INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH & DEVELOPMENT

ISSN 2278 – 0211 (Online)

A Secure Encounter-Based Key Transmission over Tor Network In Mobile Social Networks for Improving Security and Privacy

B. Suganya
Ratnavel Subramaniam College of Engineering and Technology, RVS Nagar, Dindigul
J. Viji Priya
Professor, Ratnavel Subramaniam College of Engineering and Technology, RVS Nagar, Dindigul

Abstract:
Mobile social networks are attractive applications which composed of a collection of different users from different countries. On that, the group of users can share personal information and stay connected with some of the users. Due to the lack of security infrastructure, the eavesdropper may intrude the conversation. In order to provide secure communication on mobile social networks an encounter-based system with Ciphertext-Policy Attribute Based Encryption (EBS-CPABE) is proposed. The proposed method provides efficient and secure communication with the proper security mechanisms. The Digital Signature Algorithm (DSA) is used for key generation. The key exchange mechanism is used to know about the authenticated users. A Ciphertext-Policy attribute-based encryption (CPABE) scheme is proposed for providing additional security as, if any server storing the data is compromised, then the confidentiality of the data will be compromised. In the proposed system for complex access control on encrypted data that we include Ciphertext-Policy Attribute-Based Encryption (CPABE). Also Tor network is built for enabling online anonymity. The performance of the proposed EBS is tested based on memory usage, execution time and delay rate. The experimental results obviously show that the proposed method performs well than the existing Encounter Based System (EBS).

Key words*: Ciphertext-Policy Attribute-Based Encryption (CPABE), Digital Signature Algorithm (DSA), Encounter-based, Key exchange, Mobile Social Networks, and Tor network*

1. Introduction

Mobile social networking is social networking where individuals with similar interests converse and connect with one another through their mobile phone or tablet. Much like web-based social networking, mobile social networking occurs in virtual communities. Social Network Sites (SNS) allow the users to broadcast the information and digital content across the mobile social networks. These services treat all the social network user's contacts equally. Social networking sites like Twitter, LinkedIn, and Twitter etc. have been increasingly gaining popularity. Moreover, Face book has been reporting growth rates as high as 3% per week[1]. There are significant security and privacy problems are present in most of the existing mobile social network systems. Because, these systems lack with the security and privacy metrics for secure communication.

Encounter-based social networks provide a computing infrastructure to allow for construction of varied services such as a some missed connections or real time key distribution to provide secure communication. At first look, encounter-based systems appear similar to the existing social networks. It provides different challenges for security and privacy of users and authenticity of the other user in a conversation. To provide a secure environment, public key infrastructure (PKI) is needed. A PKI is an arrangement that binds public keys with respective user identities by means of a certificate authority (CA). The user identity must be unique within each CA domain. The third-party validation authority (VA) can provide this information on behalf of CA. The PKI role assures the binding is called the registration authority (RA), which ensures that the public key is bound to the individual to which it is assigned in a way that ensures non-repudiation.PKI consists of five important concepts. 1. Central authority (CA) that issues and verifies the digital certificates. 2. Registration authority (RA) verifies the identity of users requesting information from the CA. 3. Central directory is a secure location to store and index keys. 4. Central management system and 5. Certificate policy.

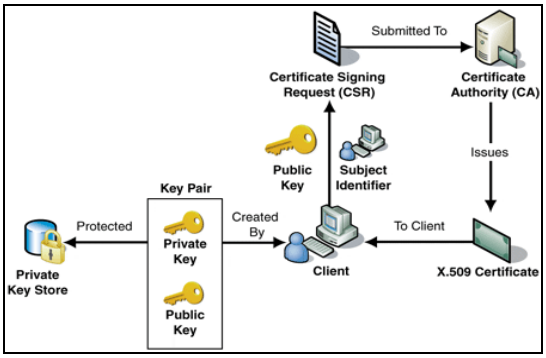

Figure 1: Public key infrastructure for secure communication

In this paper, an encounter-based system is proposed to provide efficient and secure communication in the mobile social networks. For that, a public key infrastructure is maintained in the conversation between two authenticated users. So that the eavesdropper can't receive the message, instead the eavesdropper may modify the message. But, the authenticated user can identify with the help of security mechanisms. The Digital Signature Algorithm is used for key generation. It computes the public and private keys for each user to initialize the secure conversation.Tor network are incorporated in this proposed method. The Tor network is used for enabling online anonymity. Tor directs internet traffic through a free, worldwide, volunteer network consisting of more than four thousand relays to conceal a user's location or usage from anyone conducting network surveillance or traffic analysis. Tor indented to protect the personal privacy of users as well their freedom and ability to conduct confidential business by keeping their internet activities from being monitored.

The rest of the paper is organized as follows. Section II presents a description about the previous research which is relevant to the techniques used on secure social mobile networks. Section III involves the detailed description about the proposed method. Section IV presents the performance analysis. This paper concludes in Section V.

2. Related Work

Shamir et al proposed secret sharing scheme in the private key, the authority embeds a more general secret sharing scheme for monotonic access trees. [2].*Kui et al* presented the fundamental and general framework of the PHY-based key generation schemes and categorize them into two classes namely received-signal-strength based and channel-phase-based protocols[3].*Zhang et al* presented a security and privacy design challenges which were brought by the core functionalities of the Online Social Networks (OSNs)[4].*Zhang* proposed an approach to provide a solution for privacy-preserving collaborative social-network problem[5].*Ying et al* proposed an edge-based graph randomization approach to protect the sensitive links. The theoretical studies and empirical evaluations were made with the different similarity measures to improve their confidence and accuracy of predicted sensitive links between nodes[6].

Wasef et al proposed a complementary security mechanism that can meet the security requirements. Because, the denial of service (DOS) attacks had severe consequences on network availability. Here, the security mechanisms were proposed to mitigate the effect of DOS attacks in Vehicular Adhoc Networks (VANETs)[7].*Rongxing et al*proposed a dynamic privacy-preserving key management scheme called DIKE. A privacy-preserving authentication technique was introduced. This technique not only provides the vehicle user's anonymous authentication but also enables the double-registration detection. Also, the location based services (LBS) session key update procedures were presented[8]. The LBS session was divided into several time slots, each time slot holds a different session key. A dynamic threshold technique was incorporated to achieve the session key's backward secrecy.*Ray et al* proposed a secure framework that allows interaction of social network information with LBS without compromising user privacy and security. This framework allows LBS to query its vicinity for relevant information without disclosing under identity[9].

Nitinawarat et al proposed explicit algorithm for secret key generation which was based on a maximal packing of Steiner trees in a multigraph. The goal of this approach was to generate a secret key shared by a given subset of terminals at the largest possible rate with the cooperation of any remaining terminals[10].*Nagy et al* proposed a PeerShare system. It can be used by applications to securely distribute sensitive data to social contacts of a user. A generic framework was incorporated to distribute data among different applications with authenticity and confidentiality. It was designed to be easy for both the end users and the developers of applications [11].*Masoumzadeh et al*proposed two methods to enhance perturbing anonymization methods. It is based on the concepts of the structural roles and edges between social networks[12].

Li et al proposed a technique called FindU. FindU had a set of privacy preserving profile matching schemes for proximity based mobile social networks. An initiating user can find from a group of users to limit the risk of privacy exposure. Here, only the necessary and minimal information about the private attributes of the participating users was exchanged. Also, two increasing levels of user privacy were defined, with reduced amount of revealed profile information. The set of rules was developed to realize each of the user privacy levels, which can also be personalized by the users[13].*Perrig et al* proposed a SafeSlinger approach. It leverages the proliferation of smartphones to enable people to securely and privately exchange their public keys. SafeSlinger establishes a secure channel offering secrecy and authenticity to support secure messaging and file exchange. An abstraction was supported to safely sling information from one device to another[14].*Isdal et al*presented a design point in tradeoff between privacy and performance technique

called OneSwarm. It provides users much better privacy than BitTorrent.The key aspect of this design was users explicitly configure control over the amount of trust. Here, the same data can be shared publicly or with access control with both trusted and untrusted peers[15].

3. Encounter Based System with Attribute Based Encryption (EBS-CPABE)

An encounter-based system is proposed for efficient and secure communication on the mobile social networks. Tor network with RSA algorithm are used for secure and authenticated communication. The following section describes about the secure conversation process in detail.

3.1. Key Generation-DSA

Key generation is the process of generating keys for secure environment. A generated key is used to encrypt and decrypt the data is being encrypted/decrypted. Here, DSA is used as a key generation algorithm.

Algorithm--DSA

Step1: //Parameter generation steps

- Choose san approved cryptographic hash function *H.*
- Decide the key length l and *n*
- Chose *n-bit* prime *b. n* must be less than or equal to the hash output length.
- Choose *n-bit* prime modulus *a* such that a-1 is a multiple of *b*
- Choose*d* whose multiplicative order modulo *a* is *b*

Here, $d = h^{(a-1)/b} \bmod a$ for some arbitrary *h(1<h<a-1).* The variables *(a,b,d)* may be shared between different users of the system.

Step 2: //Public and private key computation

- Choose random integer *p,* where*0 <p < b*
- Calculate $q = d^p \bmod a$
- Now, the public key is *(a, b, d, q)* and the private key is *p*

Step3: //Signing

- Generate a random per-message value *l* where *0<l<b*
- Find $x = (d^l \bmod a) \bmod b$
- If x=0 then start again with some other random *l*
- Find $y = l^{-1}(H(m) + px) \bmod b$
- If y=0 then start again with some other random *l*
- Return signature *(x ,y)*

Step4: //Verifying

- Reject the signature if *0 < x < b* or *0 < y < b* is not satisfied
- Find $r = y^{-1} \bmod b$
- Find $s_1 = H(m).r \bmod b$
- Find $s_2 = x.r \bmod b$
- Find $u = ((d^{s_1} q^{s_2}) \bmod a) \bmod b$
- If *u = x*
- The signature is valid

The algorithm explains the complete key generation process of DSA algorithm. It incorporates four major steps. i.e. parameter generation, public and private key computation, signing and verifying the signatures. With the sender message, additionally an image is also converted into hash code to provide a higher level of privacy.

3.2. Central Authority

The digital certificate certifies the ownership of a public key by the named subject of the certificate. This allows other parties to depend upon signatures or assertions made by the private key that corresponds to the public key that is certified. The matching private keys are not made available publicly, but kept secret by the end user who generated the key pair. The certificate is also a confirmation or validation by the CA that the public key contained in the certificate belongs to the server or other entity noted on the certificate. After key generation, the keys are exchanged between the sender and the receiver.

3.2.1. Immediate Key Exchange

In this key exchange scenario, the user selects the picture based on their willingness. Then compose an encounter key with the public key. The resulting message can be broadcasted. Each user in the vicinity will detect the transmission and try to decrypt it. But, only the targeted user can be able to decrypt the message properly and thus recover the encounter key. Further, this key will be used to

exchange the private messages at the rendezvous point. This process avoids the rendezvous server and colluding adversaries from determining which two users are communicating. Also, timed release encryption is used to hide the contents of the message even from its recipient until the encounter is over.

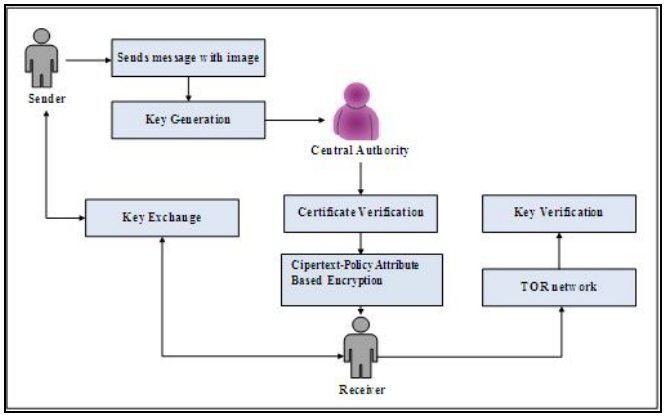

Figure 2: Flow of the proposed system

3.2.2. Delayed key exchange

The system will constantly broadcast their certificates, but not require other users to immediately evaluate the information. Later, the user can check the list of collecting public keys and select with the particular user to start the conversation. This process is not suffering from the shortcomings in the immediate pairing scheme. Additionally, the system is incorporated with the Tor network for enabling the anonymity.

3.3. Ciphertext –Policy Attribute based Encryption

A Ciphertext Policy Attribute-Based Encryption (CPABE) scheme is proposed for providing additional security. CPABE extends the cipher text-policy attribute-set-based encryption with a hierarchical structure of system users, so as to achieve scalable, flexible and fine-grained access control. In this CP-ABE process, the cipher text is encrypted with policy chosen by an encryptor, while the corresponding decryption key is created with respect to a set of attributes; user's private key will be associated with an arbitrary number of attributes expressed as strings. On the other hand, when a party encrypts a message in our system, they specify an associated access structure over attributes. A user will only be able to decrypt a ciphertext if that user's attributes pass through the ciphertext's access structure.

As long as the set of attributes associated with a decryption key satisfies the policy associated with a given cipher text, the key can be used to decrypt the cipher text. Through CP-ABE, the proposed model achieved much more security for this type of attribute based encryption process. Here the unauthorized user does not retrieve the original information.

3.4. The Tor Network

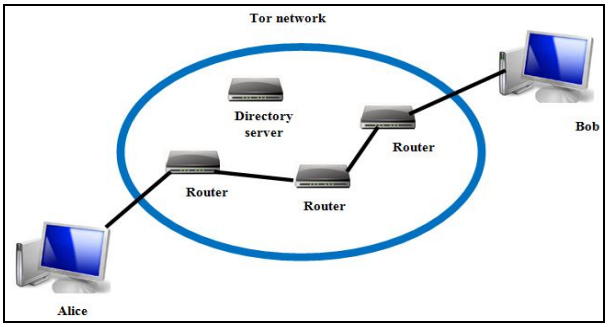

Figure 3: Architecture of Tor network

The Tor network is an overlay network; each anonymous router runs as a normal user-level process without any special authorities. Each router maintains TLS connection to every other router. Each user runs local software called a proxy to fetch directories. Each router maintains a long-term identity key and a short-term key. It is essentially used to sign the TLS certificates to sign router descriptor. The key is used to decrypt requests from users to set up a circuit and negotiate the keys. The TLS protocol establishes a short-term key when communicating between routers. It is rotated periodically and independently to reduce the impact of key compromise.

4. Performance Analysis

This section presents the performance evaluation of the proposed Encounter Based-System for efficient and secure transmission. The performance is evaluated based on the following measures:

4.1. Delay Rate

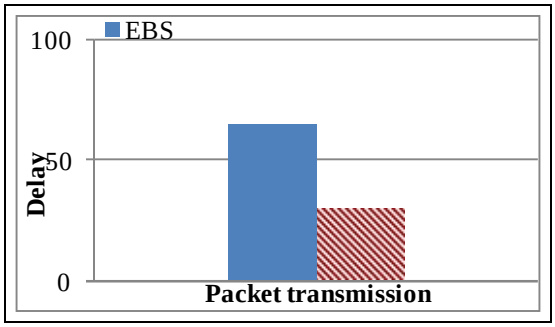

Figure 4: Delay rate for EBS-CPABE (proposed) and EBS (existing)

Fig.4. shows the comparison of delay rate between the existing Encounter Based System (EBS) with the proposed Encounter-Based System with Ciphertext-Policy Attribute Based Encryption (EBS-CPABE). It shows that the proposed system EBS-CPABE results less delay than the existing EBS method.

4.2. Execution time

It is the time taken to complete the entire process of transmission from the sender to the receiver. Fig.5 displays the execution time for the existing EBS method and the proposed EBS-CPABE. The time taken for the proposed method is lesser than the existing method.

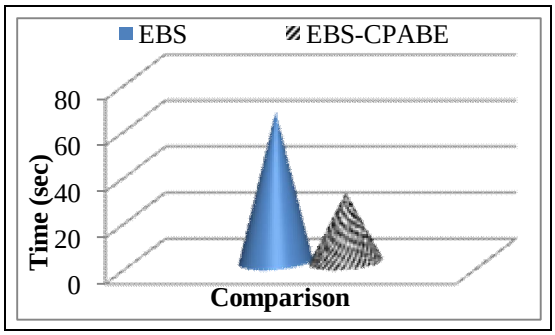

Figure 5: Execution time for EBS-CPABE (proposed) and EBS (existing)

4.3. Signature Algorithm

The EBS-CPABE system uses the DSA algorithm for key generation and the existing system uses the RSA algorithm. The proposed DSA algorithm results lesser time to generate the public and private keys for secure communication. It is shown in Fig.6.

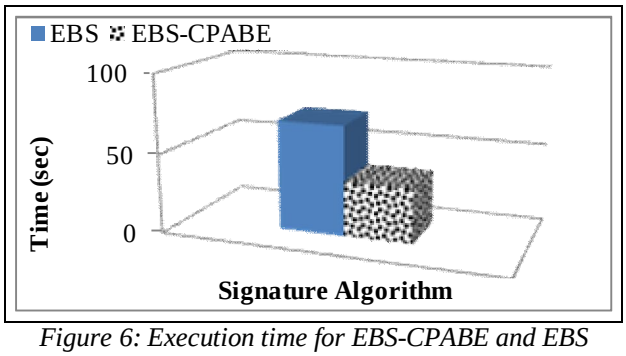

Figure 6: Execution time for EBS-CPABE and EBS

4.4. Memory usage

Fig.7 shows the amount of memory is used for the entire transmission from the source to the receiver side to provide secure communication. The proposed system takes reduced memory usage than the existing system.

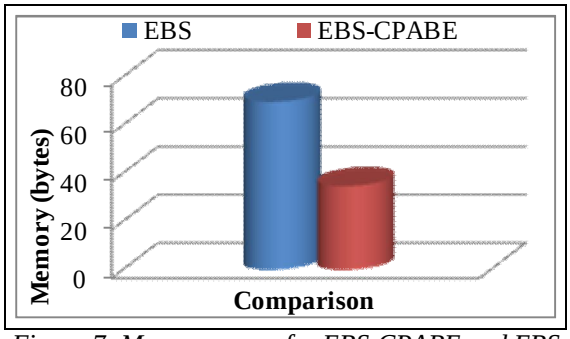

Figure 7: Memory usage for EBS-CPABE and EBS

5. Conclusion and Future Work

An Encounter-Based System is proposed to provide secure communication with the help of Tor networks. The DSA algorithm is used to generate the public and private keys for the authenticated sender and the receiver. The Tor network monitors throughout the network to check about the presence of the eavesdropper. The key exchange mechanism is used to check about the valid user with the key pair. The performance is evaluated and the result shows that the proposed EBS-CPABE results lesser delay and memory usage than the existing EBS method.

In future, Threshold Attribute-Based encryption (TABE) method will be incorporated to provide additional security for to design an error-tolerant (or Fuzzy) identity based encryption scheme that could use biometric identities. TABE extends the threshold with the hierarchical structure of the system users.

6. References

1. "Facebook, http://www.facebook.com," 2009.
2. A. Shamir. Identity Based Cryptosystems and Signature Schemes. In Advances in Cryptology – CRYPTO, volume 196 of LNCS, pages 37–53. Springer, 1984.
3. R. Kui, S. Hai, and W. Qian, "Secret key generation exploiting channel characteristics in wireless communications," Wireless Communications, IEEE, vol. 18, pp. 6-12, 2011.
4. C. Zhang, J. Sun, X. Zhu, and Y. Fang, "Privacy and security for online social networks: challenges and opportunities," Network, IEEE, vol. 24, pp. 13-18, 2010.
5. J. Zhan, "Secure Collaborative Social Networks," Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on, vol. 40, pp. 682-689, 2010.
6. X. Ying and X. Wu, "On link privacy in randomizing social networks," Knowledge and information systems, vol. 28, pp. 645-663, 2011.
7. A. Wasef, L. Rongxing, L. Xiaodong, and S. Xuemin, "Complementing public key infrastructure to secure vehicular ad hoc networks [Security and Privacy in Emerging Wireless Networks]," Wireless Communications, IEEE, vol. 17, pp. 22-28, 2010.
8. L. Rongxing, L. Xiaodong, L. Xiaohui, and S. Xuemin, "A Dynamic Privacy-Preserving Key Management Scheme for Location-Based Services in VANETs," Intelligent Transportation Systems, IEEE Transactions on, vol. 13, pp. 127-139, 2012.
9. B. Ray and R. Han, "SecureWear: A Framework for Securing Mobile Social Networks," in Advances in Computer Science and Information Technology. Computer Science and Engineering. vol. 85, N. Meghanathan, N. Chaki, and D. Nagamalai, Eds., ed: Springer Berlin Heidelberg, 2012, pp. 515-524.
10. S. Nitinawarat, Y. Chunxuan, A. Barg, P. Narayan, and A. Reznik, "Secret Key Generation for a Pairwise Independent Network Model," Information Theory, IEEE Transactions on, vol. 56, pp. 6482-6489, 2010.
11. M. Nagy, N. Asokan, and J. Ott, "PeerShare: A System Secure Distribution of Sensitive Data among Social Contacts," in Secure IT Systems. vol. 8208, H. Riis Nielson and D. Gollmann, Eds., ed: Springer Berlin Heidelberg, 2013, pp. 154-165.
12. A. Masoumzadeh and J. Joshi, "Preserving Structural Properties in Edge-Perturbing Anonymization Techniques for Social Networks," Dependable and Secure Computing, IEEE Transactions on, vol. 9, pp. 877-889, 2012.
13. M. Li, S. Yu, N. Cao, and W. Lou, "Privacy-Preserving Distributed Profile Matching in Proximity-Based Mobile Social Networks," Wireless Communications, IEEE Transactions on, vol. 12, pp. 2024-2033, 2013.
14. A. Perrig, J. McCune, M. Farb, M. Burman, and G. S. Chandok, "SafeSlinger: An Easy-to-use and Secure Approach for Human Trust Establishment," ed: CARNEGIE-MELLON UNIV PITTSBURGH PA CYLAB, 2012.
15. T. Isdal, M. Piatek, A. Krishnamurthy, and T. Anderson, "Privacy-preserving P2P data sharing with OneSwarm," SIGCOMM Comput. Commun. Rev., vol. 40, pp. 111-122, 2010.
16. J. R. Zippel. Probabilistic algorithms for sparse polynomials. In E.W. Ng, editor, EUROSAM, volume 72 of Lecture Notes in Computer Science, pages 216–226. Springer, 1979