www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 3 Issue 2 February,2014 Page No. 3933-3937

Secure and efficient application of MANET using Identity Based cryptography combined with Visual cryptography technique

R. K. Sharma[1], Neeraj Kishore[2], Parijat Das[3]

[1]Department of Mathematics,
Indian Institute of Technology New Delhi, India 110016.
rkshrmaiitd@gmail.com

[2]Department of Computer Science and Engineering,
Indian Institute of Technology New Delhi, India 110016.
mcs122804@cse.iitd.ac.in

[3] Department of Computer Science and Engineering,
Indian Institute of Technology New Delhi, India 110016.
mcs122841@cse.iitd.ac.in

Abstract: ***Data security is an important issue in military devices. This paper presents a secured and efficient way of sending data and image in encrypted form using Identity Based Cryptography and Visual Cryptography. This has direct application in MANETs specifically for military surveillance [16]. This paper also presents an advantage of using public - private key pairs in Visual Cryptography wherein generally only the private key generators are used. In this paper, the simplicity of RSA algorithm is adopted to set up the public - private key pairs of all the mobile nodes and hence for encryption and decryption [22]. Regeneration of public-private keys is adopted to make the system more secure from various attacks [6].***

Keywords: MANET, RSA, Identity Based Cryptography, Visual Cryptography.

1. Introduction

The Mobile Ad hoc Network (MANET) find useful application in military purposes as mobility is very important requirement in border surveillance. Also the robustness of MANETs to function even in unknown terrain justifies its application as military devices. Visual Cryptographic technique, due to its simplicity and efficiency makes it the appropriate choice for sending / receiving images and finds use in transmitting encrypted images to and fro base station from border military forces [4] [5]. Instead of using only private key generators, both public - private key pairs are adopted to make the system more secure.

Identity based cryptographic technique represents a system having a solitary base station with numerous mobile nodes which is identical to that of Mobile Ad hoc Network (MANET) and hence finds application in this paper [1] [2]. The steps of Identity based cryptography are adopted to set up the system and hence for encryption and decryption of data [2].

Fast encryption and decryption provided by RSA public - private keys rather than the complex and slow bilinear pairing is made use of in this paper since quick transmission of data is sometimes of utmost priority in military [22].

Regeneration of public - private keys of the complete system takes place ensuring more effective data security. Regeneration of keys occurs after each threshold amount of time has elapsed or some terminal node is captured. The scheme proposed in this paper also ensures that when somebody is captured, the system behaves in an undisturbed manner [6].

2. Problem Statement

In border patrol military forces, the armed personnel patrolling at the border needs to send some urgent data / images to their control room (base station). To deal with this, we proposed a secure scheme using identity based cryptography and visual cryptography. As the scenario is extremely prone to foreign attacks, the scheme adopted must be highly secure, efficient as well as robust to overcome the challenges of inaccessibility of unknown terrains. Moreover, an additional requirement is that system should function normally even if any military personnel have been captured.

3. Proposed Scheme

The figure depicted below represented MANET with Nodes (1...n) along with a base station having the identity information

of different mobile nodes and there corresponding public private keys.

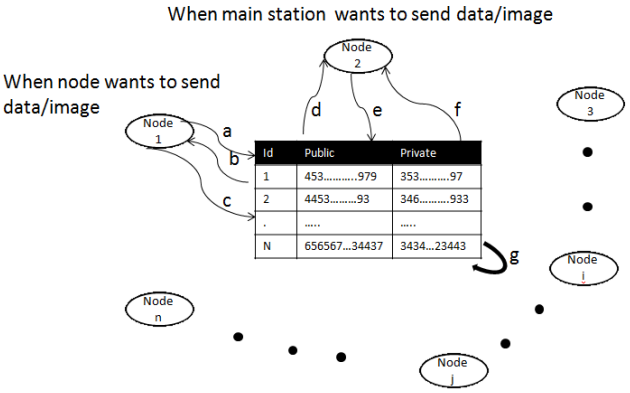

Figure 1.a : Proposed Architecture

Symbol	Meaning
a	Request Key
b	Key Given
c	Encrypted message
d	Encrypted message
e	Request Key
f	Key Given
g	Key Refreshing

Figure 1.b : Notation in Proposed Architecture

3.1 Definitions

Node (1....n): MANET mobile Nodes which are devices carried by military personnel to send / receive information. They don't have their public - private keys, only contain their identity information. During transmission, they authenticate themselves with the base station and have the key for encryption.

Main Station: It is the main control room monitoring the overall functioning of the entire network. It holds the identity / public / private keys all nodes. It also acts as Public / Private Key Generator of the network.

3.2 Purpose

Role of devices is to transmit the data / image to the main station. Role of Main Station is to regenerate the keys at appropriate time stamps. Main station also acts as Authenticator of the whole system. The main station can also transmit of data/image to mobile nodes.

4. Proposed Algorithms

4.1 Visual Cryptography Sharing Case with Two Shares

This is a special case of (2,N) visual cryptography case where N=2 and thus implies that the original image is split into two shares and both the shares are required to decrypt the information contained in the original image. Stacking the two shares into some transparency reveals information about the original image while no information can be obtained from the individual shares.

Figure 2.a : Original Image

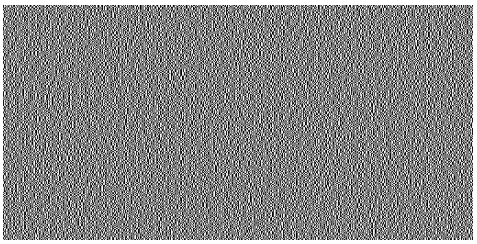

Figure 2.b : First Share

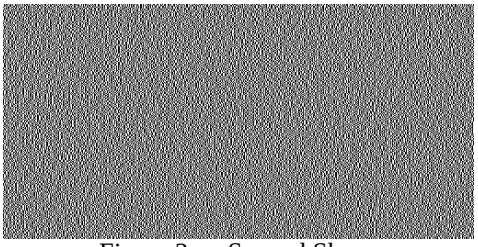

Figure 2.c : Second Share

This is typically a two stage process:
1. Encryption of secret image by creating a registered share.
2. Decryption from the registered share.

Encryption Phases:

Input: A dummy image H, a binary secret image S with S_1 X S_2 pixels, and a public key K.
Output: A registered share O of size S_1 X S_2 pixels each of which is composed of 4 sub-pixels.

Steps are as follows:

1. Compute the mean μ of the pixel values of the dummy image H.
2. Form a random numbers list R = (r_1,r_2…) where r_i ϵ {1,2,…H_1 X H_2} where H_1X H_2 is the size of the dummy image H using the key generator K (not necessarily private).
3. Using these random numbers extract the corresponding pixels from the dummy image to form a sample of size n ($n \geq 30$ here n is chosen more than 30 to take into account a sample of sufficient size) with sample mean $\bar{X}$. For each pixel $s_{i,j}$ of the secret image S, the pixel values of each pixel of the registered share O is computed by applying the following encryption rules:

If $s_{i,j} = 0$ (black) and $\bar{X} < \mu$ then $o_{i,j}$ = 

If $s_{i,j} = 1$ (white) and $\bar{X} \geq \mu$ then $o_{i,j}$ = 

If $s_{i,j} = 1$ (white) and $\bar{X} < \mu$ then $o_{i,j}$ = 

If $s_{i,j} = 0$ (black) and $\bar{X} \geq \mu$ then $o_{i,j}$ = 

4. Repeat the above step until all pixels of secret image is picked.

Decryption phases:

Input: A dummy image H', a binary registered share O with S_1 X S_2 pixels and a private key K.
Output: A decrypted secret image of size S_1 X S_2 pixels.

Steps are as follows:

1. Compute the mean μ' of the pixel values of the dummy image H'.
2. Form a random numbers list R = (r_1,r_2…) where r_i ϵ {1,2,…H_1 X H_2} where H_1X H_2 is the size of the dummy image H using the key generator K (not necessarily private) as the seed.
3. Using these random numbers extract the corresponding pixels from the dummy image to form a sample of size n (n≥30) with sample mean $\bar{X}$'. For each pixel $o_{i,j}$ of the registered share O, each pixel $s'_{i,j}$ of the secret image S is decrypted by applying the following decryption rules:

If $o_{i,j}$ =  and $\bar{X}' < \mu'$ then $s'_{i,j} = 0$ (black)

If $o_{i,j}$ =  and $\bar{X}' \geq \mu'$ then $s'_{i,j} = 1$ (white)

If $o_{i,j}$ =  and $\bar{X}' < \mu'$ then $s'_{i,j} = 1$ (white)

If $o_{i,j}$ =  and $\bar{X}' \geq \mu'$ then $s'_{i,j} = 0$ (black)

4. Repeat the above step until all pixels of registered share is picked.
Finally a decrypted image S is obtained after stacking S' over the registered share O using visual cryptography.

4.2 Identity Based Cryptography

Setup: This algorithm is run by base station initially to set up the system. The secret key is kept secret and public keys are derived. Also, the system parameters are made public.
Parameters: Message space, Cipher-Text space, p-q values (P) – {0,1}*.
Extract: This algorithm is run by the base station when a user requests his private key.
Encrypt: Takes M (Message), the system parameters (P), Public key (Pk) and outputs the encrypted message (C) {a-z,0-9}*.
Decrypt: Accepts encrypted message (C), system parameters (P), Private key (Sk) and returns M (Message).

4.3 Key Refreshing

1. PKG generates the prime parameters corresponding to the time frame ($time_t$: $param_t$). Master key (M) is generated and by its help, the public, private keys of users are generated. (P_{KT}, S_{KT}).
2. In the new time frame {(T_i) [i ϵ (0.....∞)]}, above step is repeated for each i.
3. The step 2 is repeated for each time frame or if some node is compromised.

4.4 Encryption / Decryption

Each node in this scenario has its public and private key (P_{KT}, S_{KT}) in the PKG. To make the working of system simpler and faster we use the RSA pairing for encryption / decryption. (System parameters : S_t,μ_{1t},μ_{2t} , Encryption key : (E_t,S_t), Decryption key : (D_t,S_t) where {(E_t,D_t) ϵ N })
$C = E(M) = M^{Et} \pmod{S_t}$
$M = D(C) = C^{Dt} \pmod{S_t}$

4.4 Generation of Public / Private Keys

1. Generation of System parameters (S_t,μ_{1t},μ_{2t},Ω_t {μ_{1t},μ_{2t} are sufficiently large prime No. and S_t is their multiplication, Ω_t : (μ_{1t}-1)*(μ_{2t}-1) }).
2. Generate a random prime No. (large) [i]. Generate another random large prime No. [j] satisfying the condition {(i*j)mod Ω_t=1}. Allocate these keys i : public key for MANET $node_i$ and j: private key for $node_i$.
3. Repeat step 2 for every $node_i$, i ϵ (0.....n) i.e. for all MANET nodes.

5. Results and Conclusion

The proposed scheme is implemented in MATLAB and C++ using open-ssl library of cryptography. To make use of parallelism in the implementation, pthread library of C++ is used. The initial function is to set up the base station / control room which contains the identity information of all the mobile nodes along with their public and private keys. In this initial function the open-ssl library is used to generate the keys of all the mobile terminals. The implementation generates large keys supporting up to 65536 bits.

Figure 3.a : Private key

Figure 3.b : Public key

These above keys are hash mapped with the identity of all the nodes. For hashing, standard MD5 technique [23] is used for security. The implementation supports data transfer from mobile nodes to base station and fro in parallel and for this the pthread library plays the key role. MATLAB is used in conjunction with C++ to show the image transmission to and fro from mobile nodes to base station. For data transfer, the algorithms described in Section 4 are implemented.

The keys generated by the base station takes ample amount of time which is shown in the below graph according to the key length.

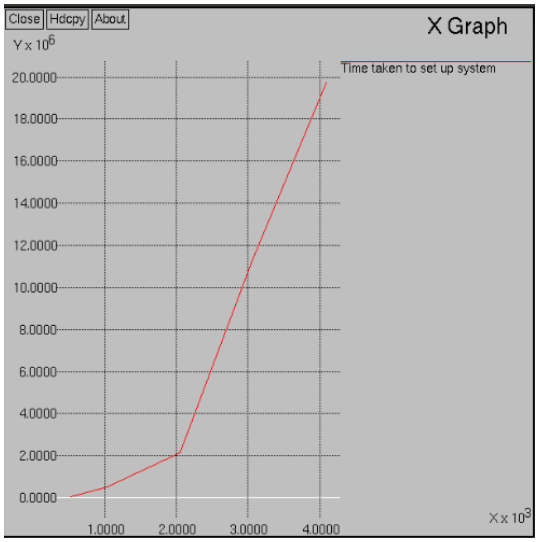

Figure 4.a : Setup Time

In figure 4.a, the x-axis shows the size of keys in bits and the y-axis is the amount of time taken to generate those keys by the base station.

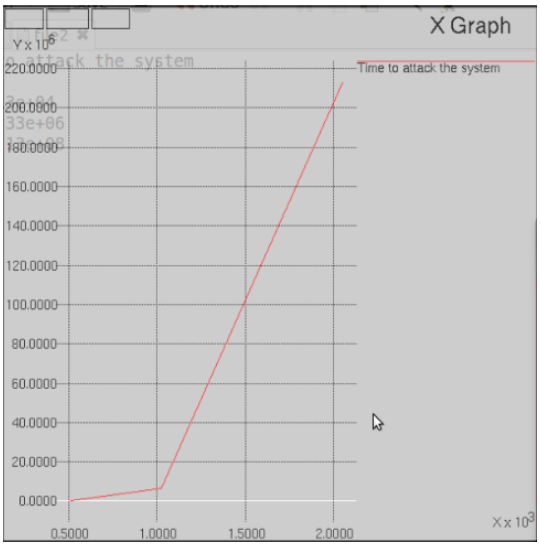

Figure 4.b : Attacking time using Brute force

In figure 4.b, the x-axis shows the size of keys in bits and the y-axis is the amount of time taken to decipher the text encrypted with the help of those keys using brute force technique.

6. Future Work

Further efforts are being made to reduce the setup time of the base station and improving the time complexity of the above mentioned Algorithm. Further improvement is under process to come up with the scheme which can efficiently tell us about some terminal node being captured.

7. References

[1] Dr.(Mrs).G.Padmavathi, "Improved Khalili - Katz - Arbaugh ID based cryptographic key management for Mobile Ad-hoc Networks". Volume 2, No. 04, June 2013 ISSN – 2278-1080 - The International Journal of Computer Science & Applications (TIJCSA).

[2] Shushan Zhao, Akshai Aggarwal, Richard Frost, Xiaole Bai, "A Survey of Applications of Identity-Based Cryptography in Mobile Ad-Hoc Networks", IEEE COMMUNICATIONS SURVEYS & TUTORIALS, 2001.

[3] Joonsang Baek, Jan Newmarch, Reihaneh Safavi-Naini1, and Willy Susilo, "A Survey of Identity-Based Cryptography" - Proceedings of PKC 2004, LNCS 2947, pages. 262-276, Springer-Verlag, 2004.

[4] Der-Chyuan Lou, Hao-Kuan Tso, Jiang-Lung Liu, "A copyright protection scheme for digital images using visual cryptography technique", Computer Standards & Interfaces, Volume 29, Issue 1, January 2007, Pages 125–131, ADC Modelling and Testing.

[5] Ren-Junn Hwang, "A Digital Image Copyright Protection Scheme Based on Visual Cryptography", Tamkang Journal of Science and Engineering, Vol. 3, No. 2, pp. 97-106 (2000).

[6] Shane Balfe, Kent D. Boklan, Zev Klagsbrun, Kenneth G. Paterson, "Key Refreshing in Identity-Based Cryptography and its Applications in MANETs". Surrey, DOI:10.1109/MILCOM.2007.4454916 In proceeding of: Military Communications Conference, 2007. MILCOM 2007. IEEE.

[7] Mihai-Lica PURA, "Quantitative Evaluation of Identity Based Cryptography in an Authentication Scenario". International conference of scientific paper - 2013 Brasov, 23-25 May 2013.

[8] Xuhua ding, Gene Tsudik, "Simple identity-based cryptography with mediated rsa" topics in cryptology — ct-rsa 2003 lecture notes in computer science volume 2612, 2003, pp 193-210.

[9] Edward S. Rogers, "Distributed Symmetric Key Management for Mobile Ad hoc Networks", IEEE,2004.

[10] Hao Yang, HaiyunLuo, Fan Ye, Songwu Lu, Lixia Zhang, "Security in mobile ad hoc networks: Challenges and Solutions", IEEE Wireless Communications, February 2004.

[11] HishamDahshan and James Irvine, "Authenticated Symmetric Key Distribution For Mobile Ad Hoc Networks", IEEE Surveys & Tutorials, 2008.

[12] Hoeper K and G. Gong, "Bootstrapping Security in Mobile Ad Hoc Networks Using Identity-Based Schemes with Key Revocation," tech. rep., Centre for Applied Cryptographic Research, Univ. of Waterloo, 2006.

[13] Hongmei Deng, Dharma P. Agrawal, "TIDS: threshold and identity-based security scheme for wireless ad hoc networks", Elsevier, Ad Hoc Networks 2 (2004) pp. 291 307.

[14] Horwitz J and B. Lynn, "Toward hierarchical identity-based encryption", EUROCRYPT, volume 2332 of Lecture Notes in Computer Science, pages 466–481. Springer, 2002.

[15] Hua Sun, XuefengZheng, Zhongjun Deng, "An Identity-based and Threshold Key Management Scheme for Ad hoc Networks", IEEE, 2009.

[16] Jianmin Chen and Jie Wu, "A Survey on Cryptography Applied to Secure Mobile Ad Hoc Networks and Wireless Sensor Networks", 2007.

[17] Matsui K., Ohnishi J., and Nakamura Y., "Embedding a Signature to Pictures under Wavelet Transform," IEICE Transactions, Vol. J79-D-II, No. 6, pp. 1017-1024(1996).

[18] Naor N. and Shamir A. “Visual Cryptography,” Advances in Cryptology: Eurocrypt’94, Springer-Verlag, Berlin, pp. 1-12(1995).
[19] Ohbuchi R., Masuda H., and Aono M., “Watermarking Three-Dimensional Polygonal Models through Geometric and Topological Modifications,” IEEE Journal on Selected Areas in Communications, Vol. 16, No. 4, pp.551-560(1998).
[20] Ohnishi J. and Matsui K., “Embedding a Seal into a Picture under Orthogonal Wavelet Transform,” The Proceedings of IEEE International Conference on Multimedia Computing and Systems, pp. 514-512(1996).
[21] Hongwei Si, Youlin Cai, Zhimei Cheng,”An Improved RSA Signature Algorithm based on Complex Numeric Operation Function. 978-0-7695-3972-0/10 $26.00 © 2010 IEEE.
[22] M. J. Wiener, “Cryptanalysis of short RSA secret exponents,” IEEE Trans. Inf. Theory, vol. 36, no. 3, pp. 553–559, May 1990.
[23] Zhao Yong-Xia, Zhen Ge," MD5 Research ". Multimedia and Information Technology (MMIT), 2010 Second International Conference on Date 24-25 April 2010.

Author Profile

[1] Dr. R. K. Sharma is a Professor & Former Head in the department of Mathematics, Indian Institute of Technology New Delhi 110016.
[2] Neeraj Kishore is an M.Tech final year student of Computer Science and Engineering Department in Indian Institute of Technology New Delhi 110016. He received his B.Tech degree in Computer Science and Engineering from National Institute of Technology, Bhopal in 2012.
[3] Parijat Das is an M.Tech final year student of Computer Science and Engineering Department in Indian Institute of Technology New Delhi 110016. He received his B.Tech degree in Electronics and TeleCommunication Engineering from Jadavpur University, Kolkata in 2011.