International Journal of Engineering Science Invention
ISSN (Online): 2319 – 6734, ISSN (Print): 2319 – 6726
www.ijesi.org ||Volume 3 || Issue 6 || June 2014 || PP.52-56

Secure Transmission over Co-operative Groups: A New Key Management Archetype and Data Leakage Prevention

[1,] Ms. Soji Charles, [2,] Mr. Scaria Alex
[1, 2,] Department of Computer Science and Engineering
Jawaharlal College of Engineering and Technology,Lakkidi, Palakkad, Kerala.

ABSTRACT: *In networks, some problems occur while broadcasting data into users due to limited communication from group to the sender and security constrains. To overcome this issues by using fusion of broadcast encryption and group key agreement as well as data leak prevention for secure communication. The main objective of the project is provide strong proof against the guilty who had leaked the data and if the possible to detect whenever the data is leaked by the guilty. The translation of data in to a secret code. Encryption is the most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to* decrypt *it. Unencrypted data is called* plain text ; encrypted data *is referred to as* cipher text*. The process of decoding data that has been encryption into a secret format. Decryption requires a secret key or password.*

KEYWORD*: Ad hoc networks, broadcast, cooperative computing, access control, information security, key management, Allocation strategies, data leakage.*

I.INDRODUCTION

The problem of efficiently and securely broadcasting to a remote cooperative group occurs in many newly emerging networks. A major challenge in devising such systems is to overcome the obstacles of the potentially limited communication from the group to the sender, the unavailability of a fully trusted key generation center and the dynamics of the sender. The existing key management paradigms cannot deal with these challenges effectively. The new key management paradigm is a hybrid of traditional broadcast encryption and group key agreement. In such a system, each member maintains a single public/secret key pair. Upon seeing the public keys of the members, a remote sender can securely broadcast to any intended subgroup chosen in an ad hoc way. Even if all the non-intended members collude, they cannot extract any useful information from the transmitted messages. After the public group encryption key is extracted, both the computation overhead and the communication cost are independent of the group size. Further, this scheme facilitates simple yet efficient member deletion/addition and flexible rekeying strategies. Its strong security against collusion, its constant overhead, and its implementation friendliness without relying on a fully trusted authority render our protocol a very promising solution to many applications. And addition to that data leakage prevention has proposed. A data distributor has given sensitive data to a set of supposedly trusted agents. Some of the data is leaked and found in an unauthorized place [1]. The distributor must assess the likelihood that the leaked data came from one or more agents, as opposed to having been independently gathered by other means. Proposes data allocation strategies (across the agents) so that can improve the probability of identifying leakages. These methods do not rely on alterations of the released data (e.g., watermarks). In some cases we can also inject "realistic but fake" data records to further improve our chances of detecting leakage and identifying the guilty party. Data leakage causes of leakage and different techniques to detect the data leakage. The value of the data is incredible, so it should not be leaked or altered. In the field of IT, huge database is being used. This database is shared with multiple people at a time. But during this sharing of the data, there are huge chances of data vulnerability, leakage or alteration [2]. So, to prevent these problems, a data leakage detection system has been proposed. This paper includes brief idea about data leakage detection and a methodology to detect the data leakage persons.

The organization of the paper is as follows. After the introduction given in Chapter I, Chapter II gives a brief description about secure transmission and data leakage prevention. Chapter's III explain system model. In chapter IV and chapter V gives proposed techniques and modules and conclusion is given respectively.

II.SECURE TRANSMISSION AND DATA LEAKAGE PREVENTION

There are different aspects for secure transmission between users. Under certain constraints, establish a one-to-many channel efficiently and securely for that formalize the problem of secure transmission to remote cooperative groups. Then propose a new key management paradigm allowing secure and efficient transmissions to remote cooperative groups by effectively exploiting the mitigating features and circumventing the constraints discussed above. Next is to introduce a provably secure protocol in the new key management paradigm and perform extensive experiments in the context of mobile ad hoc networks. In the proposed protocol after extraction of the public group encryption key in the first run, the subsequent encryption by the sender and the decryption by each receiver are both of constant complexity, even in the case of member changes or system updates for rekeying. The common problem is to enable a sender to securely transmit messages to a remote cooperative group [5]. A solution to this problem must meet several constraints. First, the sender is remote and can be dynamic. Second, the transmission may cross various networks including open insecure networks before reaching the intended recipients. Third, the communication from the group members to the sender may be limited. Also, the sender may wish to choose only a subset of the group as the intended recipients.

III.SYSTEM MODEL

In this Module create nodes and made ad hoc network. Each and every node has to generate public and secret key. And allocate a certificate authority person to provide certificate for public key during data transmission but he does not have secret key, receiver only have that secrete key. The remote sender can retrieve the receiver's public key for checking and validate through certificate authority. The potential receivers are linked together with efficient local connections. Using communication infrastructures, they can also join to heterogeneous networks. Each receiver has a public/secret key pair. The public key is certified by a certificate authority, but the secret key is kept only by the receiver. A remote sender can get back the receiver's public key from the certificate authority and validate the authenticity of the public key by checking its certificate, which implies that no direct communication from the receivers to the sender is necessary [7]. Then, the sender can send secret messages to any chosen subset of the receivers. After that officially define the model of group key agreement based broadcast encryption. Since the heart of key management is to securely distribute a session key to the intended receivers, it is sufficient to define the system as a session key encapsulation mechanism. Then, the sender can at the same time encrypt any message under the session key, and only the intended receivers can decrypt.

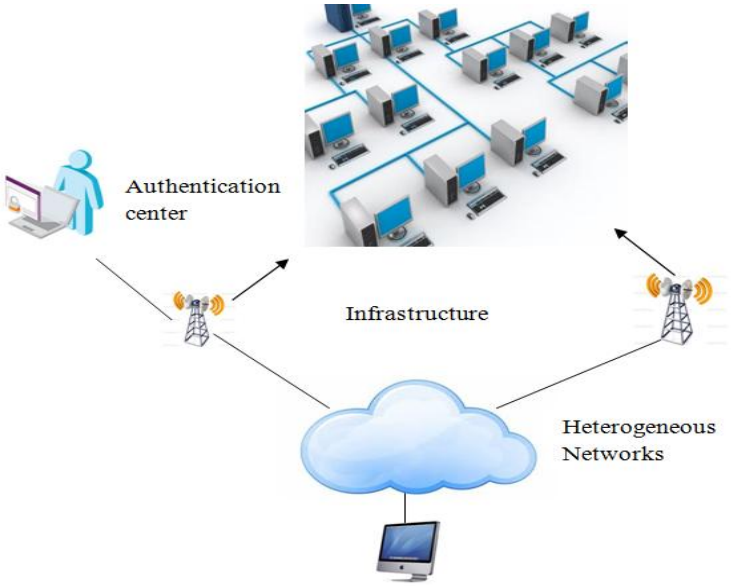

Fig.1: System Model

IV.PROPOSED TECHNIQUES AND MODULES

The proposed techniques are crossbreed of group key agreement and public-key broadcast encryption and collusion prevention.

1. crossbreed of group key agreement and public-key broadcast encryption

The new approach is a hybrid of group key agreement and public-key broadcast encryption. In this approach, each group member has a public/secret key pair. By knowing the public keys of the members (e.g., by retrieving them from a public key infrastructure that is widely available in existing network security solutions), a remote sender can securely broadcast a secret session key to any intended subgroup chosen in an ad hoc way and simultaneously, any message can be encrypted to the intended receivers with the session key [6]. Only the selected group members can jointly decrypt the secret session key and hence the encrypted message. In this way, the dependence on a fully trusted key server is eliminated. Also, the dynamics of the sender and the group members are coped with because the interaction between the sender and the receivers before the transmission of messages is avoided and the communication from the group members to the remote sender is minimized. First, have to formalize the problem of secure transmission to remote cooperative groups, in which the core is to establish a one-to-many channel securely and efficiently under certain constraints. And observe that the existing key management approaches do not provide effective solutions to this problem. On one hand, group key agreement provides an efficient solution to secure intergroup communication, but for a remote sender, it requires the sender to simultaneously stay online with the group members for multiple rounds of interactions to negotiate a common secret session key before transmitting any secret contents.

Broadcast encryption is used to enable the senders to send the broadcast message to cooperative members of a present Group without need the sender must to interact with the receivers before transmitting secret messages, but it relay on a centralized key server to generate and distribute secret keys for each member in the group. It requires that: 1) before a confidential broadcast message channel is established, numerous confidential separate channels from the key server to each receiver must be constructed 2) the key server contain the secret key of every receivers, it can read all the communications and fully trusted by any sender and the group members also [3]. It provide the security against collusion Encrypt by the sender and the decrypt by the receiver are both of less complexity and it enable to send-and-leave broadcasts message to remote cooperative groups without fully trusted third party. Even an attacker cannot retrieve any information about the messages transmitted by the sender in the remote group.

2. Data leakage prevention

Data leakage is the big challenge in front of the industries & different institutes. Though there are number of systems designed for the data security by using different encryption algorithms, there is a big issue of the integrity of the users of those systems. It is very hard for any system administrator to trace out the data leaker among the system users. It creates a lot many ethical issues in the working environment of the office. The data leakage detection industry is very heterogeneous as it evolved out of ripe product lines of leading IT security vendors [4]. A broad arsenal of enabling technologies such as firewalls, encryption, access control, identity management, machine learning content/context based detectors and others have already been incorporated to offer protection against various facets of the data leakage threat. The competitive benefits of developing a "one-stop-shop", silver bullet data leakage detection suite is mainly in facilitating effective orchestration of the aforementioned enabling technologies to provide the highest degree of protection by ensuring an optimal fit of specific data leakage detection technologies with the "threat landscape" they operate in. This landscape is characterized by types of leakage channels, data states, users, and IT platforms [8].

The modules are user login, key management, encryption, user communication, decryption, and data leak prevention.

1. **User login*:*** A data which is stored in the server can be accessed or retrieved by the client if he/she registers their detail which is stored in the database.

2. **Key management:** The major security concern in group-oriented communications with access control is key management. The key management paradigm allowing secure and efficient transmissions to remote cooperative groups by effectively exploiting the mitigating features and circumventing the constraints. This system is to securely distribute a session key to the intended receivers, it is sufficient to define the system as a session key encapsulation mechanism. Then, the sender can simultaneously encrypt any message under the session key, and only the intended receivers can decrypt.

3. **Encryption:** Information security is provided on computers and over the Internet by a variety of methods. A simple but straightforward security method is to only keep sensitive information on removable storage media like portable flash memory drives or external hard drives. But the most popular forms of security all rely on encryption, the process of encoding information in such a way that only the person with the key can decode it. Encryption is the process of encoding messages or information in such a way that only authorized parties can read it. Encryption doesn't prevent hacking but it reduces the likelihood that the hacker will be able to read the data that is encrypted. In an encryption scheme, the message or information, referred to as plaintext, is encrypted using an encryption algorithm, turning it into an unreadable ciphertext. This is usually done with the use of an encryption key, which specifies how the message is to be encoded. Any adversary that can see the ciphertext should not be able to determine anything about the original message. An authorized party, however, is able to decode the ciphertext using a decryption algorithm that usually requires a secret decryption key that adversaries do not have access to. For technical reasons, an encryption scheme usually needs a key-generation algorithm to randomly produce keys.

4. **User communication*:*** Authorized users can access the data which are stored by owner and it allows user to communicate each other**.**

5. **Decryption*:*** Decryption is the process of taking encoded or encrypted text or other data and converting it back into text that you or the computer are able to read and understand. This term could be used to describe a method of unencrypting the data manually or with decrypting the data using the proper codes or keys. Decryption is the reverse operation of encryption. It is the process of decoding the data which has been encrypted into a secret format. An authorized user can only decrypt data because decryption requires a secret key or password. Decryption is the process of decoding encrypted information so that is can be accessed again by authorized users. To make the data confidential, data (plain text) is encrypted using a particular algorithm and a secret key. After encryption process, plain text gets converted into cipher text. To decrypt the cipher text, similar algorithm is used and at the end the original data is obtained again.

6. Data leak prevention: Data leakage is defined as the accidental or unintentional distribution of private or sensitive data to unauthorized entity. Data leak prevention is a strategy for making sure that end users do not send sensitive or critical information outside of the corporate network. The term is also used to describe software products that help a network administrator control what data end users can transfer [10]. Data leakage is defined as the accidental or unintentional distribution of private or sensitive data to unauthorized entity. Sensitive data of companies and organizations includes intellectual property (IP), financial information, patient information, personal credit-card data, and other information depending on the business and the industry [9].

V.CONCLUSION

This paper is efficient and secure for cooperative group communication and it avoids the data leakage while transmission. The key management paradigm is used to enable send-and-depart broadcasts to group of users without depending on a fully trusted third party. It explains the standard model and thorough complexity analysis, extensive experiments show that the proposal is also efficient in terms of computation and communication. These features render our scheme a promising solution to group-oriented communication with access control in various types of ad hoc networks. And also proposed key pre distribution in key management process for rekey when happened the nodes addition deletion. In addition to fast transmission the data leakage prevention helps in accessing the likelihood that an agent is responsible for a leak, based on the overlap of his data with the leaked data and the data of other agents and based on the probability that objects can be guessed by other means. It is hard to resort to a fully trusted third party to secure the communication. In contrast to the above constraints, mitigating features are that the group members are cooperative and the communication among them is local and efficient.

REFERENCES

[1] Qianhong Wu, Member, IEEE, Bo Qin, Lei Zhang, Josep Domingo-Ferrer, Fellow, IEEE, and Jesús A. Manjón "Fast Transmission to Remote Cooperative Groups: A New Key Management Paradigm"- *IEEE Transactions On Networking, Vol. 21, No. 2,* April 2013.

[2] . Panagiotis Papadimitriou, Member, IEEE, and Hector Garcia-Molina, Member,IEEE "Data leakageDetection*" IEEE Transactions On Knowledge And Data Engineering, Vol. 23, No. 1,* Jan 2011.

[3] Matha Singhi, Priti Tripathi2 & Renuka Singh3 " Data Leakage Detection" *Undergraduate Academic Research Journal (UARJ), ISSN: 2278 – 1129, Volume-1, Issue-3,4,* 2012.

[4] Priyanka Barge, 1 Pratibha Dhawale, 2 Namrata Kolashetti3 " A Novel Data Leakage Detection**"** *International Journal of Modern Engineering Research (IJMER) www.ijmer.com Vol.3, Issue.1, pp-538-540 ISSN: 2249-6645* , Jan-Feb. 2013

[5] Xianping Wu, Huy Hoang Ngo, Phu Dung Le and Bala Srinivasan *Faculty of Information Technology, Monash University, Victoria, 3145, Australia* Huamei Qi *School of Information Science and Engineering, Central South University, Changsha 410083, P.R. China "*Novel Hybrid Group Key Agreement for Sensitive Information Systems" *Journal of Convergence Information Technology Volume 5, Number 1, February 2010 .doi: 0.4156/jcit.vol5.issue1.9*

[6] M.Vijayakumar#1 V.Priya Dharshini#2 Dr.C.Selvan#3 "A New Key Management Paradigm for Fast Transmission in Remote Co-operative Groups "International Journal of Computer Science and Mobile Computing *A Monthly Journal of Computer Science and Information Technology ISSN 2320–088X IJCSMC, Vol. 3, Issue. 2, February 2014, pg.197 – 201 research article.*

[7] Mrs.K.Sudha 1, Mr. J.Prem Ranjith2, Mr. S.Ganapathy3, Mr.S.Ranjith Sasidharan4 " secure transmission over remote group: a new key management prototype" *IPASJ International Journal of Computer Science (IIJCS)* Volume 2, Issue 1, January 2014 ISSN 2321-5992.

[8] Sandip A. Kale1, Prof. S.V.Kulkarni2 "Data Leakage Detection" *International Journal of Advanced Research in Computer and Communication Engineering Vol. 1, Issue 9,* ISSN (Print) : 2319-5940 ISSN (Online) : 2278-1021 *November 2012.*

[9]. Rekha Jadhav, "Data Leakage Detection" *International Journal of Computer Science & Communication Networks,Vol 3(1), 37-45 37* ISSN:2249-5789.

[10] Anusha.Koneru#1 , G.Siva Nageswara Rao#2, J.Venkata Rao#3 Guntur, Andhra Pradesh, India "Data Leakage Detection Using Encrypted Fake Objects"*International Journal of P2P Network Trends and Technology- Volume3 Issue2- 2013* ISSN: 2249-2615.