ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

A Hybrid Broadcast Encryption and Group Key Management System for Simple and Cost Effective Communication

G. Rahul
B.Tech Student,
Depatment of CSE,
TKR College of Engineering & Technology.

K. Ranjith
B.Tech Student,
Depatment of CSE,
TKR College of Engineering & Technology.

K. Shirisha
Guided,
Depatment of CSE,
TKR College of Engineering & Technology.

Abstract:

Wireless mesh networks function as regular wireless networks, but with significant differences. Mesh networks decentralize the infrastructure required to maintain a network by making each node, or computer, pull double-duty as a user and a router of Internet traffic. This way, the network exists as an organic and self-managed entity capable of servicing a varying number of users.

People joining or using wireless mesh networks for business purposes should be aware, however, that this interface isn't without security problems.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.

Keywords:

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

Introduction:

Wireless mesh architecture is a first step towards providing cost effective and dynamic high-bandwidth networks over a specific coverage area. Wireless mesh infrastructure is, in effect, a network of routers minus the cabling between nodes. It's built of peer radio devices that don't have to be cabled to a wired port like traditional WLAN access points (AP) do. Mesh infrastructure carries data over large distances by splitting the distance into a series of short hops. Intermediate nodes not only boost the signal, but cooperatively pass data from point A to point B by making forwarding decisions based on their knowledge of the network, i.e. perform routing. Such an architecture may, with careful design, provide high bandwidth, spectral efficiency, and economic advantage over the coverage area.

Wireless mesh networks have a relatively stable topology except for the occasional failure of nodes or addition of new nodes. The path of traffic, being aggregated from a large number of end users, changes infrequently. Practically all the traffic in an infrastructure mesh network is either forwarded to or from a gateway, while in ad hoc networks or client mesh networks the traffic flows between arbitrary pairs of nodes.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Remote cooperative groups using encrypted transmission. Examples can be found in access control in remote group communication arising in wireless mesh networks, mobile ad hoc networks, vehicular ad hoc networks, etc. WMNs have been suggested as a promising low cost approach to provide last-mile high-speed Internet access. A typical WMN is a multi hop hierarchical wireless network. The top layer has high-speed wired Internet entry points. The second layer is made up of stationary mesh routers serving as the multi-hop backbone to connect to each other and Internet via longrange high-speed wireless techniques.The bottom layers include a large number of mobile network users. The end users access the network either by a direct wireless link and through the chain of other peer users leading to a nearby mesh routers; then the router further connects to remote users through the wireless backbone and Internet. Security and privacy issues are of utmost concern in pushing it to the success of WMNs for their wide deployment and for supporting service oriented applications. For instance, a manager on his way to holiday may want to send a confidential email to some staff of her company via WMNs, so that the intended staff members can read the email with their mobile devices (laptops, PDAs, smart phones, etc.). Due to distributed nature and intrinsically open of WMNs, it is essential to enforce access control of sensitive information to cope with both eavesdroppers and malicious attackers.

EXISTING SYSTEM:

WMNs have been recently suggested as a promising low-cost approach to provide last-mile high-speed Internet access. A typical WMN is a multihop hierarchical wireless network. The top layer consists of high-speed wired Internet entry points. The second layer is made up of stationary mesh routers serving as a multihop backbone to connect to each other and Internet via long-range high-speed wireless techniques. The bottom layer includes a large number of mobile network users. The end-users access the network either by a direct wireless link or through a chain of other peer users leading to a nearby mesh router; the router further connects to remote users through the wireless backbone and Internet. Security and privacy issues are of utmost concern in pushing the success of WMNs for their wide deployment and for supporting service-oriented applications.

For instance, a manager on his way to holiday may want to send a confidential e-mail to some staff of her company via WMNs, so that the intended staff members can read the e-mail with their mobile devices (laptops, PDAs, smart phones, etc.). Due to the intrinsically open and distributed nature of WMNs, it is essential to enforce access control of sensitive information to cope with both eavesdroppers and malicious attackers.

DISADVANTAGES OF EXISTING SYSTEM:

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.

PROPOSED SYSTEM:

Our contribution includes three aspects. First, we 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.Second, we 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.

The new approach is a hybrid of group key agreement and public-key broadcast encryption.Third, we present 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.

ADVANTAGES OF PROPOSED SYSTEM:

The common problem is to enable a sender to securely transmit messages to a remote cooperative group. A solution to this problem must meet several constraints.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

• 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.

• Furthermore, 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.

Modules:

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 cooperativegroups 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 keyencapsulation 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 algorithmand 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 notsend sensitive or critical information outside of the corporate network. The term is also used to describe software products that help a network administrator

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

control what data end users can transfer. 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.

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 complexityanalysis, 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 withaccess 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 leakageprevention 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 byother 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 communicationamong 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, April2013.

[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 Cooperative Groups "International Journal of Computer Science and Mobile Computing A Monthly Journal of Computer Science andInformation Technology ISSN 2320–088X IJCSMC, Vol. 3, Issue. 2, February 2014, pg.197 – 201 research article.

[7]Mrs.K.Sudha1,Mr.J.PremRanjith2,Mr.S.Ganapathy3, Mr.S.Ranjith Sasidharan4 " secure transmission over remote group: a new key management prototype" IP-ASJ International Journal of Computer Science (IIJCS) Volume 2, Issue 1, January 2014 ISSN2321-5992.

[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.