [2]. These base stations initiate the aggregation protocol through the sensor nodes they can reach via short-range communication. That is, a base station builds an aggregation tree having the base station as root and simply fan-in[2] the values from leaves to the root (see Figure 1).

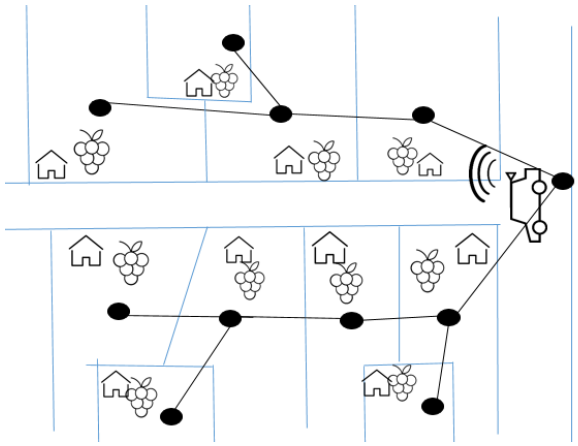

Fig. 1: Aggregation on vineyards. A mobile base station stops at the perimeter of the area and builds an aggregation tree, where the base station is the aggregator (root) node.

However, producers do not trust each other or the organization providing the monitoring service. In particular, they do not want neither another producer nor the organization to learn any of their sensor readings. The above simple aggregation protocol does not provide such privacy guarantees. In fact, this protocol cannot guarantee privacy even in the presence of semi-honest participants who follow the aggregation protocol faithfully but may learn any private sensor reading from the received messages. For example, a parent of a node in the aggregation tree, where both nodes belong to different producers, can immediately learn the measurement of its children, or an eavesdropper can capture a sensor's incoming and outgoing aggregates and easily calculate the measurement of the sensor.

In this paper, we propose a privacy-preserving aggregation protocol for the above scenario. In particular, our protocol guarantees that (1) sensor nodes cannot learn each other's readings, (2) a passive eavesdropper cannot infer any measurement

Manuscript submitted on December 3, 2016.

Szilvia Lestyan is with CrySyS Lab, Dept. of Networked Systems and Services, Budapest Univ. of Technology and Economics; email: lestyan@crysys.hu

[1] http://smartvineyard.com

[2] Fan-in is the algorithm where the values are sent from leaves to the root and gradually aggregated at each inner node, therefore the total sum appears at the root at the end of the algorithm.

in the network, (3) the aggregator node, who is untrusted, cannot learn any individual sensor reading in the network. For this purpose, sensor nodes employ secure multiparty computation as well as add noise to their readings in order to provide strong differential privacy guarantees against the aggregator. The variance of the noise is calibrated so that the aggregator can still learn the aggregate but any of its constituent measurement. We propose a novel distributed noise generation algorithm based on the geometric divisibility of the Laplace distribution, which provides increased robustness as well as flexibility over state-of-the-art solutions.

Our contributions are summarised as follows.

- We propose a novel mechanism to compute the sum of measurements (e.g. pH value of the soil, temperature, etc.) of multiple nodes in a privacy preserving and distributed manner assuming semi-honest adversaries. Our solution relies on secure multi-party primitives combined with homomorphic encryption. In addition, we noise the aggregate to prevent the untrusted aggregator from learning individual sensor readings in the network and hence providing formal privacy guarantees.
- We introduce a novel technique for privacy preserving distributed noise generation. We use the geometric infinite divisibility property of the Laplace distribution to preserve ϵ-differential privacy. This new noise generation method provides increased robustness and flexibility on distributed systems over earlier solutions.

II. Related Work

Our view of privacy preserving and computational model derived from a multi-party approach. For a survey of privacy preserving data mining see e.g. [3] and [4], and on general multi-party computation see [5] or [6] The basic idea of Secure Multiparty Computation (SMPC) is that a computation is secure if at the end of the computation, no party knows anything except its own input and the results (*privacy*). Secure two party computation was first investigated by Yao [7], and was later generalised to multiparty computation [5], [8]. These works all use a similar methodology: the function f to be computed is first represented as a combinatorial circuit, and then the parties run a short protocol for every gate in the circuit.

The aim of secure multiparty computation is to enable parties to carry out such distributed computing tasks in a secure manner. Whereas distributed computing [9] [10] classically deals with questions of computing under the threat of machine crashes and other inadvertent faults, secure multiparty computation is concerned with the possibility of deliberately malicious behavior by some adversarial entity.

On the combination of SMPC and graph algorithms, see a weighted case [11], where a protocol with which a set of n stores, selling l products between them, participate in joint computation to securely determine c_{jk}, the number of times product j and product k have sold together in all stores combined (without revealing any information about the products that any one store, individually, sells).

Others have only considered some route-planning in a similar setting: for privacy-preserving computation of APSD (all pairs shortest distance) and SSSD (single source shortest distance) see [12]; and in [13] a private computation for collision-avoiding route planning is introduced.

A comparative study has been fairly recently written on the problem of secure data aggregation in a distributed setting while preserving differential privacy for the aggregated data [14]. In their paper, they show the infinite divisibility of the Laplace distribution, and generate partial noises by drawing random variables from the *gamma*, the *Gauss* and one *Laplace* distributions.

In order to read on the application of the Laplace distribution based on the gamma distribution see [15]; where a privacy-preserving smart metering scheme that guarantees users' privacy while still preserving the benefits and promises of smart metering is proposed.

III. Applied Model

A. Network Model

Let $P_1, P_2, ..., P_N$ be parties (i.e., producer) owning private measurements $x_1, x_2, ..., x_N \in \mathbb{R}$. The parties wish to apply a function to the joint set $\bigcup x_i$ without revealing any unnecessary information about their individual values. That is, the only information learned by P_i about x_{-i} (where x_{-i} is any other measurement except x_i) is that which can be learned from the output of the algorithm, and vice-versa. We *do not assume any trusted third party* who computes the joint output on the raw data.

We also assume that a unique label is given to each party (or nodes). We do not assume a peer-to-peer system to be available, e.g. it is not necessary for all the parties to be directly connected. A channel between two parties is bidirectional and *first in first out* (FIFO), i.e. the messages received in the order in which they have been sent. Each party is represented by a single sensor node in the network. In case a producer deploys multiple sensors over his vineyard in our motivational scenario (see Section I), a single sensor is selected per vineyard which collects all measurements over the vineyard and can be reached by either the base station or by a sensor of a neighboring vineyard. Therefore, the topology of the parties can be represented with an *arbitrary strongly connected graph*.

We could also view the model as a multi-hop ad-hoc network, where nodes cooperate to form a network without using any infrastructure such as access points or base stations. Instead, nodes forward packets to each other, allowing communication among nodes outside wireless transmission range. For a survey on attacks on multi-hop ad-hoc networks see [16].

The channels between any two parties can be *secure* or *insecure* as well. A secure channel is a way of transferring data that is resistant to overhearing and tampering. In case of an insecure channel an eavesdropper can overhear any message (ciphertext) from any existing channel and try to decipher it.

Each party P_i has a set of neighbors, denoted N_i, this set contains the identities (labels) of these parties. This is the only knowledge a node (participant) can have of the global graph, e.g. it cannot "see" any other nodes besides its direct neighbours, it does not even know the total number of participants (only if it is the result of a particular protocol).

This model is *partially synchronous* (timing-based), i.e. we assume some restrictions on the relative timing of events, but execution is not completely lock-step as it is in the synchronous model. These models are the most realistic, but they are also the most difficult to program. Algorithms designed using knowledge of the timing of event can be efficient, but they can also be fragile in that they will not run correctly if the timing assumptions are violated.

B. Adversary Model

The adversary is assumed to be *semi-honest* and *static*, malicious adversaries are also partly considered [17], [18]. Therefore, semi-honest parties faithfully follow the protocol specification, yet attempt to learn additional information by analyzing the messages received during the protocol execution. Although the semi-honest adversarial model is weaker than the malicious model (where a party may arbitrarily deviate from the specification, it is often a realistic one. This is because deviating from a specified protocol which may be buried in a complex application is a non-trivial task. Moreover, producers do not collude with the potentially malicious aggregator.

C. Privacy and Security Model

It is assumed that a protocol execution can be attacked by an external entity, or even by a subset of the participating parties. The aim of this attack may be to learn private measurement or cause the result of the computation to be incorrect. In order to avoid this, every node can send its output to the trusted party, who performs the computation. But this is unlikely to happen in our scenario, thus we use and design algorithms where the same result can be achieved without using a trusted party. Different definitions of security for multiparty computation have been proposed, in this paper we are going to use the following [18]:

- *Privacy:* No party should learn anything more than its prescribed output. In particular, the only information that should be learned about other parties' inputs is what can be derived from the output itself. For example, in an auction where the only bid revealed is that of the highest bidder, it is clearly possible to derive that all other bids were lower than the winning bid. However, this should be the only information revealed about the losing bids.
- *Correctness:* Each party is guaranteed that the output that it receives is correct.
- *Independence of inputs:* Corrupted parties must choose their inputs independently of the honest parties' inputs.
- *Guaranteed output delivery:* Corrupted parties should not be able to prevent honest parties from receiving their output. For example, the adversary should not be able to disrupt the computation by carrying out a *denial of service* attack.
- *Fairness:* Corrupted parties should receive their outputs if and only if the honest parties also receive their outputs.

D. Differential Privacy

The above guarantees still allow the untrusted aggregator to learn individual sensor readings from the aggregate. Indeed, knowing a few measurements in the network (e.g., the aggregator may deploy extra sensors in the observed area to replicate the measurements) may help the aggregator to obtain a more accurate approximation of the remaining measurements.

Differential privacy ensures that the removal or addition of a single measurement from the network does not (substantially) affect the outcome of any analysis performed on the set of all measurements (such as the output of an aggregate function). Roughly speaking, this means that even if the aggregator learns all constituent measurements of the aggregate except one, it will not be able to infer this unknown measurement if the aggregate itself is differential private.

Suppose two databases D_1 and D_2, which *differ in at most one record* (measurement), where one is a proper subset of the other and the larger database contains just one additional measurement [19].

Definition 1 (Differential Privacy)**.** *A randomised algorithm $\mathcal{A}$ gives ϵ-differential privacy if for all data sets D_1 and D_2 differing on at most one record, and all $S \subset Range(\mathcal{A})$,*

$$Pr[\mathcal{A}(D_1) \in S] \leq e^{\epsilon} \times Pr[\mathcal{A}(D_2) \in S]$$

The probability is taken is over the coin tosses of $\mathcal{A}$.

The above definition guarantees that if one participant's data is removed from the dataset no outputs (and thus consequences of outputs) would become significantly more or less likely (up to ϵ). That is, all possible values of the aggregate are almost equally likely with D_1 and D_2. If ϵ is small, we have stronger privacy guarantee as the output probabilities become closer.

To provide differential privacy, the output of f (i.e., the aggregate) needs to be randomised, for example, by adding noise to that where the noise variance is calibrated to the sensitivity of the aggregate.

Definition 2 (Global sensitivity)**.** *Global sensitivity S_f of $f : D \rightarrow \mathbb{R}$ is the maximum absolute valued difference between a function's maxima and minima on neighboring datasets:*

$$S(f) = \max_{D_1, D_2} |f(D_1) - f(D_2)|$$

where D_1 and D_2 differ in a single entry.

It has been shown that by perturbing the output of a function f, we are able to reach ϵ-differential privacy [19]. The perturbation shall be a random noise added to the value of f, furthermore the distribution of the noise is dependent on the global sensitivity of f.

Theorem 1 (Laplace Mechanism)**.** *For all $f : D \rightarrow \mathbb{R}$, the following algorithm $\mathcal{A}$ is ϵ-differential private:*

$$\mathcal{A}(D) = f(D) + \mathcal{L}(S(f)/\epsilon)$$

where $\mathcal{L}(\lambda)$ is an independently generated random variable following the Laplace distribution with probability density function $g(x) = \frac{1}{2\lambda} e^{-\frac{|x|}{\lambda}}$ and $S(f)$ denotes the global sensitivity of f.

In our case, f represents the aggregate function which is the sum of sensor measurements, and its sensitivity is the maximum of any measurement that a sensor can take. If this value is too large, then every measurement can be truncated to a pre-defined threshold t by each sensor node, hence ensuring that the global sensitivity is at most t in the whole network. Therefore, to guarantee ϵ-differential privacy, we need to add a random value to the aggregate which is sampled form a Laplace distribution with zero mean and variance $2S(f)^2/\epsilon^2$.

Intuitively, if a single measurement can substantially change the output of f, then larger noise needed to be introduced to "hide" the contribution of a single record (sensor) to the aggregate. However, larger noise also deteriorates utility as the final aggregate will be inaccurate. This is a fundamental trade-off between utility and privacy: larger/smaller noise yields stronger/weaker privacy and smaller/larger utility. There seems to be no free lunch. On the other hand, the relative error of the aggregate (or "signal-to-noise ratio") can also be decreased without degrading privacy by aggregating more sensor readings. This is because the aggregate (sum) becomes larger while the added Laplace noise is still calibrated to the global sensitivity which remains unchanged by adding more readings to the aggregate.

IV. BUILDING BLOCKS

In this section, we introduce some basic building blocks that are used in our solution.

A. Privacy Preserving Primitive: Secure Sum

In SMPC, each participant holds onto a number of their own, and they would like to compute the sum of their inputs. The aggregator – one of the parties – generates a random number R, adds R to its local value and sends the result to the next party. All participants add their local value to the received number. Finally the aggregator receives the sum, subtracts R from the result and broadcasts the result. This guarantees that no one besides the aggregator will learn the correct sum of the values.

B. Homomorphic Encryption

A homomorphism is a structure-preserving map between two algebraic structures. Using homomorphic encryption, computations can be carried out on ciphertext, thus generating an encrypted result which, when decrypted, matches the result of operations performed on the plaintext. We use the Paillier cryptosystem [20] in this paper. In this scheme, if the public key is the modulus m and the base g, then the encryption of a message x is

$$Enc(x) = g^x r^m \mod m^2$$

for some random $r \in \{0, \ldots, m-1\}$. The homomorphic property is then

$$\begin{aligned} Enc(x_1) \cdot Enc(x_2) &= (g^{x_1} r_1^m)(g^{x_2} r_2^m) \bmod m^2 \\ &= g^{x_1+x_2}(r_1 r_2)^m \bmod m^2 \\ &= Enc(x_1 + x_2) \end{aligned}$$

C. Robust DFS

We build an aggregation tree using a distributed version of the depth-first search (DFS) algorithm. We need to create univoque routes between all nodes in order to avoid redundant packet channelling and to support aggregation. We must note that this problem is reminiscent of the secure routing problem in wireless or distributed networks, which has been widely studied in the literature [16]. Here, we only provide a basic solution which fits our goal. In particular, a DFS tree results in a definite order of the messages which property is indispensable for our solution to obtain the correct aggregates. The distributed version of the BFS algorithm can be found in [9] [10], the *Robust DFS* algorithm described below is analogous to the BFS one:

Building a Depth First Search Tree:

1) At any point during execution, there are some nodes that are "marked", initially just i_0, the root. The root sends a *search* message at the first round to one of its neighbours.
2) At any round, if an unmarked node receives a *search* message, it marks itself, sets and notifies its parent with a *child* message, and sends *non-child* message to those nodes from which it received a *search* message in earlier rounds.
3) After this, the node sends the *search* message to one of its neighbours.
4) This continues until a *search* message reaches a leaf node. A leaf node realises that it is indeed a leaf-node by receiving *non-child* messages from all of its children candidates (or have only one neighbour).
5) When a node declares itself as a leaf it sends an *end* message back to its parent who then chooses another neighbour of its own and waits for the next *end* message. When it received messages from all of its neighbours, the node sends the *end* it to its parent.
6) The algorithm ends when the root could also send the *end* message.

REMARK: In the non-secure version of the above protocol, a node also sends the list of its parent and children to neighboring nodes, therefore every other node in the graph may be able to reconstruct the tree (or the whole graph) using the received lists of parents and children.

Robustness: The network can lose some nodes due to power failure, hardware or software complications and many more that can cause the node to be detached from the network. Moreover, nodes can potentially be mobile, such as in wireless mobile ad-hoc or vehicular networks. To increase robustness against these failures and potential node mobility, we extend the above algorithm as follows. When a node detects that one (or) some of its neighbours are disconnected, it does the following:

1) if it is a child node, it does nothing;
2) if it is a parent, then
   a) if there is another node during the tree-building phase who was second to become its parent, i.e. sent the node

a *Search* message, then the node notifies them about the change and becomes its child;
b) if there is none like the above the node notifies one of its children to search for a new parent and they switch roles, i.e. the child becomes the parent and vice-versa;
c) if none of the above succeed, or the node has no other neighbours, then it becomes an isolated node (or tree).

Security in the presence of semi-honest adversaries:

- *Privacy:* Complies. No node learns anything about the global graph, they learn only their parent and children nodes, i.e. the local output.
- *Independence of inputs*: Complies trivially.
- *Output delivery:* Complies trivially.
- *Correctness:* Complies trivially.
- *Fairness:* Complies trivially.

Security in the presence of malicious adversaries: Consider the scenario when a node intentionally deviates from the protocol. The only thing it can do without being detected is to set several nodes as its parents, which violates the property of correctness because the malicious node becomes the child of some nodes of which it should not be thereby corrupting their output. In particular, circles may be created in the output graph, which is not a tree and hence an incorrect output of the protocol.

Complexity: The time complexity is at most $2 \cdot diam$ rounds, (where *diam* is the longest shortest path between any two nodes). The transmitted messages are composed of $3(e-1)$ *search* messages, where e denotes the number of edges, i.e., neighboring node pairs, one *child* or *non-child message* and one *end* message between each neighboring pair of nodes. Thus the time complexity is $\mathcal{O}(diam)$ and the communication complexity is $\mathcal{O}(e)$.

D. Distributed Noise Generation

To achieve differential privacy, Theorem 1 suggests that Laplace noise with scale $\lambda = S(f)/\epsilon$ needs to be added to the value of the aggregate function f. A natural question arises: *Which node should add this noise to the aggregate?* As the aggregator is untrusted, the sensor nodes themselves need to add the required amount of noise in a distributed manner. A naive solution would be that a single node is selected to inject all the Laplace noise. However, this approach requires the cooperation of nodes which can be expensive. Also, this makes the protocol less robust against privacy attacks as the selected single node may be malfunctioning (i.e., do not add the noise) or already left the network.

Instead, in our solution, each node *probabilistically and independently* decides whether it adds some noise share to this aggregate such that the sum of these added noise shares yields the required amount Laplace noise needed to guarantee differential privacy. For that, we rely on the following property of the Laplace distribution [21]:

Definition 3 (Geometric Infinite Divisibility)**.** *A random variable Y (and its probability distribution) is said to be **geometric infinitely divisible** if for any $p \in (0,1)$ it satisfies the relation:*

$$Y \overset{\mathrm{d}}{=} \sum_{i=1}^{\mu_p} Y_p^{(i)}$$

where μ_p is a geometric random variable with mean $1/p$, and the random variables $Y_p^{(i)}$ are independent and identically distributed for each p, and μ_p and $Y_p^{(i)}$ are independent.

The Laplace distribution exhibits the above geometric infinite divisibility, which is shown by the following theorem [21].

Theorem 2. *Let Y possess a Laplace distribution $\mathcal{L}(\lambda)$ with zero mean. Then, Y is geometric infinitely divisible and for any $p \in (0,1)$ the above holds with $Y_{\mu_p}^{(i)} \sim \mathcal{L}(\lambda\sqrt{p})$.*

V. SECURE AGGREGATION

Our solution combines the *Secure Sum* primitive (in Section IV-A) with homomorphic encryption (in Section IV-B) and distributed noise injection to preserve differential privacy (in Section IV-D). A DFS tree is assumed to be already built (as described in Section IV-C) before running our aggregation protocol.

A. Basic protocol

The operation of the aggregator and sensor nodes are shown in Algorithm 1 and 2, respectively.

Algorithm 1 Secure Aggregation: Aggregator node

1: Generate public-secret key pairs (pk_1, sk_1) and (pk_2, sk_2)
2: $p := 1/N$
3: $G := 0$
4: **for all** child $j \in [1, m]$ **do**
5: Send $\{G, p, pk_1, pk_2\}$ to a child j
6: Receive $\{G_j, c_{j1}, c_{j2}\}$ from child j
7: $G := \vee_{i=1}^{j} G_i$
8: $c_1 := \prod_{j=1}^{m} c_{j1} = Enc_{pk_1}\left(\sum_{i=1}^{N} r_i + \sum_{i=1}^{N} x_i + \sum_{i=1}^{N} Y_i\right)$
9: $c_2 := \prod_{j=1}^{m} c_{j1} = Enc_{pk_2}(\sum_{i=1}^{N} r_i)$
10: Decrypt (c_1, c_2) to retrieve the noisy aggregate R, where
11: $R = Dec_{sk_2}(c_2) - Dec_{sk_1}(c_1) = \sum_{i=1}^{N} x_i + \sum_{i=1}^{N} Y_i$
12: $\sum_{i=1}^{N} Y_j \sim \mathcal{L}(S/\varepsilon)$

We assume that the aggregator (root) node knows the size N of the network. First, the root generates two pairs of homomorphic asymmetric keys (pk_1, sk_1) and (pk_2, sk_2), then sets the noise parameter p (see Definition 2) to $1/N$ and sends the public keys along with p to its children. The children forward this message to their children and so forth, until the message reaches the a leaf node.

When a leaf receives the message of the aggregator from its parent, it tosses a biased coin which results in head with probability p (denoted by $G = 1$ in Alg. 2). If the result of the coin toss is 0, the node generates a Laplace noise with scale $S\sqrt{p}/\epsilon$, where S denotes the global sensitivity of the

Algorithm 2 Secure Aggregation: Non-aggregator (sensor) node

1: Receive $\{G,\ p,\ pk_1,\ pk_2\}$ from the parent
2: **for all** child $j \in [1, m]$ **do**
3: Send $\{G,\ p,\ pk_1,\ pk_2\}$ to a child j
4: Receive $\{G_j, c_{j1}, c_{j2}\}$ from child j
5: $G := \vee_{i=1}^{j} G_i$
6: **if** $G = 1$ **then**
7: $Y := 0$
8: **else**
9: $G \sim \mathcal{B}(p)$, where $\mathcal{B}$ is the Bernoulli distribution
10: **if** $G = 0$ **then**
11: $Y \sim \mathcal{L}(S\sqrt{p}/\epsilon)$
12: **else**
13: $Y := 0$
14: Generate r uniformly at random
15: Send (G, c_1, c_2) to the parent, where
16: $c_1 := Enc_{pk_1}(r + x + Y) \cdot \prod_{j=1}^{m} c_{j1}$
17: $c_2 := Enc_{pk_2}(r) \cdot \prod_{j=1}^{m} c_{j2}$

sum (see Theorem 1), which is the maximum value of any sensor measurement (or its truncation threshold). Afterwards, the node generates a random number r, which is added to the node measurement x and encrypted with key pk_1 to get c_1. In addition, r is also encrypted with the other key pk_2 to get c_2. The encrypted messages c_1 and c_2 along with the result G of the coin toss are sent back to the parent as a reply. Any intermediate node between a leaf and the aggregator repeats the same steps as the leaf node after receiving all reply messages from its children, except that it also checks if it receives $G = 1$ from any of its children, that is, any node in the corresponding subtree observed head by executing the coin toss. If so, it will not add Laplace noise to its own measurement before encryption. As a result, the sensor nodes fan-in the values along the edges of the built DFS tree. When the root receives all reply messages from its children it aggregates them likewise all other sensor nodes, then decrypts the received ciphertexts with secret keys sk_1 and sk_2. After decryption, the aggregator removes the random value $\sum_{i=1}^{N} r_i$ from the aggregate by subtracting $Dec_{sk_1}(c_1)$ from $Dec_{sk_2}(c_2)$, thus obtaining the aggregated measurements with the Laplace noise. Specifically,

$$c_1 = \prod_{i=1}^{m} c_{i1} = Enc_{pk_1}\left(\sum_{i=1}^{N} r_i + \sum_{i=1}^{N} x_i + \sum_{i=1}^{N} Y_i\right)$$

$$c_2 = \prod_{i=1}^{m} c_{i1} = Enc_{pk_2}\left(\sum_{i=1}^{N} r_i\right)$$

where x_i and r_i are the measurement and random value generated by node i, respectively, and Y_i is the noise share (which is 0 or follows $\mathcal{L}(S\sqrt{p}/\epsilon)$) added to the aggregate by node i. Therefore,

$$Dec_{sk_2}(c_2) - Dec_{sk_1}(c_1) = \sum_{i=1}^{N} x_i + \sum_{i=1}^{N} Y_i$$

and hence the aggregator obtains the noisy aggregate which is ϵ-differential private due to Theorem 2 and 1. In particular, each node repeats the coin tossing until the first node succeeds to get 1 (head), which then notifies the rest of the nodes that they do not need to generate more noise, hence $Y = 0$ for all subsequent nodes. In other words, we have a geometrically distributed number of random values drawn from the Laplace distribution with scale $\mathcal{L}(S\sqrt{p}/\epsilon)$, which means that $\sum_{i=1}^{N} Y_i$ follows a Laplace distribution with $\mathcal{L}(S/\epsilon)$ based on Theorem 2. Moreover, as $p = 1/N$, all nodes generate Laplace noise exactly once with large probability. Nevertheless, p is a parameter which can be set depending on node failures hence providing increased robustness and flexibility over prior works.

Notice that, in the geometric distribution, we must have infinite possibilities to succeed, which might not be the case if each node tosses the coin exactly once (i.e., with some positive, albeit small probability none of the nodes have head after finishing the above protocol, which means that the Laplace noise shares will not sum up to the required Laplace noise needed for ϵ-differential privacy). To alleviate this problem, we allow the nodes to make as many rounds as needed for one successful coin toss in the DFS tree. Therefore, we need to repeat the above protocol until at least one head occurs at any node where each node adds Laplace noise to the aggregate (without adding their measurement x to the random r in Line 16 of Alg. 2).

Motivation of geometric divisibility: There have been proposed several schemes for distributed noise generation to guarantee differential privacy [14], all of them are based on the divisibility of the Laplace distribution. The reason we chose geometric divisibility for our model lies in its flexibility. In particular, any network nodes may fail from time to time due to various reasons; if we used any technique described in [14], the failed nodes would not add noise to the sum which would imply extra noise generation tasks from other nodes, or the resetting of the parameters of the distribution. One workaround for this problem could be to select a subset of all nodes for the noise generation task, but this is difficult for distributed systems. In our scheme, there is no need for such coordination; upon the detection of the failure of a child node, the parent can report its own measurement towards its parent without any modification of the protocol. This is because G in Algorithm 2 is drawn independently at each sensor node. Moreover, the probability p of this biased coin toss can also be flexibly adjusted depending on the anticipated number of node failures which also provides stronger robustness.

B. Extension to a malicious aggregator

In Algorithm 1, the aggregator can easily decrypt the partial sums, corresponding to each of its children, before forwarding that to other children, thus it can learn the partial sums of the aggregate. To overcome this problem, the *children* of the aggregator can add additional random value that cancel out when their partial sums are summed. For example, if node P_i adds $+R_{i,j}$, then another child P_j of the root node needs to add $-R_{i,j}$ to its partial sum[3]. This way the aggregator must add all

[3]A similar method is used in [15]

the partial sums belonging to each of its children in order to get the correct aggregate. This implies that a secure channel needs to be established between any pair of children to agree on the value of $R_{i,j}$. For example, the children of the aggregator can derive a shared secret key K, using any key exchange protocol such as Diffie-Hellman, which is known to all the children of the aggregator except the aggregator[4]. Then, similarly to [15], $R_{i,j}$ can be computed as $R_{i,j} = PRF(K, P_i, P_j)$ where $PRF(\cdot)$ is a pseudo-random function.

If the aggregator is malicious, it can also misbehave by lying to one of its child node that $G = 1$ (i.e., it falsely claims that there has been a sensor node before whose coin toss resulted in head). This causes less Laplace noise to be added in the network than what is required to achieve ϵ-differential privacy. We can however easily amend Algorithm 1 to resist against such attack by using key K shared between all children of the aggregator. In particular, the children of the aggregator can compute a message authentication code (MAC) using K on the value of G and attach this MAC to the message sent to the aggregator. This MAC is required to be forwarded by the aggregator to other children as part of the message in Line 5 of Algorithm 1, and hence, any child node can detect, by verifying the MAC, if the aggregator modifies G.

C. Analysis

First, consider the requirements of security based on secure multi-party computation described in our *Privacy and Security Model*.

Security in the presence of semi-honest adversaries:

- *Privacy:* Complies. No node learns anything more than its prescribed output. The root learns some additional information - the partial sums of its children and the partial sums of the random numbers-, but it cannot derive the individual inputs.
- *Independence of inputs:* Complies. All inputs are encrypted, one node has to break the encryption in order to learn anything.
- *Output delivery:* Complies trivially.
- *Correctness:* Complies trivially.
- *Fairness:* Complies trivially.

Security in the presence of malicious adversaries: The privacy of the above SMPC still complies. If the root is the adversary unfortunately even independence fails, since the root can in any way alter the result depending on the received sum. Moreover, with this kind of an adversary we cannot guarantee any other requirement. Although, if an inner node is malicious independence complies, but the rest are do not regarding the subtree under the malicious node.

The reason for adding random numbers to the output in the algorithm is the following. Assume that we expect the inputs to be in a closed, short interval, taking discrete values. In such a case anyone could try all values by applying *brute-force* attack to get the information. The pairs of keys are used for the following reason. If we used no encryption, noise nor random numbers we could face several attack scenarios. For example, if the inputs were very diverse, then a partial sum at an inner node would not carry any information about the underlying sub-tree or the global graph for a node. However if the values are similar one could easily approximate the size of a subtree or even the whole graph. Finally, if an eavesdropper had access to one node's incoming and outgoing messages it could easily calculate the node's input, and also the partial sum sent to the node.

The second key which encrypts the (sum of) random numbers is necessary because we can eliminate the first attack mentioned above. The first key - which encrypts the sum of the measurements, the noise and the random number(s) - is used for preventing the eavesdropper's attack, but if we used solely this key, then an eavesdropper could still capture the incoming and the outgoing messages of one node, encrypt the random numbers with the broadcasted key, and by simple subtraction learn that nodes measurement. Thus the need for two different homomorphic encryption keys.

Differential privacy: According to Theorem 2 on the geometric divisibility of the Laplace distribution with $\mathcal{L}(\lambda)$, the algorithm generates μ_p values drawn from the Laplace distribution with parameters $\mathcal{L}(\lambda\sqrt{p})$, where μ_p is a random variable having geometric distribution. The sum of these values has distribution $\mathcal{L}(s)$. The aggregated result with the noise is in line 11 of algorithm 1:

$$\sum_{i=1}^{N} x_i + \sum_{j=1}^{\mu_p} Y_j = \sum_{i=1}^{N} x_i + Y_{\mathcal{L}(\lambda)}$$

where Y has Laplace distribution $\mathcal{L}(\lambda)$.

We used a biased coin with probability $p = 1/N$, because the geometric distribution is the probability distribution of the number X of Bernoulli trials needed to get one success, supported on the set $1, 2, 3, ...$; therefore we get a geometric random variable number of nodes. Therefore the nodes align in a sequence of the DFS tree and keep on sequentially flipping a biased coins independently from each other until they get the first success. Furthermore, we want to set the probability of success of the geometric distribution to $1/N$, where N is the number of nodes in the graph. Thus the expected value of a random variable with geometric distribution is $1/p = N$, hence with high probability we are going to have all the nodes in the graph adding noise to their output exactly once. Since the geometric distribution has infinite support we cannot limit the number of trials to N. Therefore if all nodes have already tossed a coin but none succeeded, then we must restart the experiment from the first node until we succeed, thus we gain the infinite support of trials.

In summary, since Theorem 2 is fulfilled by the algorithm it follows that differential privacy is preserved.

VI. CONCLUSION

In this paper we have presented a new method for preserving ϵ-differential privacy in a distributed sensor system. We have

[4]Notice that sensor nodes (i.e., producers) do not collude with the aggregator (i.e., organization)

presented our model as a strongly connected graph having processing units at the nodes. These participants want to engage in a privacy preserving computation to gain the aggregated result of their measurements. We have applied secure multiparty computation protocols as basic building blocks to preserve security; moreover, we have introduced a new distributed noise generation protocol, where we used the geometric infinite divisibility of the Laplace distribution. This distribution has a property, namely the geometrically distributed number of noise segments, that we utilised to make our protocol more robust against node failures, and flexible in the expected value of the number of nodes participating in the noise generation.

Building an even more secure version of an algorithm as always is a challenge. Here the next step could be to create secure versions under the assumption of malicious nodes. Considering pseudo-random generators and synchronization in order to test a node's honesty is a possible approach.

Future work: This paper has focused on the feasibility of privacy preserving data aggregation over Multi-hop networks. Performance evaluation of the proposed algorithms in both wireless and wired multi-hop networks, incorporating energy efficiency and computational constraints, constitutes important future work.

ACKNOWLEDGMENT

First, I would like to express my special thanks of gratitude to Gergely Ács and to Gergely Biczók who provided insight and expertise that greatly assisted my work. Second, I would like to thank my M.Sc. thesis adviser, András Lukács for his interesting ideas and guidance.

REFERENCES

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," *IEEE communications magazine*, vol. 40, no. 8, pp. 102–114, 2002.

[2] J. Luo and J.-P. Hubaux, "Joint mobility and routing for lifetime elongation in wireless sensor networks," in *Proceedings IEEE 24th Annual Joint Conference of the IEEE Computer and Communications Societies.*, vol. 3. IEEE, 2005, pp. 1735–1746.

[3] C. Clifton, M. Kantarcioglu, J. Vaidya, X. Lin, and M. Y. Zhu, "Tools for privacy preserving distributed data mining," *ACM SIGKDD Explorations Newsletter*, vol. 4, no. 2, pp. 28–34, 2002.

[4] C. C. Aggarwal and S. Y. Philip, *A general survey of privacy-preserving data mining models and algorithms*. Springer, 2008.

[5] Y. Lindell and B. Pinkas, "Secure multiparty computation for privacy-preserving data mining," *Journal of Privacy and Confidentiality*, vol. 1, no. 1, p. 5, 2009.

[6] R. Cramer and I. Damgård, *Multiparty Computation, an Introduction*. Basel: Birkhäuser Basel, 2005, pp. 41–87. [Online]. Available: http://dx.doi.org/10.1007/3-7643-7394-6_2

[7] A. C. Yao, "Protocols for secure computations," in *2013 IEEE 54th Annual Symposium on Foundations of Computer Science*. IEEE, 1982, pp. 160–164.

[8] O. Goldreich, "Secure multi-party computation," *Manuscript*, 1998.

[9] M. Raynal, *Distributed Algorithms for Message-Passing Systems*. Berlin, Germany: Springer-Verlag, 2013.

[10] N. A. Lynch, *Distributed Algorithms*. The Morgan Kaufmann Series in Data Management Systems, 1996.

[11] T. Raeder, M. Blanton, N. V. Chawla, and K. Frikken, "Privacy-preserving network aggregation," in *Pacific-Asia Conference on Knowledge Discovery and Data Mining*. Springer, 2010, pp. 198–207.

[12] J. Brickell and V. Shmatikov, "Privacy-preserving graph algorithms in the semi-honest model," in *International Conference on the Theory and Application of Cryptology and Information Security*. Springer, 2005, pp. 236–252.

[13] K. B. Frikken and M. J. Atallah, "Privacy preserving route planning," in *Proceedings of the 2004 ACM workshop on Privacy in the electronic society*. ACM, 2004, pp. 8–15.

[14] S. Goryczka, L. Xiong, and V. Sunderam, "Secure multiparty aggregation with differential privacy: a comparative study," in *Proceedings of the Joint EDBT/ICDT 2013 Workshops*. ACM, 2013, pp. 155–163.

[15] G. Ács and C. Castelluccia, "I have a dream!(differentially private smart metering)," in *International Workshop on Information Hiding*. Springer, 2011, pp. 118–132.

[16] Y. C. Hu and A. Perrig, "A survey of secure wireless ad hoc routing," *IEEE Security and Privacy*, pp. 28–39, 2004.

[17] L. Kissner and D. Song, "Privacy-preserving set operations," in *Advances in Cryptology–CRYPTO 2005*. Springer, 2005, pp. 241–257.

[18] B. P. Yehuda Lindell, "Privacy preserving data mining," *Annual International Cryptology Conference*, pp. 36–54, 2000.

[19] C. Dwork, "Differential privacy: A survey of results," in *International Conference on Theory and Applications of Models of Computation*. Springer, 2008, pp. 1–19.

[20] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," *International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 223–238, 1999.

[21] T. K. Kotz, Samuel and K. Podgorski., *The Laplace Distribution and Generalizations*. Springer, 2001.

Szilvia Lestyán received B.Sc. and M.Sc. degrees both in applied mathematics from the Eötvös Loránd University, Budapest, Hungary, in 2013 and in 2015 respectively. Currently she is applying for a doctorate course (PhD) in informatics at the Budapest University of Technology and Economics, where she will conduct research at the Laboratory of Cryptography and System Security (Crysys Lab) in the field of machine learning in privacy and security.

Multi-Camera Broadcasting Model with Automation of Optimal Scene Switching

D. Cymbalak, F. Jakab, M. Michalko, O. Kainz and R. Vapenik

Abstract— **Manuscript deals with introduction of model for automatic selection of the scene with the best position of the object of interest in a multi-camera live broadcasts. The novel metric for evaluation of object appearance in multi-camera scenes was proposed and designed following the deep analysis of relevant broadcasting technologies and object tracking methods. Evaluation of object appearance in scene comprises not only from the location and size of the object of interest in the actual frame but also from streaming transmission parameters and the subjective rating from the broadcast recipients. The proposed metrics serve as the basis for the establishment of a system for selecting the best scene with switching in the real-time. Model has been experimentally deployed in two alternative implementations using common and mobile devices. Results were compared with human based broadcast direction. Based on this comparison, the ability to respond to changes in the scene and also to capture the object of interest in the stream was observed. The resulting application of model should be adapted in different fields such as broadcast of conferences, sport events or security systems.**

Keywords*— *Broadcast, Multi-camera, Scene selection, Object tracking

I. INTRODUCTION

In recent years there has been a tremendous expansion of video technologies in terms of internet traffic. The amount of this traffic has grown exponentially and led to the formation of a new technologies dealing with the video processing, distribution and even recognition. Research presented in this paper is addressing the interconnection of the outputs from the late developments in streaming and computer vision to the area of multi-camera systems with automatic director.

We support research activities in Slovakia/This project is being co-financed by the European Union. Paper is the result of the Project implementation: University Science Park TECHNICOM for Innovation Applications Supported by Knowledge Technology, supported by the Research & Development Operational Programme funded by the ERDF.

D. Cymbalak is with University Centre for Innovation, Technology Transfer and Intellectual Property Protection on Technical University of Kosice, Slovakia (e-mail: david.cymbalak@cnl.sk).

F. Jakab is with University Centre for Innovation, Technology Transfer and Intellectual Property Protection and Department of Computer and Informatics on Technical University of Kosice, Slovakia (e-mail: frantisek.jakab@cnl.sk).

M. Michalko is with Department of Computer and Informatics on Technical University of Kosice, Slovakia (e-mail: miroslav.michalko@cnl.sk).

O. Kainz is with Department of Computer and Informatics on Technical University of Kosice, Slovakia (e-mail: ondrej.kainz@cnl.sk).

R. Vapenik is with Department of Computer and Informatics on Technical University of Kosice, Slovakia (e-mail: roman.vapenik@cnl.sk).

Tracking the object of interest in a scene from multiple cameras has become principal focus of the many researches, especially those dealing with security systems. Multi-camera broadcasts, however, exist also in other areas of life. Tracking of an object in video with subsequent shot evaluation is generally not the focal point of researches. Due to this reason, the ambition of this paper is to introduce a solution, which is to replace the manual switching of the output image in multi-camera streaming, i.e. provide the new approach to personalized broadcast, where each viewer receives a directed broadcast in real-time based on prior preferences and defined object of interest in the scene. Goal is to create an automatized model for streaming of exactly one video source, based on periodic evaluation of multiple video sources. Such source is to have the highest evaluation at given moment following the proposed metric. Idea of metric used for evaluation lies in rating of video sources based on actual position, size and other selected parameters of shot. Prior to design and implementation, the analysis of current streaming technologies is carried out as a theoretical basis for proposal of streaming management mechanisms and also another analysis of current detection of tracking algorithms resulting in a proposal of mechanism enabling evaluation of sources.

II. MULTI-CAMERA STREAM AND OBJECT TRACKING

A. Multi-cameras Systems

Views from individual cameras utilised in multi-camera system may overlap and continuously cover specific part of space or can be isolated without any overlapping, providing there is a greater distance between cameras.

Multi-camera system with overlapping views may be utilized to estimate the height of the tracked object in 3D space [1] or in creation of a global map of covered area, while providing the location of tracked objects on a map. In case of this configuration, the object is often detected concurrently by several cameras. For that reason, utilization of methods for definition of common areas in image and common points of interest is appropriate [2]. Field of view (FOV) lines are constructed based on fields of view [3], these lines are common for several views. Tracking of objects in case of multi-camera system with non-overlapping views from cameras is troublesome mainly due to separation in space and time during tracking of the object. In this case, the distance in time and space cannot be used as relevant information between particular nodes of system, unlike tracking approaches that utilize one camera. Example of utilization of methods for object tracking in multi-camera systems is selection of tracked person across the viewing areas, case of

security systems [4]. Another field of utilization is highlighting the position of objects, e.g. players, ball, puck or other gear utilized at sports events.

Multi-camera surveillance systems commonly indicate the tracked object in a form of highlighted geometrical primitives surrounding the object across the outputs from all cameras or mark the position of object in global view on the map of monitored space. Due to this, the viewer has to monitor the output from all cameras and seek the highlighted square, circle or points of tracked object, i.e. coordinates and position in global map. Object in global map represents particular point, not the entire video. Useful solution is hence to stream the content from individual cameras of system, while utilizing streaming technologies and show only the view from one camera. One that detects the tracked object in scene and provides its best location.

B. Streaming Technology

Streaming technologies ensure the transfer of multimedia content over the computer network, in both audio and video along additional content, from the provider to the recipient [5].

Many advantages emerge when we compare streaming multimedia formats to standard ones [6], the most significant are the following: possibility to control the bit rate of content, content protection against unauthorized use, possibility to select or filter the recipients of content and easy content management. Bearing in mind just stated and particularly due to the availability, these technologies are widely utilized in education systems, i.e. e-learning, and also in videoconferencing solutions [7]. Not only receiving of content but also broadcast directly from mobile devices is possible thanks to advanced development in the area of mobile devices [8].

Currently prevails a certain form of inconsistencies when it comes to usage of codecs and streaming formats in different browsers. H.264/AVC is an advanced codec developed by groups ITU-T VCEG and ISO/IEC MPEG. Codec consists of two layers: video coding layer (VCL) and network abstraction layer (NAL) [9]. VCL represents the video content itself and NAL is handling the structure of data, it is also carrier of information necessary for transfer. Such data is used by transport layer and storage media. [10].

Inherent component of streaming technologies are streaming protocols that ensure the transfer of packets with multimedia content. Streaming video server provides distribution of multimedia content into multiple packets and also initializes transfer to the end customer. Variant of client-server model is a content delivery network (CDN) model. Main streaming server, in the solutions based on CDN, initially sends multimedia content to a group of content delivery servers that are strategically deployed at the edge of a network. Another emerging model of service delivery related to streaming is distribution over P2P networks [11].

C. Objeckt Tracking in Stream

Following section is related to tracking itself or tracing the object in the sequence of images, i.e. in the video, considering one camera system. Analysis carried out for one camera system is to be beneficial in the process of proposing the evaluation metrics of multi-camera system. Resulting from this is the real model proposed in this paper.

Image detection methods use image segmentation, this technique divides the image into the area referred to as the foreground, where the tracked object is to be found. Second part is called background, this part is not relevant for further processing. The resulting foreground is consisted of so called image elements and based on predefined pattern the relevant element is detected. Foreground may be extracted based on certain parameters such as colour, shape or texture.

In terms of tracking the object in the video it is important to carry out object detection on the selected series of frames, separated by time, of the particular video. The location with respect to the captured view is calculated for each processed frame that contains the detected object. Series of location data subsequently define the nature of the object's movement, either in the form of a sequence of points with coordinates or in the form of a function.

Detection of moving objects in the video can be accomplished through the filtering out the background. Filtering of the background based on the chromaticity or gradient may be implemented on the level of the pixel, region or the entire image. Methods for tracking of deviations in the individual video frames face various issues that occur during capturing of a real environment, these are: gradual or sudden changes in lighting, low level of colour uniqueness of tracked object from the background, unwanted shadow of the object, change in the background of the object being tracked or the constant movement of the object when detection initializes. All just stated factors affect the recognition success rate. Hence it is only appropriate to use so-called learning algorithms to continuously monitor changes in the tracked object and also complement the model pattern used for object detection.

Common tracking system consists of three components: object representation, dynamic model and search mechanism. Object itself may be represented by either a holistic descriptor such as colour histogram and related brightness value of a pixel, or by local descriptor such as local histogram and chromaticity. Dynamic model is used to simplify the computational complexity in tracking of the object. Search mechanism is used to optimize the tracking of the real object and can utilize both deterministic and stochastic methods. Essential component in tracking methods is a motion model that can express, for example, translational movement, transformation based on similarities and the affinity transformation [12].

The existing methods used in object tracking in real-time include: incremental visual tracking (IVT) [13], variance ratio tracker (VRT) [14], fragments-based tracker (FragT) [15], online boosting tracker (BoostT) [16], semi-supervised tracker (SemiT) [17], extended semi-supervised tracker (BeSemiT) [18], Tracker (L1T) [19], multiple instance learning tracker (MIL) [20], visual tracking decomposition algorithm (VTD) [21] and track-learning-detection method (TLD). Reliability and functionality of these algorithms can be verified, for

example, by measuring the success while keeping up the detection of the monitored object and by shift of central position detection. In this paper two algorithms were selected, reporting the best results for use in the proposed system: TDL and CMT algorithms.

TLD (Tracking-Learning-Detection) algorithm was developed for tracking and detection of objects in a video in a real-time. The object of interest is defined following the initialization of the square in one frame, such frame serves as a template. TLD simultaneously tracks the object, determines its features from the following frames and detects and verifies the occurrence of an object in the image. The result itself is tracking of the object in real-time. Accuracy and reliability is constantly improving as the duration of the tracking is getting longer, cause of this is learning of new features of tracked object, e.g. change of position, size, rotation, or luminosity [22].

Tracking algorithm used in the TLD is based on phase of recursive tracking in forward and reverse direction (Fig. 1), Canada-Lucas algorithm is executed in both directions and median is calculated as a final step. Detection in the TLD uses sparse filtering, file classifier and the nearest neighbour classifiers. TLD learning is performed in the form of P-N learning, extracted data is classified, while obtaining the its structure in the form of object path, positive (P) constraints are applied, with subsequent implementation of negative (N) constraints, then new data is generated and updated in the object classifier. P-type image segments represent objects with a high probability of correlation, when compared with the template, and vice versa, image segments of N-type represent objects with low probability of correlation [23].

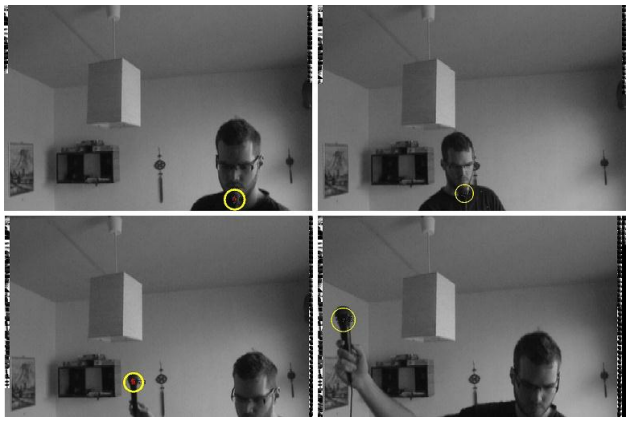

Fig. 1. Experimental testing of Tracking-Learning-Detection algorithm for tracking the microphone in the video stream.

CMT algorithm - Consensus-based matching and tracking is based on the keypoints method in combination with a matching-and-tracking framework (Fig. 2). CMT algorithm and his pythom implementation (pyCMT) expects input to be a sequence of frames and initialization region as pattern for detection in the very first frame. The goal of this algorithm is to renew the position of the pattern in each following frame and thus obtain the position of the tracked object. The output is the information of tracked object's position. Operation of CMT algorithm includes three essential steps: comparison of the correlation and keypoints tracking, voting and approval. To localize the object in each frame, the voting on position of central point from each keypoint is acquired. In order to detect the other points, the system based on approval of correlation in the voting is used. Changes in size, location and rotation of detection region are visible as the transformation of votes follows the specific position of keypoints. Utilization of the fast keypoint detectors and binary descriptors introduces suitable domain for the application of the algorithm in terms of video processing in a real-time [24].

Fig. 2. Experimantal realization of tracking the head, microphone and hand based on CMT algorithm.

III. DESIGN OF MODEL FOR OPTIMAL SHOT SELECTION

The principal goal is to propose a metric that is to combine rating based on parameters with regard to the presence of the object in the shot as gained by the tracking algorithm, having the parameters of picture and voice. As a result, each node of multi-camera system is to be evaluated every second, based on this in each second the source of video stream is estimated and provides the best view and quality on the object of interest. Subsequently such shot becomes the primary and the only broadcasted view.

A. Metric for evaluation of video sequence

The principal metric in the proposed model will evaluate video sequence of each video source connected to the multi-camera system. Based on this metric the system will be able to determine which shot is best designed to visually track the object of interest in real-time. The metric (M_n^t) for evaluation of video sequence has been designed as the sum of the five components of the metrics, which are multiplied by a constants defined in the input vector (Equation 1).

$$M_n^t = (c_p \times Mp_n^t + c_v \times Mv_n^t) \times Md_n^t + c_h \times Mh_n^t + c_q \times Mq_n^t \qquad (1)$$

Depending on the type of broadcast in which the proposed model is to be deployed, the utilization of c constants allows adjustment of weights of individual metric components, or exclusion of selected components from the evaluation.

Positional component of metrics (Mp_n^t), used for the evaluation of video sequence, is based on data as extracted from tracking algorithm deployed in every stream of multi-camera broadcasts. A significant effect on metrics component are the x and y coordinates, representing the occurrence of the

object's central point contained within the input vector for a particular source of the stream. The positional component itself has been designed to act as the optimal composition of the golden ratio, i.e. the centre of the tracked object of interest should be located as close as possible to the nearest golden section of the shot (Fig. 3).

In this case, it is also possible to seek a composition where the object of interest is approaching the best location with respect to the termination of Fibonacci spiral in the four different shots. In this case, zones are designed to keep the most highly rated areas closests to the intersections of the golden rations of shot (see Equations 2).

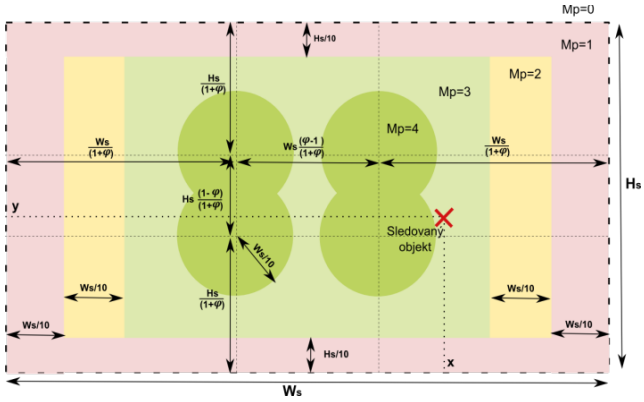

Fig. 3. Zonal division of scene based on golden ratio with positional component of metric calculation.

$$\boldsymbol{Mp_n^t = 0} \Leftrightarrow \; x = null \;\; OR \;\; y = null$$

$$\boldsymbol{Mp_n^t = 1} \Leftrightarrow \; x < \frac{W_s}{10} \;\; OR \;\; x > W_s - \frac{W_s}{10}$$

$$OR \;\; y < \frac{H_s}{10} \;\; OR \;\; y > H_s - \frac{H_s}{10}$$

$$\boldsymbol{Mp_n^t = 2} \Leftrightarrow \; x < \frac{W_s}{5} \;\; OR \;\; x > W_s - \frac{W_s}{5}$$

$$\boldsymbol{Mp_n^t = 4} \Leftrightarrow$$

$$\left(x - \frac{W_s}{(1+\varphi)}\right)^2 + \left(y - \frac{H_s}{(1+\varphi)}\right)^2 < \left(\frac{W_s}{10}\right)^2$$

$$OR \; \left(x - \frac{W_s}{(1+\varphi)}\right)^2 + \left(y - \frac{\varphi \times H_s}{(1+\varphi)}\right)^2 < \left(\frac{W_s}{10}\right)^2$$

$$OR \; \left(x - \frac{\varphi \times W_s}{(1+\varphi)}\right)^2 + \left(y - \frac{H_s}{(1+\varphi)}\right)^2 < \left(\frac{W_s}{10}\right)^2$$

$$OR \; \left(x - \frac{\varphi \times W_s}{(1+\varphi)}\right)^2 + \left(y - \frac{\varphi \times H_s}{(1+\varphi)}\right)^2 < \left(\frac{W_s}{10}\right)^2$$

$$\boldsymbol{Mp_n^t = 3} \Leftrightarrow else \qquad (2)$$

Dimensional component (Mv_n^t) (Equation 3) of the proposed metrics is based on the parameters as derived by tracking algorithm for estimation of the actual height h and width w of tracked object in the shot with dimensions W and H. In this situation, the evaluation of this component is to be increased with increasing size of the reference object.

$$Mv_n^t = \sqrt{\frac{w^2 + h^2}{{W_s}^2 + {H_s}^2}} \qquad (3)$$

Component concerning the reliability (Md_n^t) (Equation 4) of the object detection is directly dependent on the input data. This data represents reliability of detection d of tracking algorithm at time t contained within the input vector. Consequently, the component is to be in the form of percentage correlation, indicating the match of detected object in the image at time t to the pattern used for tracking.

$$Md_n^t = d \qquad (4)$$

The proposed metric also includes a component enabling the control of the resulting metric through the subjective evaluation (Mh_n^t) by the recipients of stream from multi-camera broadcasts. In case of specific broadcast, each recipient would be able to evaluate each stream source at time t by a percentage value, i.e. change own evaluation dynamically throughout the broadcast. In order to guarantee the relevant processing of the evaluation of individual stream sources it is essential to introduce the calculation of evaluation based on Bayesian estimation – bearing in mind the stream is dependent on the number of recipients who are able to evaluate it, not only on the average evaluation (Equation 5).

$$Mh_n^t = \frac{\left(\sum_{k=1}^{k=j} r_k\right) + (c_{min} \times r_{av})}{j + c_{min}} \qquad (5)$$

Following the analysis of evaluation methods of video quality, the calculation of objective video quality component of metric (Mq_n^t) (Equation 6) dependent on three fundamental parameters of picture was designed. These image parameters are the following: resolution of video stream (width W and height H), the actual transmission bandwidth B^t (bit-rate) and frame rate F^t compared to optimal bandwidth B_{op} and optimal frame rate F_{op}.

$$Mq_n^t = \frac{\sqrt{{B_{op}}^2 - \left(B_{op} - B^t\right)^2}}{2 \times \left(\sqrt{{W_s}^2 + {H_s}^2}\right) \times 10^{-3}} * \frac{\sqrt{{F_{op}}^2 - \left(F_{op} - F^t\right)^2}}{F_{op}} \qquad (6)$$

B. *Processing the results of evaluation*

Processing requires individual results of partial evaluation metrics of image to be stored in the matrix (Equation 7) containing other sub-metrics for all sources of stream n at time t:

$$Rcomp^t = \begin{pmatrix} Mp_1^t & Mv_1^t & Md_1^t & Mh_1^t & Mq_1^t \\ Mp_2^t & Mv_2^t & Md_2^t & Mh_2^t & Mq_2^t \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ Mp_n^t & Mv_n^t & Md_n^t & Mh_n^t & Mq_n^t \end{pmatrix} \qquad (7)$$

Subsequently, the results of overall metrics R^t for each source at time t assemble the image metrics vector (Equation 8) of results for the entire multi-camera system in time t:

$$R^t = (M_1^t \;\; M_2^t \;\; \ldots \;\; M_n^t) \qquad (8)$$

The final step is to select the stream source in real-time following the calculations of chosen metrics. Such source provides, in the specific broadcast the highest result of the

overall evaluation. Basis of selection is to calculate the maximum (Equation 9) of vector R, i.e. maxima of resulting numerical evaluations of all currently connected broadcasting sources:

$$\max_{0<k\leq n} M_k^t \tag{9}$$

Each image capturing device generates a certain latency until the image gets to the output. In the terms of multi-camera heterogeneous system, e.g. consisted from standard SDI cameras, mobile phone with enabled 3G transfer, sports camera with Wi-Fi connectivity or IP camera via fixed line, the delay between video input and the output has to be on the same level. The ambition is to ensure that the object of interest in the image at time t is present in the same global position for all the input video sources during processing. This can be done indirectly by processing the audio track of stream, where the part of audio track from reference source with the lowest latency is selected at regular intervals and compared with other sources. The system would therefore be able re-evaluate how many *ms* is the shift from detected audio sequence of specific source (Fig. 4).

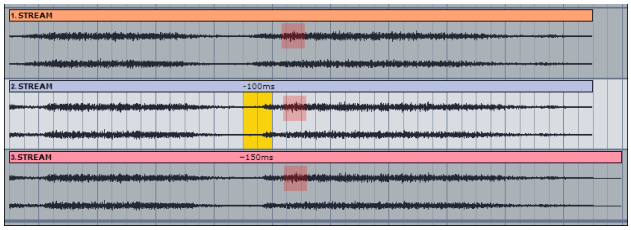

Fig. 4. Synchornization of delay via audio track of multiple streams

IV. IMPLEMENTATION OF MODEL

Building a system following the proposed model is possible on multiple levels according to the character of use. Implementation diagram of the system, based on the model using the external video sources, is depicted in Fig. 5. Note that distribution mechanism is employed prior to the evaluation.

Individual sources of live broadcasts from different angles are transmitted through the streaming distribution device, i.e. streaming server. The transferred stream of each video source, acquired from the distribution mechanism, is received and then processed by the tracking algorithm. Input is in the form of single instance per each video source. Results of tracing are sent, in a real-time, by each instance of object tracking mechanism. Evaluation is performed by the calculation mechanism, which receives the initial parameters of metrics as the input, these are: constants for subjective assessment, vector containing the constants of compression ratio and optimal frame rate, and vector encompassing the constants of the individual components of the global metrics. At the same time, the vector comprising of scene parameters and stream quality is provided to the calculation mechanism. Such vector is based on the encoding used in distribution mechanism or input encoder of video source. Evaluation mechanism of recipient associated with the content playback mechanism collects the ratings from recipients and provides them as the input to the calculation mechanism. Calculation mechanism continuously collects the input parameters. Output of this mechanism, a vector of ratings from all the input sources, is sent directly to the control mechanism. The control mechanism determines the best rating and source to be set as the output of the current broadcast, both is done in real-time. Control itself is thus connected directly to the content playback mechanism, where the distribution mechanism provides only the stream with the best rating to the recipient.

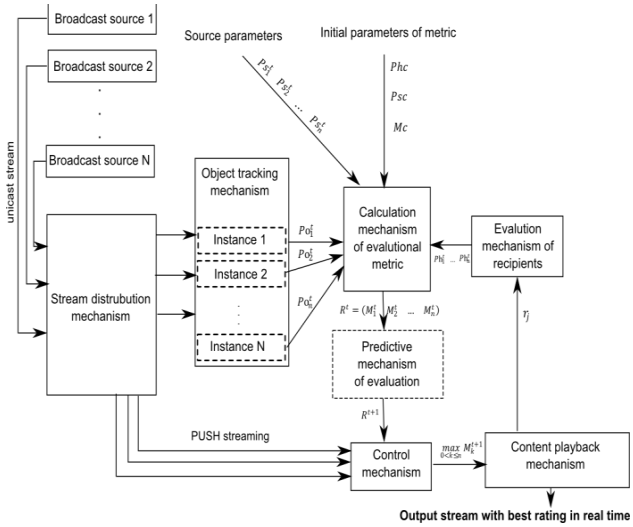

Fig. 5. Implementation scheme with stream distribution mechanism

Several system implementations were carried out as a part of this project, all were following the proposed model for the automatic selection of the optimal shot while utilizing specific streaming and computer vision technologies. One of such system configuration was the implementation encompassing the mobile devices with build-in camera, experimentally linked to the evaluation mechanisms located behind the streaming server (Fig. 6).

In this configuration, two Android mobile devices, one iOS mobile device and sports GoPro camera were used as the sources of the image. Image extracted from Android devices was received directly by WSE streaming server, in this case by means of created RTMP encoder. iOS devices utilized Wowza GoCoder and stream from GoPro camera was distributed via FFmpeg to WSE server. As a result, all the image sources were distributed through streaming server. Subsequently, each distributed RTMP stream was processed by FFmpeg in separate instances of pyCMT tracking algorithm. Individual pyCMT instances passed on results of the position and size of the tracked object for further calculation of the final metrics, along with the WSE server stream and calculation of recipients rating parameters. The final metrics values were send, containing the information of maxima and identifier of best evaluated via vmix API. Then the output stream was passed to the output in the virtual mix, which received each stream separately from WSE server. Subsequently, the output stream encoded the required format through FMLE and forwarded it to a recipient's FlowPlayer player and to a control output.

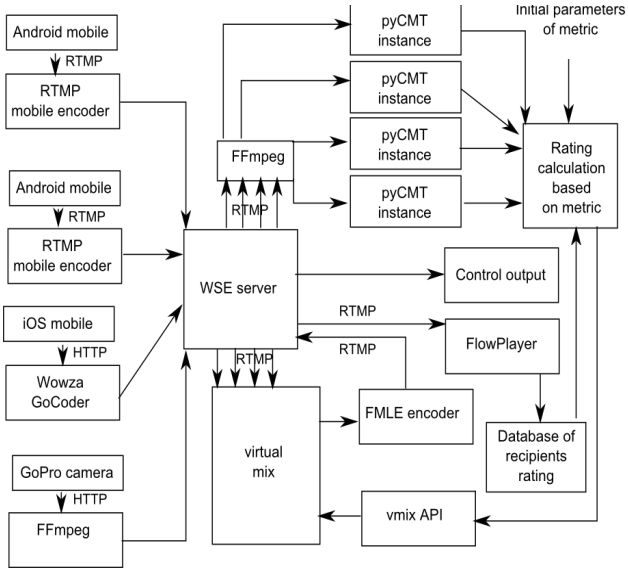

Fig. 6. System configuration with using pyCMT mechanism

Several experiments were carried out in the simulation environment. The moving object of interest was captured simultaneously using multiple cameras, both in different environments and different image dynamics. Then, the feedback, whether the object of interest in sequence t is visible, was retrieved from the recipients. Subjective evaluation of each sequence was done to provide the evaluation of the composition quality of the tracked object and also its distinctiveness when compared to the expectations of the viewer. Comparison included the manual director as is present in the standard system of video mix, this provided the information about the video stream selected as the output in time t. In case of same real-time video sequence, the table for comparison was continuously filled with the results as gathered from both, the automatic director based on the proposed model and manual director in standard video mix. Results included in the table create a map of the object visibility in the video sequence from both perspectives - comparison of the selection of output image and evaluation of composition. This allows us to express the correlation of automatic director to manual director, i.e. when it runs faster or, vice versa, when the lag is present.

Proposed model was experimentally tested on extensive sequences of live broadcasts throughout each development and optimization phase of relevant metrics. Experimental multi-camera broadcast was selected as a sample of the model variability. This included combination of standard cameras and mobile devices build-in cameras. Pattern for the initialization box used for tracking of the object was set to copy the figure of a lecturer in front of blackboard (Fig. 7).

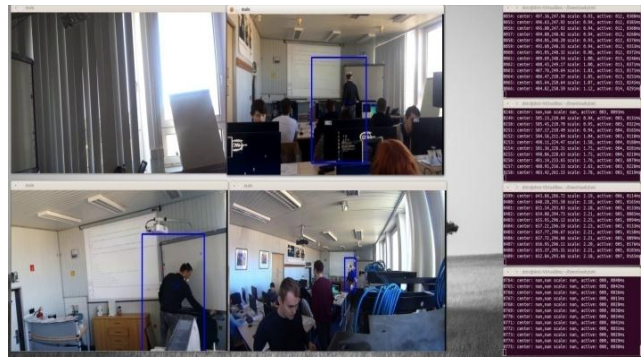

Fig. 7. Experiment of tracking the lecturer in 4-camera stream

Simultaneously, the video streams assigned to a streaming mix were processed and combination of parameters from the evaluation mechanism and another combination of qualitative parameters allowed final evaluation metrics to provide the information of current source. Such source was set, at time t, as the output by streaming mix (Fig. 8).

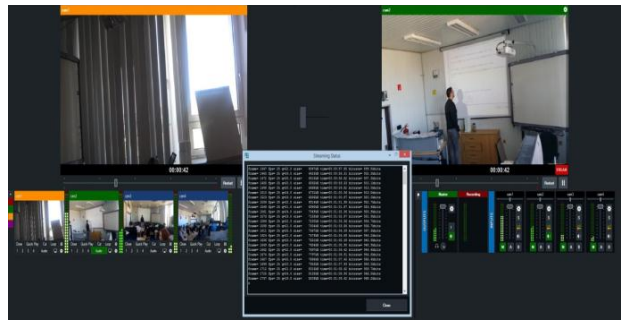

Fig. 8. Experiment of choosing the best rated stream based on tracking

The results of the final evaluation of individual sources for the selected broadcast sequence is depicted on the graph, see fig 9.

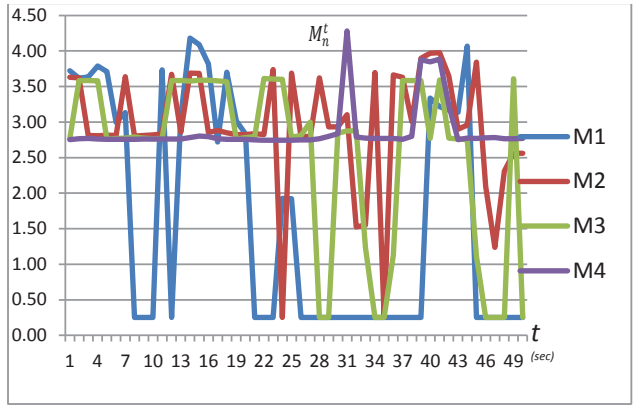

Fig. 9. Results of 4-camera stream evaluation by proposed automatic system

Comparison of the results served for the evaluation of object composition in the selected sequence of a broadcast,

both automatized system using proposed model (blue) and manual director (red) were deployed (see Fig. 10).

This experiment shows that automatic selection of the best view does not match the manual director, dissimilarity rate is estimated to be two thirds. Object of interest (lecturer) was in the case of automatic selection visible throughout the entire broadcast of segment. Manual director achieved error rate of 2% - it means the object was not in the shot in 2% of duration of the broadcast segment. The automatic system scored worst composition rating then manual direction in 36% of duration of broadcast segment. However in 54% of duration of broadcast segment the composition of object of interest (figure of lecturer) with automatic system has better rating then manual direction. In this experiment, the model succeeded especially in case of object arrival and disappearance from the image, response time was in the case of proposed model faster when compared to the manual mode.

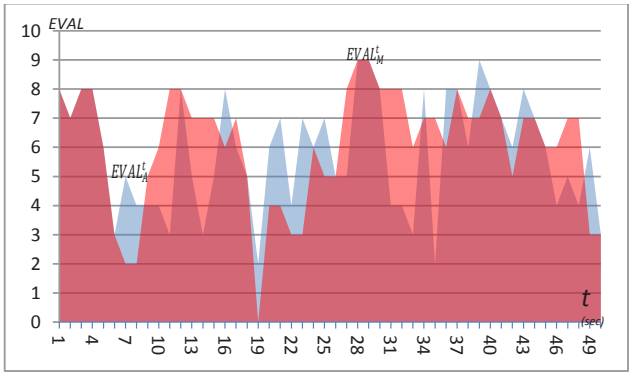

Fig. 10. Comparison of evaluation of composition between proposed model (blue) and manual direction (red) in 4-camera stream experiment

The overall model for the selection of the best image in a multi-camera system proposed in this paper is adaptable for usage in different types of broadcasts. The primary objective was to develop a model for the selection of optimal shot that would be useful for heterogeneous multi-camera system, e.g. broadcasting of the events from multiple angles using different types of devices such as classic camera, mobile phone, sports camera, drone, IP camera, etc. (Fig. 11)

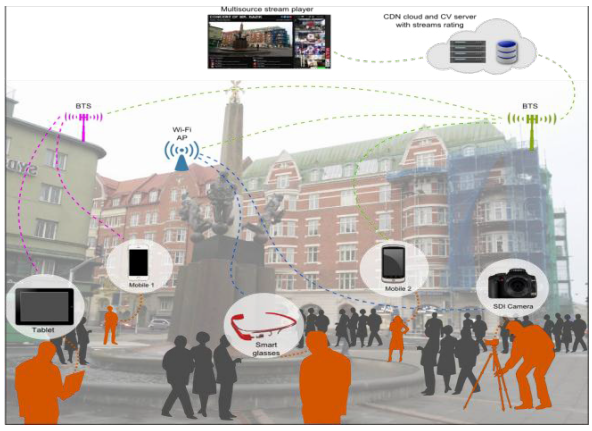

Fig. 11. Example of use case of proposed model

CONCLUSION

In this paper, the innovative model for automatic selection of the most suitable shot regarding the object of interest in the multi-camera system was proposed. Depth analysis of the current streaming and computer vision technology lead to a proposal of evaluation metrics for individual broadcast sources. The proposed evaluation metric was adapted to a different types of uses through changing the value of weights of individual metric components. Overall, the evaluation of multi-camera system sources is derived from several factors: the current position and size of the reference object in the shot, the parameters of the video broadcast and audio track, lastly also the objective and subjective evaluation by viewers. Described evaluation metrics became the basis for the establishment of a system for the selection of the most suitable shot and related switching of the output streaming source in a real-time. The created model was experimentally verified in a number of alternative implementations using standard and mobile devices. The results compared with the standard manual director showed the advantages of model in the form of faster response time to changes in a shot and a tendency to capture the object of interest in the image when being closest to the ideal composition. Experimental testing has shown the ability of adaptation the model for different types of applications, such as broadcast sporting events, security systems, industrial monitoring or conference broadcasts.

REFERENCES

[1] CHU C. et al..: Tracking Across Multiple Cameras with Overlapping Views Based on Brightness and Tangent Transfer Functions, Distributed Smart Cameras (ICDSC), 2011 Fifth ACM/IEEE International Conference on. IEEE, 2011.

[2] ZHU L. – HWANG J. – CHENG H.: Tracking of multiple objects across multiple cameras with overlapping and non- overlapping view, IEEE Intl. Symposium on Circuits and Systems, s. 1056-10360, Taipei, 2009

[3] KHAN S. – SHAH M.: Consistent labeling of tracked objects in multiple cameras with overlapping fields of view, IEEE Trans. Pattern Analysisand Machine Intelligence, vol. 25, no. 10, s. 1355-1360, 2003

[4] ZAMBANINI, S. - BLAUENSTEINER, P. - KAMPEL, M.: Automated multi-camera surveillance for the prevention and investigation of bank robberies in Austria: A case study Crime Detection and Prevention ICDP, 2009

[5] O'DRISCOLL G. : Next generation IPTV services and Technologies, Hoboken: Wiley, 2008, ISBN:978-0470163726

[6] HAYAKAWA T. et al..: Management of Multimedia Data for Streaming on a Distributed e-Learning System, 26th International Conference on Advanced Information Networking and Applications Workshops, 2012

[7] ANDERSON T. : The theory and Practice of Online LEarning, second edition, AU Press : Edmonton, 2011

[8] CHEN D. M. et al..: Streaming Mobile Augmented Reality on Mobile Phones, ISMAR, 2009

[9] DHONSALE K.V. : Overview, implementation and comparison of Audio Video Standard (AVS) China and H.264/MPEG -4 part 10 or Advanced Video Coding Standard, 2012

[10] WIEGAND T. et al..: Overview of the H.264 / AVC Video Coding Standard, IEE Transactions on Circuits and Systems for Video Technology, 2003

[11] LIU Y - GUO Y - LIANG C.: A survey on peer-to-peer video streaming systems, Peer-to-Peer Netw Appl, 2008

[12] WANG Q. et al..: An Experimental Comparison of Online Object Tracking Algorithms, Proceedings of SPIE: Image and Signal Processing Track, 2011

[13] ROSS D. et al..: Incremental learning for robust visual tracking, International Journal of Computer Vision 77(1-3), s. 125–141, 2008

[14] COLLINS R. – LIU T. – LEORDEANU M.: Online selection of discriminative tracking features, IEEE Transactions on Pattern Analysis and Machine Intelligence 27, s. 1631–1643, 2005.

[15] ADAM A. – RIVLIN E. – SHIMSHONI I.: Robust fragments-based tracking using the integral histogram, Proceedings of IEEE Conference on Computer Vision and Pattern Recognition, s. 798–805, 2006.

[16] GRABNER H. – BISCHOF H.: On-line boosting and vision, Proceedings of IEEE Conference on Computer Vision and Pattern Recognition, s. 260–267, 2006.

[17] GRABNER H. – LEISTNER C. – BISCHOF H.: Semi-supervised on-line boosting for robust tracking, Proceedings of European Conference on Computer Vision, s. 234–247, 2008.

[18] STALDER S. – GRABNER H. - VAN GOOL A.: Beyond semi-supervised tracking: Tracking should be as simple as detection, but not simpler than recognition, Proceedings of IEEE Workshop on Online Learning for Computer Vision,2009.

[19] MEI X. - LING H.: Robust visual tracking using l1 minimization, Proceedings of the IEEE International Conference on Computer Vision, s. 1436–1443, 2009.

[20] BABENKO B. – YANG M. – BELONGIE S.: Visual tracking with online multiple instance learning, Proceedings of IEEE Conference on Computer Vision and Pattern Recognition, s. 983–990, 2009

[21] KWON J. - LEE K.: Visual tracking decomposition, Proceedings of IEEE Conference on Computer Vision and Pattern Recognition, pp. 1269–1276, 2010.

[22] KALAL Z. – MATAS J. – Mikolajczyk K.: P-N learning: Bootstrapping binary classifiers by structural constraints, Proceedings of IEEE Conference on Computer Vision and Pattern Recognition, pp. 49–56, 2010.

[23] KALAL Z. - MIKOLAJCZYK K. - MATAS J.: Forward-Backward Error: Automatic Detection of Tracking Failures, International Conference on Pattern Recognition, Istanbul, Turkey, ICPR 2010

[24] NEBEHAY G. - PFLUGFELDER, R: Clustering of Correspondences for Deformable Object Tracking, Computer Vision and Pattern Recognition, IEEE, 2015

D. Cymbalak received his M.Sc. and Ph.D. degree in Informatics from Technical University in Kosice (Slovakia). He is a member of University Centre for Innovation, Technology Transfer and Intellectual Property Protection on Technical University of Kosice. He is also member research institution - Computer Networks Laboratory at Technical University of Kosice. His research includes telepresence technologies, video streaming solutions, web and cloud services and computer vision.

F. Jakab (IEEE member) graduated from the Faculty of Computer Science and Electrical Engineering at the St. Petersburg Institute of Electrical Engineering in the field of System Engineering (Russian Federation). He established Computer Networks Laboratory (www.cnl.sk, in 1995) at TUKE. Main areas of his research activities: computer networks, new form of multimedia based communication (videoconferences, IP streaming). He coordinated important educational initiatives and projects linked to cooperation with practice, international projects in the Leonardo, Tempus, the European Commission Framework Programmes. He was at the birth of a global educational initiative Cisco Networking Academy. He stands behind the success of the Cisco Networking Academy global initiative in the region of the Eastern Europe. He is a head of the Application Section of the Communication Technology Forum Association in Slovakia, director of the University Centre for Innovation, Technology Transfer and Intelectual Property Protection at Technical university of Kosice. In 2006 he was awarded a prestigious award "IT Personality of the Year" in Slovakia. He has participated in the establishment of The Kosice IT Valley Association.

M. Michalko received his M.Sc. and Ph.D. degree in Informatics from Technical University in Kosice (Slovakia). For more than 10 years he is member of well recognized research institution - Computer Networks Laboratory at Department of Computers and Informatics at Technical University of Kosice (DCI TUKE). Now he is an Assistant Professor at DCI TUKE and his lectures are focused on Computer Networks. His research includes multimedia content delivery, video streaming services, web and cloud services, innovative teaching&learning techniques and IoE/IoT solutions.

O. Kainz was born in 1988. In 2013 he graduated (MSc. in Applied informatics) from the Technical university in Kosice, Slovakia. He is a PhD student at the Department of Computers and Informatics of the Faculty of Electrical Engineering and Informatics at the Technical university of Kosice. His scientific research interests include computer vision, e-learning, human-computer interfaces, computer graphics, computer networks, biological engineering and body area network.

R. Vapenik graduated (MSc. in Informatics) from the Technical university in Kosice, Slovakia. He is a PhD student at the Department of Computers and Informatics of the Faculty of Electrical Engineering and Informatics at the Technical university of Kosice. His scientific research interests include streaming technologies, computer networks and multimedia content delivery.

Android APK on-the-fly tampering

Zdeněk Říha, Dušan Klinec and Vashek Matyáš

***Abstract*—The Android operating system is widely deployed and relied upon by both providers and users of various applications. These applications get frequently downloaded from other sources than just Google Play. This makes Android and its application treatment a popular target for attackers. We first present an automated offline attack injecting a previously prepared code to a previously unseen Android application installation file (APK) in an automatic manner. Moreover, we present a novel transparent on-the-fly extension of our attack when a proxy server performs code injection during a new APK download.**

***Index Terms*—Android security, application security, application download, code injection, malware contamination**

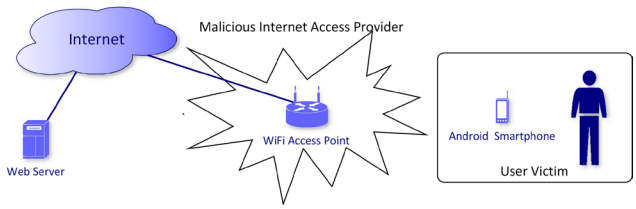

Fig. 1. The high-level architecture of our attacker's setup. The infrastructure for the Internet access (typically a WiFi access point) is under the control of an attacker who can manipulate unprotected communication.

I. INTRODUCTION

The Android mobile operating system has penetrated 88% of the smartphone operating system market by 2016 [5]. The bare operating system as delivered by phone manufacturers typically provides just a basic functionality. Therefore, it is more-or-less expected that most users install additional applications either to enhance smartphone features or just for fun. The official way to obtain Android applications is to use the Google Play service. Android phones use the pre-installed application (client) that directly connects to Google Play servers. Alternative sources of applications are also supported, but this feature is disabled by default for security reasons.

Still, many users activate the feature allowing installation of applications from other (often unknown) sources to be able to install applications with alternative distribution models, not present on the Google Play Store (e.g., tourist guide applications are often distributed locally on-site in places without Internet access).

Various and numerous applications are banned from the distribution in Google Play (e.g., advanced security scanners software requiring root privileges, copyright infringement materials, advertising blocking applications or even privacy tools aimed at stopping other applications from collecting data on users).

We demonstrate two methods of automatically injecting attacker's code (e.g., backdoor) into the APK files transparently to the user. See the high-level architecture of the typical attacker's setup in Figure 1. The user would see the APK download phase progress as usual, but receive a modified file. Since "free" installation of applications from ad hoc sources is a crucial feature for Android smartphones, we raise this issue to both the user and developer communities.

Motivations of the attackers to inject a malware into Android applications can vary. The malware can have the form of a spyware, leaking the location of the user, SMS messages and other sensitive user data, etc.; botnet client, transforming the mobile phone into a zombie, or anything else that can lead to economic or other profit (e.g., Bitcoin mining).

APK file integrity is protected with a digital signature. The list of hashes for practically all the files in a package is digitally signed and stored as a PKCS#7/CMS signature file (including the X.509 certificate of the signer). The digital signature is verified during the installation process and if the verification fails then the installation is aborted. This mechanism is able to detect integrity issues within the APK file (e.g., missing files, extra files or modified files) and addresses download errors (e.g., a truncated APK file).

Experience from other application domains (most notably, but not exclusively, the SSL/TLS) shows that users have serious issues when having to make decisions about Public Key Infrastructure (PKI) tasks and questions [6], [15]. Android is based on a very simplified PKI.

For the APK files, the signer certificate is self-signed and is generated by a developer without any aid of a Certification Authority (CA). When a new application (a new package name) is installed, any certificate is accepted. The signer's certificate is only important in some particular situations – the signer must be the same when upgrading an application, to allow applications to run in the same process and to share code or data between applications through permissions.

In our scenario, we assume that the user is downloading and installing a new application. Therefore, it is easily possible to modify the content of an APK file and afterwards to sign it with a different private key of attacker's choice.

As no CA is involved, the values of the name fields in the (public key) certificate can be arbitrarily chosen by the attacker. To sign the application, we use the same *jarsigner* utility (part of the Java Development Kit) that developers use. We generated a new private key and certificate for our experiment described below.

Affiliation: Masaryk University, Faculty of Informatics, Botanicka 68a, CZ-602 00 Brno, Czechia. (zriha | xklinec | matyas @fi.muni.cz)

A. Aims and limitations of our work

The *core contribution* of this paper is a novel approach for the on-the-fly automated modification of APK files. In the case of the offline APK modification we assume to have the complete APK file at our disposal (i.e., fully downloaded file) and run a script to inject the payload. Yet our primary contribution comes with the demonstration of a code injection (at a proxy) – the online version of the modification modifies the APK on-the-fly while being downloaded from a remote server to the Android device of the victim (i.e., during the man-in-the-middle attack). The online modification must create an impression of a continuous download of the APK. To our best knowledge, the on-the-fly attack is a novel approach not published before.

Our paper investigates the security consequences of the feature allowing for installation of applications from unknown sources and presents a way how to automatically inject malware into Android applications. Security of the Google Play service is out of the scope of this paper.

Our ultimate goal is to demonstrate the ease of injecting an additional code so that it remains hidden from the phone user. The process of the code injection (even into previously unseen applications) is fully automated and the download of the package is not disrupted from the user point of view. The process of the modification works in a streaming mode, changing the APK file on-the-fly.

B. Paper roadmap

In Section II, we map related work on the Android attacks topic. Section III describes the basic offline variant of the attack, Section IV outlines the on-the-fly variant of the attack. Technical details are described in Section V and Section VI demonstrates the practical usability of the proposed approach in our experiments. Section VII briefly discusses possible countermeasures and the following section concludes our paper.

II. RELATED WORK

The APK file modification is not novel. It has been demonstrated several times that the APK file can be decompressed, disassembled, modified and then reassembled and repackaged [25], [1]. There are standard Java tools that can decompress the APK file, disassemble the compiled Java classes, recompile the source code and repackage the APK file including the APK signature generation. The analysis of the source code and its proper modification usually remains a manual and case-by-case work.

Code injection was also previously demonstrated with other executable file formats (e.g., Windows EXE [4]).

In [7] E. Aydogen and S. Sen generate repackaged (obfuscated) APK files using *apktool*. The resulting APK files are used to evaluate the performance of antivirus systems.

A DroidChameleon framework presented in [23] is a tool for generating malwared versions of the Android applications with use of transformation techniques, repackaging and reassembling APKs. They tested common antivirus products and commercial antimalware applications with modified APKs. All APK modifications are offline, the paper does not discuss on-the-fly APK manipulations.

ADAM [31] is another malware generator framework that uses repackaging and obfuscation to generate new malware samples to stress antivirus products. The paper focuses only on an offline APK repackaging.

In [18] J. Jeon et al. intruduces Dr. Android and Mr. Hide. Dr. Android is a tool that removes application permissions and replaces them with calls of fine-grade variants accesible through Mr. Hide (a set of Android services). Dr. Android is based on the *apktool* (to repackage the application) and *redexer* (to transform the Dalvik bytecode).

AppSpear [28] is rebuilding packed and protected applications into normal form so that they can be analyzed by standard tools.

APK files are often decompiled to analyze the behaviour of applications. In [13] W. Enck et al. presented the *ded* tool for decompiling Android DEX code to the Java source codes and carried a static code analysis on 1100 Android applications with the Fortify tool. In [8] L. Batyuk et al. statically analyze the bytecode and produce precise security reports. P. Bertholome et al. [9] extend the work and not only reports the situations where the user's privacy can be disclose, but also inject a new code to allow use to decide whether he want to prevent the operation.

Many Android vulnerabilities have been published in the past few years, but APK related vulnerabilities are not that numerous. The most serious bug on this topic is the so-called Android Master Key vulnerability [16] affecting APK installation in such a way that the tampered package is accepted as a valid one. The vulnerability is based on the fact that the APK file, having the ZIP structure, can contain multiple entries of the same name, this is quite unusual, but generally allowed in ZIP files. The existence of such duplicates is not explicitly checked by the installer. The APK installer and the signature verifier are separate components, each using a different third-party ZIP parsing library.

The core problem is that the signature verifier takes into consideration the first ZIP file entry while the installer takes the last one. Exploiting this vulnerability is straightforward. Taking an original APK file, it is sufficient to insert infected files as second ZIP entries with duplicate names. As a result, the original ZIP entries are verified while the infected files are being installed. The Android Master Key vulnerability is a serious bug that has been fixed in the Android version 4.3 (Jelly Bean).

The Android Master Key vulnerability is an effective way to infect an APK file. The core advantage of this approach is based on the fact that no modification of the original signature is required (even if the installed content has actually changed). Our approach is also based on the fact that APK file has a ZIP structure but we are not using the Android Master Key vulnerability, instead we are generating a new signature as we are changing some files inside the APK.

III. OFFLINE APK MODIFICATION

Android applications are distributed in the form of APK [2] files. APK has internally a ZIP structure that includes primarily

the following elements:

- *Manifest:* Metadata including versions, permissions and bindings (file `AndroidManifest.xml`);
- *Compiled portable code:* Java classes in DEX format (file `classes.dex`);
- *Compiled native code:* Platform dependent compiled code – separate folders for particular platforms (folder `lib` and its subfolders);
- *Precompiled resources:* For example compiled XML files (file `resources.arsc`);
- *Other resources:* Images, icons, sounds, etc. (folders `res` and `assests`);
- *Package integrity data:* The digital signature (folder `META-INF`).

In the offline APK modification we automate the use of commonly available Java tools to decompose the APK file, modify the package content and build the APK again.

In the very first step, we call the *apktool* to decompile the package. This leads to unzipping of the file structure, conversion of binary XML files to textual formats (including the `AndrodManifest.xml` file) and disassembly of the `classes.dex` file (containing all compiled Java classes) into the so-called *smali* files (textual versions of the Dalvik bytecode).

The *apktool* provides a good compatibility for the APK manipulation, but there are some packages that fail to decompile with *apktool*. This basically sets the success rate of the attacks. Particular numbers depend significantly on the source of the database of APK files and also on the version of the *apktool*. In a database of 500 APKs downloaded from the zippyshare.com about 15% of the APK files fail to decompile with the *apktool*.

The next step of the offline attack is the smali files modification. In this phase we use the pre-prepared smali code we would like to inject. Those are added to other disassembled smali files. Usually we also need to modify the existing smali files in order to start the malicious code automatically after the application startup, to provide binding to the original code or to register to system events. Smali file modification is straightforward and also automated. In our scenario we tested starting a new service and registering for interesting intents (e.g., *ACTION_BOOT_COMPLETED, SMS_RECEIVED*). The new functionality (the new service) is separate from the original code and there is no aim to actually modify the original functionality, so chances of unintended interactions/malfunctions are very low. We particularly need to avoid naming collisions.

The `AndroidManifest.xml` has to be modified in the following cases: a) our code needs permissions missing in the original application, then we add the required permissions; b) new service/activity/IntentReceiver is added, it has to be registered in `AndroidManifest.xml`. Once the modification is finished, the assembly process takes place to create a tampered APK. This includes calling the *apktool* to compile the `AndroidManifest.xml` and smali files. Then the whole package is signed with a newly generated asymmetric key using the *jarsigner* utility. An optional step is to use the *zipalign* utility that aligns zip entries at 4B boundaries. The result of this process is a tampered APK file with the injected code, still correctly signed with a new certificate and private key.

IV. ONLINE APK MODIFICATION

The previous approach works well in cases where the attacker has got a big repository of APK files available so they can be infected and then provided to users. A more universal approach is to build a proxy server that modifies on-the-fly the APKs being downloaded in order not to raise any suspicion of users about the potential malicious activities being performed on the APK file during the download process.

The online attack works in the streaming mode. Thus the APK file being downloaded is read by our proxy and on the other end the proxy produces an infected APK file. The main idea of this process is the re-ordering of files inside the APK ZIP file structure.

Usually there is no need to modify resource files in the APK and typically the resource files occupy a non-negligible amount of space in the APK. We use this fact to create an impression of continuous download. Files that have to be modified (e.g., `AndroidManifest.xml`, `classes.dex`, digital signature files) are stored sideways, postponed from being sent to the user. The rest of the files (e.g., resources) are sent to the user directly. We use a stream ZIP parser to perform this task.

A. Attack launch

Once the whole APK file is available at the proxy side, the offline attack is launched on to the downloaded APK file. Note that the user has downloaded only files that are not modified during the attack and does not have the complete APK file yet. From the user's perspective, the download process is still in progress. When the offline attack finishes, the tampered APK file is analyzed and files differing from the original APK file are transmitted to the user. This would normally lead to a download pattern where a significant part of the APK file is downloaded with a normal speed, then the connection hangs for a moment (ranging from seconds to minutes), and then the download continues with the normal speed again.

To avoid a visible delay in the middle of the download process, it is possible to artificially reduce the download speed from the beginning so that the delay in the middle is not present or minimized.

The main benefit of this approach is that download on the user side starts quite quickly (i.e., the download progress bar shows the download has really started). The naïve strategy would be to use the offline attack on the proxy side and once the attack finishes the whole infected APK file would be dumped to the user's download stream. Yet that could raise suspicion of users since the modification takes some time — from a few seconds to a few minutes — the user would see 0% at the progress bar for a significant time. This could indicate connectivity problems or indications of malicious modifications. A cautious user might tend to cancel the APK download.

B. File size issue

There are two major ways of transfer encoding using HTTP as the download protocol. The server can use either the chunked encoding or the normal mode. In the chunked encoding, the overall content length of the payload is not sent to the user in the HTTP headers. This mode of transport enables to generate the content dynamically or support scenarios where the content length is not known to the server at the beginning. The downside of this approach is the missing progress illustration of the download. The other option is to use the normal transfer encoding with the content length header present among the HTTP headers.

Since we want to mimic the normal file download with the progress displayed to the user, we need to use the latter option. The problem is that the APK modification inflates the APK file by some amount of data, from bytes to kilobytes. Since estimation of the difference of the file sizes is not reliable, we cannot tell the resulting APK file size precisely before the APK tampering takes place.

Our approach is to estimate the resulting APK size by adding some extra space as a reserve. It should hold that real APK size is smaller than the APK size sent in headers, otherwise the user receives an incomplete and thus invalid APK file. Then we have additional bytes of data that need to be added to the APK somehow. Each ZIP file entry has an *Extra field* according to the ZIP standard [21]. This Extra field is of a variable size, taking at most 65535 B. It serves for storing a special application/platform information in a ZIP file and provides extensibility to the ZIP format. In most APK files it is usually unused. This is the place where we put additional bytes to obtain a "padded" version of the APK file where file size matches the one sent in the beginning of the transfer.

Padding is done once the APK tampering has been finished on the server side and the size of padding bytes is calculated. In this phase of the attack we have the list of files that need to be sent to the victim. The padding bytes are spread across the extra fields of this file entries and sent to the user. As the ZIP structure itself is not a subject of the signature the padding or the order of files in the ZIP does not affect the sigature of the package.

V. TECHNICAL DETAILS

The offline attack as described above was implemented in Java. The attacker has to prepare the code to be injected. The code being injected needs to be expressed in the smali language, but an attacker can prepare the malware code in Java, compile it (using standard development tools) and decompile it (using the *apktool*) to obtain the needed smali code. This needs to be done only once and the same malware smali code can be injected into many APK files.

The offline attack wraps the whole process of decompression, decompilation, injection, compilation, signature and compression. The process is a simple sequence of a few steps heavily using the standard *apktool* utility, thus providing good compatibility with APK files of various types. The disadvantages of the utility include the complexity (of what it is doing in a single command) and therefore also relatively slow speed.

The online attack was also implemented in order to demonstrate its applicability. Please note that it works only for HTTP, not for HTTPS. In our setup we have used a dedicated proxy server (a Fedora Linux box[1]) with two network interfaces. `Interface 1` is an Ethernet type connected to the Internet. `Interface 2` is a WiFi card for a hotspot emulation. We have chosen the *hostap*[2] software that emulates a wireless access point on this interface.

The hostap is connected to the *TinyProxy*[3], which is an open-source lightweight transparent proxy. We modified the source code of the TinyProxy to hook all `HTTP GET` requests for files with the APK extension. If an APK is being downloaded, it invokes the Java implementation of the online attack and passes the download stream to its standard input while sending its standard output to the user. TinyProxy also estimates the final file size of the APK after modification by adding a fixed amount of bytes to the total size.

The online attack application is written in Java, using the ZIP stream parser from the *Apache Commons*[4] Library. It implements the attack described earlier, together with a simple download speed limit algorithm.

Our testbed implementation is placed into public domain under the Apache License v2 hosted on GitHub: `https://github.com/ph4r05/ZIPStream`.

VI. EXPERIMENTAL VALIDATION

In order to validate our approach, we tested our setup with a dozen of real APK files on real smartphones (Samsung Galaxy S3, HTC One X, Samsung Galaxy S2 mini, Motorola Moto G and Sony XPeria Z2) with Android of versions 2.3.7, 4.2.2, 4.3, 4.4.4 and 5.0.2. The principles of the APK file modification are independent on the Android version and do not depend on a particular vulnerability of the OS. As long as the signature of the APK file can be made by any signer, the attack will basically work. All tested APK files worked on all tested phones.

As the repackaging itself is automated, it is easy to perform in a larger scale. We repackaged over 100 of APK files. On other hand, installation, running and verification that the original functionality of the APK was not affected is a manual work. We tested that on few dozens of applications.

Our tests aim to show the times needed to download sample APK files. We performed these tests with our transparent proxy server connected to a fast local network with the web server. The download of the original file that was not intervened by the proxy server was very fast. When the file was modified on-the-fly on the server then the modification needed a non-trivial amount of time and the download took significantly more time (and the file being downloaded was larger). The on-the-fly modification suffers from a well visible signature of the download process when the download practically stops for a long moment. Our solution to this problem is based on

[1]The basic hardware configuration was intentionally chosen as a low performance (router-like) computer: Intel Pentium 4 CPU 3GHz Dual Core, 2GB RAM, 7200 RPM SATA hard disk.

[2]http://wireless.kernel.org/en/users/Documentation/hostapd

[3]https://banu.com/tinyproxy/

[4]https://commons.apache.org/

APK file	Original size	New size	Time (orig. file)	Time (modified file)	Time (modif'd file with speed lim.)
Navigation utility ('C')	293 kB	793 kB	1 s	13 s	51 s
Game ('F')	4126 kB	4626 kB	2 s	19 s	53 s
Antivirus solution ('E')	3523 kB	4023 kB	2 s	31 s	62 s

TABLE I
THE TIME STATISTICS OF THE DOWNLOAD PROCESS OF THREE TYPES OF APPLICATIONS.

slowing down the user download speed from the beginning so that the on-the-fly modification can be masked by a slow link behavior.

Table I illustrates the times needed to download our sample APK files (injecting a sample privacy-related malicious code):

- File 'C' is a very basic navigation utility.
- File 'F' is a basic game with rich graphics and a simple logic.
- File 'E' is a leading provider's antivirus solution with a complex code.

These three files represent various characteristics of applications, in particular the size of the application and the proportion of the code and resources. Note that the sizes of files 'E' and 'F' are similar, but the processing times of the files differ significantly. We need to emphasize that the most time consuming part of this effort is the DEX file processing. The more Java code (the larger the `classes.dex` file) the longer the package processing takes as the decompilation and compilation of the Java/smali code is more complex than processing of other files (e.g., images and other resources). This explains the longer processing time of the file 'E', which contains more Java code than file 'F'.

Our tests were performed using a very low performance computer to imitate single purpose devices acting as routers or access points (e.g., Linux based APs). A more powerful computer can perform better. E.g., we ran some of the tests on a notebook based on Intel Core i7-3540 (3GHz) and an SSD disc – such a setting can reduce the modification times by about one half.

The speed limitation needs to estimate the ideal speed that can be achieved constantly. The time needed to process the package depends on the proportion of the files that need not be modified (and can be therefore sent directly) and files that will be (potentially) modified (and will be sent after the package modification and resigning). The speed also depends on the size of the Java code that significantly influences the decompilation and compilation times. Setting the compression level may introduce another dimension to choose between the compression level and slowdown in the modification/transfer speed.

Figure 2 demonstrates one of the performed tests. It represents the download process of the file 'F' in three tested situations. The green (solid) graph line shows the download without the proxy, the red (dotted) line shows the download process when the proxy modifies the file, and the yellow (dashed) line shows the download process with a modified file and with the speed limitation enabled. Note that the file size of the modified file is about 500 kB bigger (the injected code is accessing local resources/data and transmitting them to a remote server).

Our speed estimate is conservative and is suitable also for packages with a larger amount of Java code (like the file 'E'). Looking at Figure 2, it is possible to conclude that in this particular case the download speed could be faster and the download would still not suffer from the download stall in the middle.

VII. POSSIBLE COUNTERMEASURES

The simplest countermeasure is to use the SSL/TLS to protect the communication (e.g., the HTTPS protocol). The security issues of SSL/TLS (including possible attacks) are out of the scope of this paper.

Requesting permissions at run time in newer versions of Android may reveal undesired hidden functionality of an application, but only if that feature is active and the user pays attention to the popping up messages.

The application can check the signing certificate at runtime (so called certificate pinning) [3]. An attacker could modify the reference certificate during the repackaging attack, but doing so automatically would assume a particular process of the certificate verification in the application.

Y. Zhauniarovich et al. [29] are suggesting the use of a secondary signature of the APK file that would be added by the application store. This method requires a trusted certificate of the store to be available in the Android before the application installation.

M. Conti et al. introduce OASIS [11], a trusted component processing sensitive data on behalf of applications. Applications cannot access data directly, but only via a handle. Therefore the OASIS system can enforce complex policies like allowing access to contacts to display them but prohibiting sending contacts over the Internet (even if Internet access is generally allowed).

Increasingly popular are anti-decompilation, anti-cracking and anti-reverse-engineering mechanisms. These can be as simple as calling one particular method in the Java code (e.g., [27]) or more complex (e.g., [22], [28]).

A detection that the APK file was modified and repackaged can be based on multiple principles. A significant effort has been spent to detect repackaged APK files in Android markets. In these cases researchers and providers have a large number of APK files and analyze their statistical properties, e.g.,

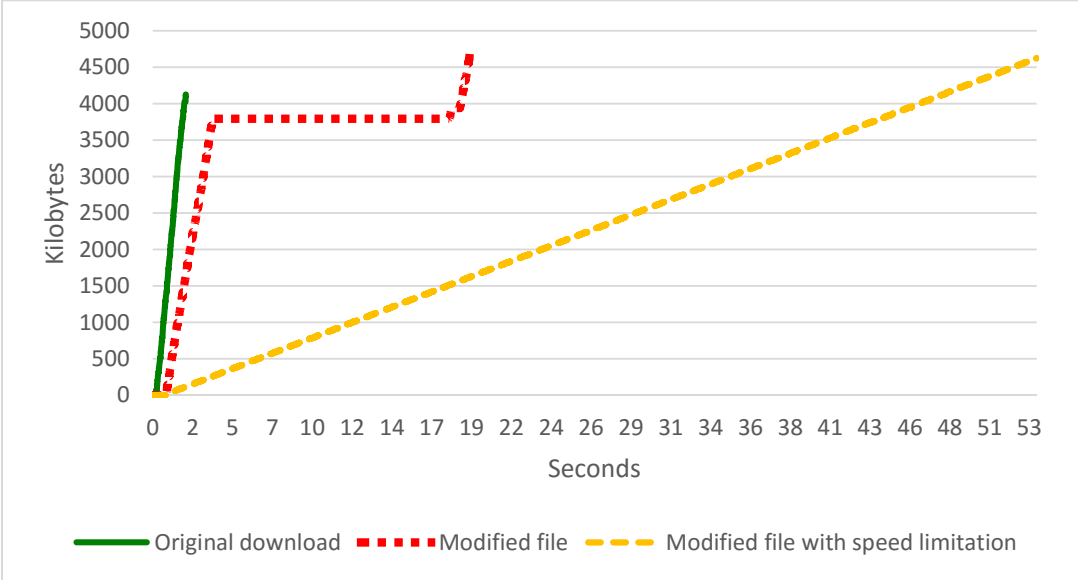

Fig. 2. The download process of a sample APK file (the game 'F'). The solid green line shows the download without the proxy, the dotted red line shows the download process when the proxy does modify the file and the yellow dashed line shows the download process with a modified file and with the speed limitation enabled.

similarity between code (including the dependency graphs between method) and resources (typically images) in packages [32], [19], [12], [30], [24], [17], [10]. The online on-the-fly attack is modifying the APK file during a particular download of a user. Focusing on the markets or file repositories does not solve the problem.

At the side of the Android device the detection can benefit from the changes the attacker has to do in the APK file. During the attack some Java code is added, the Android manifest is modified and the signature is updated with a new private key and certificate. The injected code depends strongly on the attacker and her aims. The attacker has to balance the power of the code and its detectability. The more power of the injected code the bigger is the size of the new code, the more hooks appear in the Android Manifest and the more permissions are required in the Android Manifest. Permission-based malware detection is common these days [26]. Therefore, requiring too many powerfull permissions can lead to a quick detection of an antivirus solution.

In targeted attacks, the attackers do not usually need excessive permissions and rely on commonly used permissions to get access to personal data (e.g., READ_SMS). The code is tailor-made and therefore signature based detection using known malware signature databases is not of a significant help.

In our experiment, we coded two variants of the additional functionality[5]. The first was a simple "Hello World" text appearing from time to time on the screen. The second was a realistic privacy attack collecting messages, contacts and call logs, and transmitting these to a web server located in the Internet. We tested both variants with three leading antivirus solutions and no alert was raised during our tests.

Kirin [14] is a mobile application certification service used during application installation to check for potentially dangerous combinations of permissions.

The detection techniques can also focus on the signer. If the application is new, then the signer cannot be matched with the previous one as is the case of an application update. Basically all signers are equal and the operating system itself has difficulties deciding where a particular application should be signed by a particular signer or not. A reputation system of the signers (or of the APK files) can help [20]. The rarer is the signer or the APK the more suspicious the application is. This technique requires a community support, but is already used in some common PC-based antivirus or firewall solutions.

In our implementation of the online on-the-fly attack we estimate the total new size of the file and then pad the file with zeros in the ZIP extra fields to match exactly the estimated file size. The extra fields are used also in normal APK files. The *zipalign* utility (a part of the Android Developer Tools) aligns all uncompressed data in the APK file on 4-byte boundaries by changing the size of the extra fields. After applying the *zipalign* utility the extra fields occupy single bytes, our implementation is currently adding extra fields in the order of 10 kB. This can lead to an easy detection. Once this feature leads to detections a more accurate estimation of the new file size would be needed.

VIII. CONCLUSION

In this paper, we practically demonstrated new fully automated offline and on-the-fly attacks on the Android APK for

[5]These codes are not available for download.

an arbitrary APK provided at the time of the attack. Without seeing a particular APK file before, we are able to inject a prepared code to the application and infect it this way. The practicality of this attack was demonstrated with a transparent HTTP proxy in the middle performing an APK tampering on-the-fly for all HTTP downloaded APK files.

IX. ACKNOWLEDGEMENTS

The authors thank to the anonymous reviewers for their comments. Vashek Matyáš was partly supported by the Czech Science Foundation project GBP202/12/G061.

REFERENCES

[1] Inserting keylogger code in Android SwiftKey using apktool. Online [Accessed Dec 14, 2016], Mar 2013. http://www.android-app-development.ie/blog/2013/03/06/inserting-keylogger-code-in-android-swiftkey-using-apktool/.

[2] Android Developers Reference. Online [Accessed Dec 14, 2016], 2015. http://developer.android.com/guide/developing.

[3] Retrieve the apk signature at runtime for Android. Online [Accessed Dec 14, 2016], Jun 2015. http://stackoverflow.com/questions/8682731/retrieve-the-apk-signature-at-runtime-for-android.

[4] Backdooring EXE Files. Online [Accessed Dec 14, 2016], Dec 2016. https://www.offensive-security.com/metasploit-unleashed/backdooring-exe-files/.

[5] Smartphone OS Market Share, 2016 Q2. Online [Accessed Dec 14, 2016], Sep 2016. http://www.idc.com/prodserv/smartphone-os-market-share.jsp.

[6] D. Akhawe and A. P. Felt. Alice in warningland: A large-scale field study of browser security warning effectiveness. In *Presented as part of the 22nd USENIX Security Symposium (USENIX Security 13)*, Washington, D.C., 2013. USENIX.

[7] E. Aydogan and S. Sen. Automatic generation of mobile malwares using genetic programming. In A. M. Mora and G. Squillero, editors, *Applications of Evolutionary Computation*, volume 9028 of *Lecture Notes in Computer Science*. Springer, 2015.

[8] L. Batyuk, M. Herpich, S. A. Camtepe, K. Raddatz, A.-D. Schmidt, and S. Albayrak. Using static analysis for automatic assessment and mitigation of unwanted and malicious activities within android applications. In *Proceedings of the 2011 6th International Conference on Malicious and Unwanted Software*, MALWARE '11, Washington, DC, USA, 2011. IEEE Computer Society.

[9] P. Berthom, T. Fcherolle, N. Guilloteau, and J.-F. Lalande. Repackaging android applications for auditing access to private data. In *ARES*. IEEE Computer Society, 2012.

[10] J. Chen, M. Alalfi, T. Dean, and Y. Zou. Detecting android malware using clone detection. *Journal of Computer Science and Technology*, 30(5), 2015.

[11] M. Conti, E. Fernandes, J. Paupore, A. Prakash, and D. Simionato. Oasis: Operational access sandboxes for information security. In *Proceedings of the 4th ACM Workshop on Security and Privacy in Smartphones & Mobile Devices*, SPSM '14, New York, NY, USA, 2014. ACM.

[12] J. Crussell, C. Gibler, and H. Chen. Attack of the clones: Detecting cloned applications on android markets. In S. Foresti, M. Yung, and F. Martinelli, editors, *Computer Security ESORICS 2012*, volume 7459 of *Lecture Notes in Computer Science*. Springer Berlin Heidelberg, 2012.

[13] W. Enck, D. Octeau, P. McDaniel, and S. Chaudhuri. A study of Android application security. In *Proceedings of the 20th USENIX Conference on Security*, SEC'11, Berkeley, CA, USA, 2011. USENIX Association.

[14] W. Enck, M. Ongtang, and P. McDaniel. On lightweight mobile phone application certification. In *Proceedings of the 16th ACM Conference on Computer and Communications Security*, CCS '09, pages 235–245, New York, NY, USA, 2009. ACM.

[15] A. P. Felt, A. Ainslie, R. W. Reeder, S. Consolvo, S. Thyagaraja, A. Bettes, H. Harris, and J. Grimes. Improving SSL Warnings: Comprehension and Adherence. In *Proceedings of the Conference on Human Factors and Computing Systems*, 2015.

[16] J. Forristal. Android Master Key Exploit – Uncovering Android Master Key That Makes 99% of Devices Vulnerable. Online [Accessed Dec 14, 2016], Mar 2013. https://uwnthesis.wordpress.com/2013/07/04/uncovering-android-master-key-that-makes-99-of-devices-vulnerable/.

[17] S. Hanna, L. Huang, E. Wu, S. Li, C. Chen, and D. Song. Juxtapp: A scalable system for detecting code reuse among android applications. In U. Flegel, E. Markatos, and W. Robertson, editors, *Detection of Intrusions and Malware, and Vulnerability Assessment*, volume 7591 of *Lecture Notes in Computer Science*. Springer Berlin Heidelberg, 2013.

[18] J. Jeon, K. K. Micinski, J. A. Vaughan, A. Fogel, N. Reddy, J. S. Foster, and T. Millstein. Dr. Android and Mr. Hide: Fine-grained Permissions in Android Applications. In *ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM)*, Raleigh, NC, USA, October 2012.

[19] S. Jiao, Y. Cheng, L. Ying, P. Su, and D. Feng. A rapid and scalable method for android application repackaging detection. In J. Lopez and Y. Wu, editors, *Information Security Practice and Experience*, volume 9065 of *Lecture Notes in Computer Science*. Springer, 2015.

[20] D. Papp, B. Kcs, T. Holczer, L. Buttyn, and B. Bencsth. Rosco: Repository of signed code. In *Proceedings of the Virus Bulletin Conference*, Prague, Czech Republic, 2015.

[21] PKWARE. Zip file format specification. Technical Report version 6.3.2, PKWARE, 2007. http://www.pkware.com/documents/casestudies/APPNOTE.TXT.

[22] M. Protsenko and T. Muller. Protecting android apps against reverse engineering by the use of the native code. In S. Fischer-Hbner, C. Lambrinoudakis, and J. Lpez, editors, *Trust, Privacy and Security in Digital Business*, volume 9264 of *Lecture Notes in Computer Science*. Springer, 2015.

[23] V. Rastogi, Y. Chen, and X. Jiang. Droidchameleon: Evaluating Android anti-malware against transformation attacks. In *Proceedings of the 8th ACM SIGSAC Symposium on Information, Computer and Communications Security*, ASIA CCS '13, New York, NY, USA, 2013. ACM.

[24] X. Sun, Y. Zhongyang, Z. Xin, B. Mao, and L. Xie. Detecting code reuse in android applications using component-based control flow graph. In N. Cuppens-Boulahia, F. Cuppens, S. Jajodia, A. Abou El Kalam, and T. Sans, editors, *ICT Systems Security and Privacy Protection*, volume 428 of *IFIP Advances in Information and Communication Technology*. Springer Berlin Heidelberg, 2014.

[25] D. Taitelbaum. Hacking for fun and for profit (mostly for fun). Online [Accessed Dec 14, 2016], Dec 2012. http://www.slideshare.net/davtbaum/hacking-for-fun-and-for-profit.

[26] F. Tchakounté. Permission-based malware detection mechanisms on Android: Analysis and perspectives. *Journal of computer science and software application*, 1(2), Dec 2014.

[27] J. Xu, S. Li, and T. Zhang. Security analysis and protection based on smali injection for android applications. In X.-h. Sun, W. Qu, I. Stojmenovic, W. Zhou, Z. Li, H. Guo, G. Min, T. Yang, Y. Wu, and L. Liu, editors, *Algorithms and Architectures for Parallel Processing*, volume 8630 of *Lecture Notes in Computer Science*. Springer, 2014.

[28] W. Yang, Y. Zhang, J. Li, J. Shu, B. Li, W. Hu, and D. Gu. Appspear: Bytecode decrypting and dex reassembling for packed android malware. In H. Bos, F. Monrose, and G. Blanc, editors, *Research in Attacks, Intrusions, and Defenses*, volume 9404 of *Lecture Notes in Computer Science*. Springer, 2015.

[29] Y. Zhauniarovich, O. Gadyatskaya, and B. Crispo. DEMO: Enabling Trusted Stores for Android. In *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security*, CCS '13, 2013.

[30] Y. Zhauniarovich, O. Gadyatskaya, B. Crispo, F. La Spina, and E. Moser. Fsquadra: Fast detection of repackaged applications. In V. Atluri and G. Pernul, editors, *Data and Applications Security and Privacy XXVIII*, volume 8566 of *Lecture Notes in Computer Science*. Springer Berlin Heidelberg, 2014.

[31] M. Zheng, P. P. C. Lee, and J. C. S. Lui. ADAM: an automatic and extensible platform to stress test Android anti-virus systems. In *Detection of Intrusions and Malware, and Vulnerability Assessment - 9th International Conference, DIMVA 2012, Heraklion, Crete, Greece, July 26-27, 2012, Revised Selected Papers*, 2012.

[32] W. Zhou, Y. Zhou, X. Jiang, and P. Ning. Detecting repackaged smartphone applications in third-party Android marketplaces. In *Proceedings of the Second ACM Conference on Data and Application Security and Privacy*, CODASPY '12, New York, NY, USA, 2012. ACM.

Zdeněk Říha is teaching at the Masaryk University, Faculty of Informatics, in Brno, Czech Republic. He received his PhD degree from the Faculty of Informatics, Masaryk University. In 1999 he spent 6 months on an internship at Ubilab, the research lab of the bank UBS, focusing on security and usability aspects of biometric authentication systems. Between 2005 and 2008 he was seconded as a Detached National Expert to the European Commission's Joint Research Centre in Italy. Zdenek can be contacted at zriha AT fi.muni.cz.

Dušan Klinec is security consultant, developer and research fellow at the Centre for Research on Cryptography and Security, Masaryk University, CR. Dusan focuses on secure end-to-end communication, secure cloud solutions, cryptanalysis, whitebox cryptography and software security in general. He also participated projects focused on wireless sensor networks and cryptanalysis using genetic algorithms. Dusan received his Master degree from Masaryk University, with his Master thesis on whitebox attack resistant cryptography and graduated with honours. He was an intern at CERN where he worked on projects related to GRID computing and IPv6 compliance. He can be contacted at dusan.klinec AT gmail.com.

Václav (Vashek) Matyáš is a Professor at the Masaryk University, Brno, CZ, and Vice-Dean for Industrial and Alumni Relations, Faculty of Informatics. His research interests relate to applied cryptography and security, where he published over 150 peer-reviewed papers and articles, and co-authored several books. He was a Fulbright-Masaryk Visiting Scholar with Harvard University, Center for Research on Computation and Society in 2011-12, and previously he worked also with Microsoft Research Cambridge, University College Dublin, Ubilab at UBS AG, and was a Royal Society Postdoctoral Fellow with the Cambridge University Computer Lab. Vashek edited the Computer and Communications Security Reviews, and worked on the development of Common Criteria and with ISO/IEC JTC1 SC27. He received his PhD degree from Masaryk University, Brno and can be contacted at matyas AT fi.muni.cz.

The IEEE Region 8 flagship conference in Africa, **IEEE AFRICON**, is to be hosted in the famous V&A Waterfront in beautiful **Cape Town, South Africa**.

IEEE AFRICON 2017 provides a platform for academic and industry professionals from all over the world, to share ideas, present their latest research and to network.

The conference covers the full spectrum of IEEE activities.

Submission of papers

Prospective authors are invited to submit original technical papers in English, of up to 6 pages in IEEE conference format. Accepted and presented papers will be published in the IEEE AFRICON 2017 proceedings and submitted for inclusion in the IEEE Xplore Digital Library.

Paper submissions by: 7 April 2017

Please consult the conference website for more information and regular updates.

Themes for which papers are solicited include (but are not limited to):

- Communication and Signal Processing
- Control, Robotics and Automation
- Remote Sensing
- Electromagnetics and Antennas
- Power Electronics and Devices
- Energy and Power Systems
- Renewable Energy & Sustainable Engineering
- Mobile Computing
- Cloud Computing
- e-Health, ICT4D
- Software Engineering
- Artificial Intelligence and Cognitive Computing
- Biomedical Engineering
- Electro-optic Systems
- Nanotechnology
- Engineering management and education.

http://africon2017.org


Aquarium at the conference venue


Penguins at Boulders Beach

region8 IEEE | IEEE South Africa Section | ICS | UNIVERSITEIT VAN PRETORIA UNIVERSITY OF PRETORIA YUNIBESITHI YA PRETORIA | SAIEE

SISY 2017

IEEE 15th INTERNATIONAL SYMPOSIUM ON INTELLIGENT SYSTEMS and INFORMATICS

September 14-16, 2017
Subotica, Serbia

Organizers
Óbuda University, Budapest (Hungary)
Subotica Tech (Serbia)
IEEE SMC Technical Committee on Computational Cybernetics

Sponsors
IEEE Hungary Section
IEEE SMC Chapter (Hungary)
IEEE CI Chapter (Hungary)
IEEE IES and RAS Chapters (Hungary)

Technical Co-Sponsor
IEEE SMC Society

In Technical Co-operation with
Vojvodina Academy of Sciences and Arts (Serbia)
Ministry of Sciences and Ecology of Serbia (Serbia)
IEEE CI Chapter (Serbia)
Hungarian Fuzzy Association

Venue
The symposium will be held at Subotica Town Hall and Subotica Tech, Serbia.

Language
The official language of the symposium is English.

Submission of Papers
There are invited and regular papers. All paper submission is processed through conference website. Papers sent by e-mail are not acceptable.

Instructions for Authors
The format of the final manuscript can be found on the conference web site of SISY 2017 (http://conf.uni-obuda.hu/sisy2017).

Registration
The registration fee is EUR 300. Student and IEEE members: EUR 250.

Author's Schedule
Full paper submission: ..... May 19, 2017
Notification: ..... July 3, 2017
Final manuscript submission: ..... August 10, 2017
Sorry, but no deadline extension.

Topics
Computational Intelligence (track chair: Róbert Fullér): Machine Learning, Genetic Algorithms, Neural Nets, Fuzzy Systems, Fuzzy and Neuro-Fuzzy Control, Knowledge Based Systems, Expert Systems.

Intelligent Robotics (track chair: Branislav Borovac): Control, Flexible Arm Control, Perception and Recognition, Reasoning, Learning, Robotic Systems, Human-Robotic Interaction, Service Robots, Surgery Robots, Machine Vision.

Intelligent Mechatronics (track chair: Radu-Emil Precup): Sensing and Sensor Data Fusion, Motion Control, Intelligent Actuators.

Intelligent Manufacturing Systems (track chair: László Horváth): Flexible Manufacturing Systems, Production Planning and Scheduling, System Simulation, Rapid Prototyping, Concurrent Engineering, Virtual Reality.

Informatics (track chair: Levente Kovács): The Web, Business & Digital Culture, Databases, Design & Graphics, Digital Audio, Video and Photography, Hardware, Home & Office, Networking & Sys Admin, Operating Systems, programming, Science & Math, Security Software Engineering, Healthcare Informatics, Teaching Informatics, Informatics in education process

Applied Mathematics (track chair: Ivana Štajner-Papuga)

Honorary Chairs
C. L. Philip Chen, University of Macau
Mihály Réger, Óbuda University, Hungary
Endre Pap, Univ. of Novi Sad, Serbia
Aleksandar Rodić, Mihailo Pupin Institute, Belgrade, Serbia
Ljiljana Trajkovic, Simon Fraser Univ., Canada

General Chair
Imre J. Rudas, Óbuda University, Hungary

General Co-Chair
Branislav Borovac, Univ. of Novi Sad, Serbia

Technical Program Committee Chair
Ivana Štajner-Papuga, Univ. of Novi Sad

Technical Program Committee
Rudolf Andoga, Tech. Univ. of Košice
Bernard de Baets, Genth, Belgium
Péter Baranyi, BME, Hungary
Ivana Berković, Technical Faculty Mihajlo Pupin, Zrenjanin
József Dombi, University of Szeged
Imre Felde, Óbuda University
Ladislav Főző, Tech. Univ. of Košice
Róbert Fullér, Óbuda University, Hungary
Péter Galambos, Óbuda University
Angel Luis Garrido, Univ. of Zaragoza, Spain
Tom D. Gedeon, Murdoch University, Australia
Tamás Haidegger, Óbuda University
Ladislav Hluchý, Slovak Academy of Sciences
László Horváth, Óbuda University
Sándor Jenei, University of Pécs
Zsolt Csaba Johanyák, Kecskemét College, Hungary
Aleksandar Jovanović, Belgrade, Serbia
Duško Katić, Institute Mihajlo Pupin, Belgrade
Jozef Kelemen, Silisian University
Erich Peter Klement, Linz, Austria
Zora Konjović, Novi Sad, Serbia
Péter Korondi, BME
László Kovács, University of Miskolc
Levente Kovács, Óbuda University, Hungary
Szilveszter Kovács, University of Miskolc
Krisztián Lamár, Óbuda University
Radko Mesiar, Bratislava, Slovakia
András Molnár, Óbuda University, Budapest
László Nádai, Óbuda University, Budapest
Szilveszter Pletl, Subotica Tech, Serbia, and Univ. of Szeged, Hungary
Radu-Emil Precup, Politehnica Univ. in Timişoara
Stefan Preitl, Politehnica Univ. in Timişoara
Miloš Racković, Novi Sad, Serbia
Dragica Radosav, Technical Faculty Mihajlo Pupin, Zrenjanin
Dušan Surla, Novi Sad, Serbia
Sándor Szénási, Óbuda University, Hungary
József K. Tar, Óbuda University, Hungary
Dušan Teodorović, Belgrade, Serbia
József Tick, Óbuda University, Hungary
Domonkos Tikk, BME, Hungary

Organizing Committee Chair
Márta Takács, Óbuda University, Hungary

Organizing Committee Co-Chair
Éva Pataki, Subotica Tech, Serbia

Organizing Committee
Gizella Csikós-Pajor, Subotica Tech
József Gáti, Óbuda University
Franciska Hegyesi, Óbuda University
Gyula Kártyás, Óbuda University
Krisztina Némethy, Óbuda University
Anita Szabó, Subotica Tech
Lívia Szedmina, Subotica Tech

Secretary General
Anikó Szakál
Óbuda University, Budapest, Hungary
E-mail: szakal@uni-obuda.hu

http://conf.uni-obuda.hu/sisy2017

Call for Papers

Special Session on Urban Mobility – Communication Technologies and Safety for Autonomous Vehicles

(part of the 14th International Conference on Telecommunications, Zagreb, Croatia, June 2017)

Background and scope:

There is a growing importance of ICT in profiling the competitiveness of cities. The next step for the smart city is the *automated city* – one that is predictive and responsive without human intervention. Such a city could avoid traffic congestion before it occurs and distribute resources, such as emergency services and maintenance, without time-consuming human decision-making. Communicating vehicles form an essential part of this vision. The success of the first generation large-scale V2X testbeds and the planned followers, manufacturers/policy maker activities, and the maturing standards of cooperative intelligent transport systems (C-ITS) predict the inevitable and quick proliferation of vehicular networks in urban environments. Urban mobility applications will also rely on collecting available information from sensor networks in and around the city and make the operation of public services (like lighting, heating, garbage collection, etc.) intelligent. This will be based partially on crowdsensing, especially in densely populated areas where insuring the appropriate number of sensing users is easier. Public safety is another category of applications where the power of the crowd is used to indicate unusual/abnormal behaviour of people, extreme situations like riots, demonstrations and similar. In this Special Session we will catch up with the latest research and product developments, measurement methods, application scenarios and concept studies related to urban mobility supporting technologies.

Topics of interest include:

Novel protocols and techniques for V2X communication (radio resource management, mobility management, data dissemination, etc.); Heterogeneous Vehicular Networking approaches; Connected vehicle technologies in 4G and beyond; V2X applications and services for enhanced driver experience, increased transportation efficency, decreased emission, enhanced road safety, etc.; Network management, deployment support and QoS provisioning for V2X architectures; Sensor fusion in vehicular networks; Cross-layer design and optimization for V2X communication infrastructures; Mobile crowdsourcing for urban analytics; Mobile crowdsourcing applications; ICT in road vehicles: on-board and connected car services; New proof-of-concept cyber attacks against modern vehicles; Attack surfaces and risk analysis for autonomous vehicles; Security testing methods and testbeds for autonomous vehicles; Security countermeasures against cyber attacks for autonomous vehicles; Software vulnerability management and security patching for autonomous vehicles; Security of sensor data collection and processing in autonomous vehicles; Digital forensic requirements and solutions for autonomous vehicles; Privacy issues induced and solutions required by autonomous vehicles; Cryptographic algorithms and protocols for protecting vehicle communications

Publication of accepted papers:

Prospective authors are invited to submit novel, previously unpublished full papers (up to 8 pages), addressing the topics of interest, for consideration for the special session. Accepted and presented papers will be published in the conference proceedings and submitted to IEEE Xplore. Authors of best papers will be invited to submit a sufficiently extended version of their conference paper for potential publication in the Infocommunications Journal (www.infocommunications.hu) Special Issue on Smart Cities.

More information is available at http://www.contel.hr/2017/special-session-urban-mobility/

General Co-Chairs
Deepak Uttamchandani
University of Strathclyde, Scotland, UK
Krikor Ozanyan
University of Manchester, UK

Technical Program Co-Chairs
Ravinder Dahiya
University of Glasgow, Scotland, UK
Srinivas Tadigadapa
The Pennsylvania State University, USA

PCO
Conference Catalysts, LLC

Paper Submission Service
Epapers

Conference Email Contact
Chris Dyer
cdyer@ConferenceCatalysts.com

Important Dates

Proposals for Tutorials
May 21, 2017

Proposal for Focused Sessions
May 21, 2017

3-Page Paper Submission Deadline
June 18, 2017

Notification of Paper Acceptance
August 10, 2017

Submission of Final Papers
August 31, 2017

IEEE
IEEE Sensors Council

ANNOUNCEMENT & CALL FOR PAPERS

IEEE SENSORS 2017 is intended to provide a forum for research scientists, engineers, and practitioners throughout the world to present their latest research findings, ideas, and applications in the area of sensors and sensing technology.

IEEE SENSORS 2017 will include keynote addresses and invited presentations by eminent scientists and engineers. The conference solicits original state-of-the-art contributions as well as review papers.

Topics of Interest

- Sensor Phenomenonology, Modeling, and Evaluation
- Sensor Materials, Processing, and Fabrication
- Chemical and Gas Sensors
- Microfluidics and Biosensors
- Optical Sensors
- Physical Sensors: Temperature, Mechanical, Magnetic, and others
- Acoustic and Ultrasonic Sensors
- Sensor Packaging
- Sensor Networks
- Sensor Applications
- Sensor Systems: Signals, Processing, and Interfaces
- Actuators and Sensor Power Systems
- Demos
- Sensors In Industrial Practice

Focused Sessions

IEEE SENSORS 2017 will have focused sessions on emerging sensor-related topics. Details related to the Call For Focused Sessions is on the conference website.

Publication of Papers

Presented papers will be included in the Proceedings of IEEE SENSORS 2017 and in IEEE Xplore pending author requirements being met. Authors may submit extended versions of their paper to the IEEE Sensors Journal.

Exhibition & Demo Opportunities

The Conference exhibit area will provide your company or organization with the opportunity to inform and display your latest products, services, equipment, books, journals, and publications to attendees from around the world.

For further information, contact Chris Dyer, cdyer@conferencecatalysts.com

Industry Day

A special track designed to encourage industry participation will include industry showcase/demonstrations, industry networking, and an industry panel luncheon. Special flexible one-day registration will be available to facilitate industry participation.

Visit the website for the most up to date information relating to abstract submission, tutorials, and special sessions information and deadlines.

ieee-sensors2017.org

IEEE GLOBECOM™

IEEE Global Communications Conference
4-8 December 2017 // Singapore
Global Hub: Connecting East and West
CALL FOR PAPERS

IEEE
IEEE ComSoc
IEEE Communications Society

The 2017 IEEE Global Communications Conference (GLOBECOM) will feature a comprehensive technical program including 13 symposia, tutorials, workshops and an industrial program featuring prominent keynote speakers, technology and industry forums and vendor exhibits.

TECHNICAL SYMPOSIA

- Ad Hoc and Sensor Networks
- Cognitive Radio and Networks
- Communication and Information System Security
- Communication QoS, Reliability and Modeling
- Communication Software, Services and Multimedia Applications
- Communication Theory
- Green Communications Systems and Networks
- Mobile and Wireless Networks
- Next-Generation Networking and Internet
- Optical Networks and Systems
- Signal Processing for Communications
- Wireless Communication
- Selected Areas in Communications
  - Access Networks and Systems
  - Big Data
  - Cloud Networks
  - Data Storage
  - e-Health
  - Internet of Things
  - Molecular, Biological, and Multi-scale Communication
  - Power Line Communications
  - Satellite and Space Communications
  - Smart Grid Communications
  - Social Networks

Please address questions regarding the Technical Symposia to Technical Program Committee (TPC) Chair: Ying-Chang Liang (liangyc@ieee.org), and TPC Co-Chairs: Teng Joon Lim (eleltj@nus.edu.sg) and Chengshan Xiao (xiaoc@mst.edu).

Accepted and presented technical and workshop papers will be published in the IEEE GLOBECOM 2017 Conference Proceedings and submitted to IEEE Xplore®. See the website for author requirements of accepted authors. Full details of submission procedures are available at www.ieee-globecom.org.

TUTORIALS
Proposals are invited for half-day tutorials in communications & networking. Please address questions regarding tutorials to Tutorial Chair: Rui Zhang (elezhang@nus.edu.sg).

WORKSHOPS
Submissions are sought for workshops on the latest technical and business issues in communications and networking. Please address questions on workshops to Workshop Chair: Tony Quek (tonyquek@sutd.edu.sg).

IMPORTANT DATES	Symposia Papers	Workshop Proposals	Tutorial Proposals
	1 April 2017	15 February 2017	15 March 2017

For more information about IEEE GLOBECOM 2017, visit www.ieee-globecom.org.

ORGANIZING COMMITTEE

General Chair
Dim-Lee Kwong
(I2R, Singapore)

General Vice Chairs
Shiang Long Lee
(Singapore Technologies, Singapore)
Pak Lum Mock
(Starhub, Singapore)

Executive Chair
Lawrence Wong (NUS, Singapore)

Executive Vice Chairs
Ying-Chang Liang
(UESTC, China & I2R, Singapore)
Sumei Sun (I2R, Singapore)

TPC Chair
Ying-Chang Liang
(UESTC, China & I2R, Singapore)

TPC Co-Chairs
Teng Joon Lim (NUS, Singapore)
Chengshan Xiao
(Missouri S&T, USA)

Tutorial Chair
Rui Zhang (NUS, Singapore)

Tutorial Co-Chairs
Lingyang Song (PKU, China)
Stefano Bregni
(Politecnico Milano, Italy)

Workshop Chair
Tony Quek (SUTD, Singapore)

Workshop Co-Chairs
Wei Zhang (UNSW, Australia)
Gang Wu (UESTC, China)

Guidelines for our Authors

Format of the manuscripts

Original manuscripts and final versions of papers should be submitted in IEEE format according to the formatting instructions available on
http://www.ieee.org/publications_standards/publications/authors/authors_journals.html#sect2,
"Template and Instructions on How to Create Your Paper".

Length of the manuscripts

The length of papers in the aforementioned format should be 6-8 journal pages.
Wherever appropriate, include 1-2 figures or tables per journal page.

Paper structure

Papers should follow the standard structure, consisting of *Introduction* (the part of paper numbered by "1"), and *Conclusion* (the last numbered part) and several *Sections* in between.
The Introduction should introduce the topic, tell why the subject of the paper is important, summarize the state of the art with references to existing works and underline the main innovative results of the paper. The Introduction should conclude with outlining the structure of the paper.

Accompanying parts

Papers should be accompanied by an *Abstract* and a few *index terms (Keywords)*. For the final version of accepted papers, please send the *short cvs* and *photos* of the authors as well.

Authors

In the title of the paper, authors are listed in the order given in the submitted manuscript. Their full affiliations and e-mail addresses will be given in a footnote on the first page as shown in the template. No degrees or other titles of the authors are given. Memberships of IEEE, HTE and other professional societies will be indicated so please supply this information. When submitting the manuscript, one of the authors should be indicated as corresponding author providing his/her postal address, fax number and telephone number for eventual correspondence and communication with the Editorial Board.

References

References should be listed at the end of the paper in the IEEE format, see below:

a) Last name of author or authors and first name or initials, or name of organization
b) Title of article in quotation marks
c) Title of periodical in full and set in italics
d) Volume, number, and, if available, part
e) First and last pages of article
f) Date of issue

[11] Boggs, S.A. and Fujimoto, N., "Techniques and instrumentation for measurement of transients in gas-insulated switchgear," IEEE Transactions on Electrical Installation, vol. ET-19, no. 2, pp.87–92, April 1984.

Format of a book reference:

[26] Peck, R.B., Hanson, W.E., and Thornburn, T.H., Foundation Engineering, 2nd ed. New York: McGraw-Hill, 1972, pp.230–292.

All references should be referred by the corresponding numbers in the text.

Figures

Figures should be black-and-white, clear, and drawn by the authors. Do not use figures or pictures downloaded from the Internet. Figures and pictures should be submitted also as separate files. Captions are obligatory. Within the text, references should be made by figure numbers, e.g. "see Fig. 2."
When using figures from other printed materials, exact references and note on copyright should be included. Obtaining the copyright is the responsibility of authors.

Contact address

Authors are requested to submit their papers electronically via the EasyChair system. The link for submission can be found on the journal's website:
www.infocommunications.hu/for-our-authors

If you have any question about the journal or the submission process, please do not hesitate to contact us via e-mail:

Rolland Vida – Editor-in-Chief:
vida@tmit.bme.hu

Árpád Huszák – Associate Editor-in-Chief:
huszak@hit.bme.hu

IEEE pimrc'17

28th Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications
08-13 OCTOBER 2017 // MONTREAL, QUEBEC, CANADA

Perswade | IEEE ComSoc IEEE Communications Society | IEEE

SPECIAL CELEBRATION-YEAR EDITION! | FIRST CALL FOR PAPERS | www.pimrc2017.org

IEEE PIMRC 2017 will be held at the Bonaventure Hotel, Montreal, QC, Canada, from October 8th to 13th, 2017, under the theme "Engaged Citizens and their New Smart Worlds". Montreal is a vibrant multicultural, multilingual and welcoming city that offers visitors a unique and well-blended taste of Europe in North America. "Autumn is a second spring when every leaf is a lower", said Albert Camus. And there is no better city and time to experience it than Montreal during its fall foliage season peak in early to mid-October. Leafs and flowers are iconic symbols of Montreal, Quebec, and Canada. And 2017, a milestone celebration year, marks the 375th anniversary of Montreal's founding, the 150th anniversary of Canada's confederation, and the 50th anniversary of the 1967 World's Fair. Expo 67 was held in Montreal under the theme "Man and His World", based on Saint-Exupéry's book "Terre des Hommes" so filled with dreams and hopes for the future. Fifty years later, inspired by the same phrase found by Saint- Exupéry to express the human need for lessening isolation and for solidarity, IEEE PIMRC 2017 invites all creators of new wireless techs & apps to reflect upon it to see how it could be given tangible form by properly connecting everything wirelessly in the new smart world of sustainable economies and digital societies.

General Chair
- Sofiène Affes, INRS, Canada

TPC Co-Chairs
- Kaibin Huang, HKU, Hong Kong
- Geert Leus, TU Delft, Netherlands
- Shahrokh Valaee, UoT, Canada

Finance Chair
- Abdelaziz Samet, INRS, Canada

Local-Arrangements Co-Chairs
- Tarek Djerafi, INRS, Canada
- Serge Tatu, INRS, Canada

Awards Chair
- Vijay Bhargava, UBC, Canada

Tutorials Co-Chairs
- David Gesbert, EURECOM, France
- Stefan Parkvall, Ericsson, Sweden

Panels Co-Chairs
- Benoît Pelletier, InterDigital, Canada
- Tarik Taleb, Aalto Univ., Finla

Demos & Exhibitions Chair
Peng Hu, Seneca, Canada

Keynotes Chair
- Lajos Hanzo, Univ. Southampton

Workshops Co-Chairs
- Wei Yu, UoT, Canada
- Peiying Zhu, Huawei, Canada

Special-Sessions Co-Chairs
- Mohamed Ibnkahla, Carleton, Canada
- Xianbin Wang, UWO, Canada

Patronage Chair
- TBA

Publicity Co-Chairs
- Octavia Dobre, MUN, Canada
- Roch Glitho, Concordia Univ., Canada
- Lutz Lampe, UBC, Canada
- Yifeng Zhou, CRC, Canada

International Advisors
- Slim Alouini, KAUST, Saudi Arabia (Middle East & Africa)
- Khaled Ben Letaief, HKUST, Hong Kong, and HBKU, Qatar (Asia & Pacific)
- Robert Heath, Univ. Texas Dallas, USA (Americas)
- Robert Schober, Erlangen-Nüremberg, Germany (Europe)

Prospective authors are invited to submit technical papers of their previously unpublished work. Topics of interest include, but are not limited to:

Track 1: Fundamentals and PHY
- Advanced modulation schemes for 5G, IoT, ...
- Antennas and beamforming
- Channel estimation and equalization
- Channel modeling and simulation
- Cognitive and green radio
- Cooperative/relayed communications
- Energy harvesting , wireless power transfer
- Interference characterization & mitigation
- Microwave/DSP circuits and devices
- Multi-antenna signal processing
- PHY aspects of WLAN, WPAN, and WBAN
- PHY performance: capacity, outage, BER
- PHY network coding and security
- Positioning, localization, and tracking
- Power-efficient communications
- Propagation: mmW, Terahertz, light-wave
- Signal processing for wireless
- Single and multi-user MIMO
- Source and channel coding
- Synchronization techniques
- Vehicular communications
- Wireless broadband for 5G, IoT, ...

Track 2: MAC & Cross-Layer Design
- Adaptive MACs
- Cognitive MACs
- Cross-layer designs involving MAC
- Delay-tolerant MAC designs
- Docitive MACs
- Implementation, test-beds & prototypes
- Information-theoretical approaches to MAC designs
- Joint access-backhaul scheduler designs
- Joint MAC and networking layer designs
- MAC for low-power embedded networks
- MAC for MANETs/VANETs
- QoS/QoE-enabling MAC & future mobile networks
- Radio resource management, allocation, and scheduling
- Reconfigurable MACs
- Scheduler for multi-tier cellular systems
- Scheduler for cooperative systems
- Scheduler for relay systems
- Security issues in MAC designs
- Time-critical MAC designs

Track 3: Mobile/Wireless Networks
- Ad hoc networks
- Body area networks
- Cognitive radio networks
- Congestion, load & admission control
- Delay-tolerant networks
- Dynamic spectrum management
- Future wireless internet
- Green wireless networks
- Location management
- Mobile and wireless IP
- Mobile computing
- Multi-hop networks
- Network architectures
- Routing, QoS and scheduling
- Satellite communications
- Self-organizing networks
- Smart cities, grids, etc.
- Transport layer
- Vehicular networks
- Wireless multicasting, broadcasting, and geo-casting
- Wireless sensor networks

Track 4: Services, Apps and Business
- Audio and video broadcast applications
- Authentication, authorization & accounting
- Context/location-aware pervasive systems
- Cyber-physical system/real-world Internet
- Emerging wireless/mobile applications
- Intra-vehicle communications
- Mobile multimedia services
- Link data and networked knowledge
- Next generation digital home networks
- P2P services for multimedia
- Personalization, profiles and profiling
- Secure network and service access
- Self-adaptation on the service layer
- Semantic technologies
- Service discovery
- Cloud computing, virtualization, & service-oriented architectures
- Service portability
- User interfaces, user-machine interactions
- Wireless emergency and security systems
- Wireless robotics, wearables, implants, and wireless for AR/VR and immersion, ...

Manuscripts shall not exceed five double column pages. Complete information about the electronic paper submission process will be made available in the conference website. All accepted and presented papers will be submitted for inclusion in IEEE Xplore®.

SCIENTIFIC ASSOCIATION FOR INFOCOMMUNICATIONS

Who we are

Founded in 1949, the Scientific Association for Infocommunications (formerly known as Scientific Society for Telecommunications) is a voluntary and autonomous professional society of engineers and economists, researchers and businessmen, managers and educational, regulatory and other professionals working in the fields of telecommunications, broadcasting, electronics, information and media technologies in Hungary.

Besides its 1000 individual members, the Scientific Association for Infocommunications (in Hungarian: Híradástechnikai Tudományos Egyesület, HTE) has more than 60 corporate members as well. Among them there are large companies and small-and-medium enterprises with industrial, trade, service-providing, research and development activities, as well as educational institutions and research centers.

HTE is a Sister Society of the Institute of Electrical and Electronics Engineers, Inc. (IEEE) and the IEEE Communications Society.

What we do

HTE has a broad range of activities that aim to promote the convergence of information and communication technologies and the deployment of synergic applications and services, to broaden the knowledge and skills of our members, to facilitate the exchange of ideas and experiences, as well as to integrate and harmonize the professional opinions and standpoints derived from various group interests and market dynamics.

To achieve these goals, we…

- contribute to the analysis of technical, economic, and social questions related to our field of competence, and forward the synthesized opinion of our experts to scientific, legislative, industrial and educational organizations and institutions;
- follow the national and international trends and results related to our field of competence, foster the professional and business relations between foreign and Hungarian companies and institutes;
- organize an extensive range of lectures, seminars, debates, conferences, exhibitions, company presentations, and club events in order to transfer and deploy scientific, technical and economic knowledge and skills;
- promote professional secondary and higher education and take active part in the development of professional education, teaching and training;
- establish and maintain relations with other domestic and foreign fellow associations, IEEE sister societies;
- award prizes for outstanding scientific, educational, managerial, commercial and/or societal activities and achievements in the fields of infocommunication.

Contact information

President: **GÁBOR MAGYAR, PhD** • *elnok@hte.hu*

Secretary-General: **ISTVÁN BARTOLITS** • *bartolits@nmhh.hu*

Operations Director: **PÉTER NAGY** • *nagy.peter@hte.hu*

International Affairs: **ROLLAND VIDA, PhD** • *vida@tmit.bme.hu*

Address: H-1051 Budapest, Bajcsy-Zsilinszky str. 12, HUNGARY, Room: 502

Phone: +36 1 353 1027

E-mail: *info@hte.hu*, Web: *www.hte.hu*