Private Key Management for Data Transfer with Shared Random Secret Key

Mohanavalli .S[#1], Gori Mohamed .J[#2]

[#1]*Student, Computer Science, Mohamed Sathak A.J. College Of Engineering Chennai, India*

[#2]*Assistant Professor, Computer Science, Mohamed Sathak A.J. College Of Engineering Chennai, India*

Abstract *- Network in general refers to a setup in which computers are interconnected and in-turn this allows communication between one another. This paper is based on the key generation and distribution problem in a two-way relay channel, in which there is no direct channel between the key generating terminals. We propose an effective key generation scheme that achieves a substantially larger key rate than that of a direct channel mimic approach. Secure key distribution schemes for group communications allow establishing a secure multi cast communication between a group manager and group members through an insecure broadcast channel. The improved efficiency for key management is realized by periodically refreshing all public private key pairs as well as any multicast keys in all the nodes using only one newly generated function broadcasted by the key generator entity. The article classifies, analyzes and compares the most significant key distribution schemes, by looking at the selective key distribution algorithms, at the pre-distributed secret data management, and at the self-healing mechanisms. It reviews polynomial-based algorithms, exponential arithmetic based algorithms, hash-based techniques, and others. Propose classification of schemes based on the applied cryptographic primitives.*

Keywords - *Secret key preparation, data privacy, selective key distribution algorithms, self healing mechanisms, Hash Message Authentication Code(HMAC)algorithm.*

I. INTRODUCTION

In a network of connected terminals, security is one of the major area of interest. The term network security refers to security of computers against intruders and malicious softwares. The information transmitted and stored in a network terminal must be protected against physical damage and administrative damage. The term internet security refers to the security of data when it is transmitted across internet. Effective network security targets a variety of threats and stops them from entering or spreading on network. Network security is usually handled by a network operator or system administrator who executes the security policy, in which faults can be easily isolated, new devices can be configured and added correctly in a network.

Related work: Insecure mechanisms provided in the existing network almost none of the schemes is suitable for large scale WSN in real-world applications. Existing solutions usually present some trade-off between scheme performance and security level Identifies basic building blocks of the scheme and describes in detail all major types of existing solutions. It also contains a thorough security and efficiency analysis of each solution, and points out issues not identified. It decreases the workload on the Group Manager. It reduces network traffic as well as the risk of user exposure through traffic analysis. It is easier to identify similarities in mechanisms reused in several solutions.

II. LITERATURE SURVEY

A. *Self-Healing Sensor Network Key Distribution Scheme For Secure Communication*

Wireless sensor network (WSN) consists of a large number of small, low cost sensor nodes which have limited computing and energy resources. As the wireless medium is characterized by its lousy nature, reliable communication is difficult to assume in the key distribution schemes. Therefore, self-healing is a good property for key distribution in wireless applications. How to establish secure session keys is one of the central tasks for wireless sensor network communications. General Key distribution schemes for traditional computer networks could not be directly shifted to wireless sensor network environments. A self-healing key distribution scheme enables a large group of sensor nodes to establish a session key dynamically over a lousy wireless network. The main idea of self-healing key distribution scheme is that users are capable to recover lost session keys on their own, without requesting additional transmission from the group manager that saves the additional communication cost over the network and reduces the network traffic, even if during a certain session some broadcast messages are lost due to network faults.

B. *Efficient Self-Healing Key Distribution With Revocation For Wireless Sensor Networks Using One Way Key Chain*

Security of group communication for large mobile wireless sensor network hinges on efficient key distribution and key management mechanism. As the wireless medium is characterized by its lossy nature, reliable communication cannot be assumed in the key distribution schemes. Therefore, self-healing is a good property for key distribution in wireless applications. The main idea of self-healing key distribution scheme is that even if during a certain session some broadcast messages are lost due to network faults, the users are capable of recovering lost session keys on their own, without requesting additional transmission from the group manager. The only requirement for a user to recover the lost session keys, is its membership in the group both before and after the sessions in which the broadcast packets containing the keys are sent. Self-healing approach of key distribution is stateless in the sense that a user who has been off-line for some period is able to recover the lost session keys immediately after coming back on-line. In this paper, we propose two constructions for scalable self-healing key distribution with t revocation capability. The novelty of our constructions are that we apply a different and more efficient self healing mechanism compared to the ones in the literature using one-way key chain.

C. *An Efficient Public Key Trace And Revoke Scheme Secure Against Adaptive Chosen Cipher Text Attack*

We propose a new public key trace and revoke scheme secure against adaptive chosen cipher text attack. Our scheme is more efficient than the DF scheme suggested by Y. Dodis and N. Fazio. Our scheme reduces the length of enabling block of the DF scheme by (about) half. Additionally, the computational overhead of the user is lower than that of the DF scheme; instead, the computational overhead of the server is increased. The total computational overhead of the user and the server is the same as that of the DF scheme, and therefore, our scheme is more practical, since the computing power of the user is weaker than that of the server in many applications. In addition, our scheme is secure against adaptive chosen cipher text attack under only the decision Diffe-Hellman (DDH) assumption and the collision-resistant hash function H assumption, whereas the DF scheme also needs the one-time MAC (message authentication code) assumption.

D. *Self-Healing Key Distribution Schemes For Wireless Networks: A Survey*

The objective of self-healing key distribution is to enable group users to recover session keys by themselves, without requesting additional transmissions from the group manager (GM), even when they miss some broadcast messages. One major benefit of the self-healing key distribution mechanism is the reduction of energy consumption due to the elimination of such additional transmission. Also in some applications, e.g., uni-directional broadcast channel from the GM, the self-healing key distribution mechanism seems to be the ideal solution. Desired features of self-healing key distribution schemes include energy awareness, short broadcast message, efficient user's addition, revocation and so on. A primary challenge is managing the trade-off between providing an acceptable level of security and conserving scarce resources in particular energy which is critical for wireless network operations. Over a decade, a great number of self-healing key distribution schemes have been proposed for establishing a group key amongst a dynamic group of users over an unreliable, or lossy, network. In this paper a comprehensive survey is conducted on the state-of-the-art in the field of self-healing key distribution. First, we clarify the security requirements of self-healing key distribution scheme for their special application environment.

E. *Securing The Border Gateway Routing Protocol*

We analyze the security of the BGP routing protocol, and identify a number of vulnerabilities in its design and the corresponding threats. We then present a set of proposed modifications to the protocol which minimize or eliminate the most significant threats. The innovation we introduce is the protection of the second-to-last information contained in the AS PATH attributes by digital signatures, and the use of techniques developed for detecting loops in path-finding protocols to verify the selected route's path information. With these techniques we are able to secure full path information in near constant space, and avoid the recursive protection mechanisms previously assumed necessary.

III. PROPOSED WORK

The proposed work should satisfy a prospective group key distribution scheme. It should prevent unauthorized user nodes, which are not in group, from learning the group key. The system should be more flexible and can be used in multi-cast networks with centralized management. Key distribution scheme has to provide fresh keys. Functionality of the scheme is decomposed into three separate aspects, namely: selective key distribution mechanism, pre-distributed secret data management and self-healing mechanism, which are used to classify and compare schemes.

The proposed mechanism addresses the required security aspects by the SG system and, at the same time, manages the process in an efficient fashion. The savings in resource consumption as the result of our

mechanism can be used to handle more data delivery and/or to increase the security of the system by refreshing the keys more often, which brings to SG the opportunity to utilize keys of smaller sizes, further reducing resource consumption in the system. Communications security is achieved by message encryption and authentication using shared symmetric secret group key.

A. Architectural Details

The architecture diagram is a pictorial representation of the overall process It begins with the login page when the authentication of the user is successful. The file transmission is made by the sender, where we have provided buttons for selecting the intended user to which the data has to be sent. There is also a button for the key protocol to identify the receiver's authentication. There is a centralized database which stores the keys that are generated randomly. When the user clicks on the login button set of keys are generated for the sender after which the sender can encrypt the data and send it to the receiver.

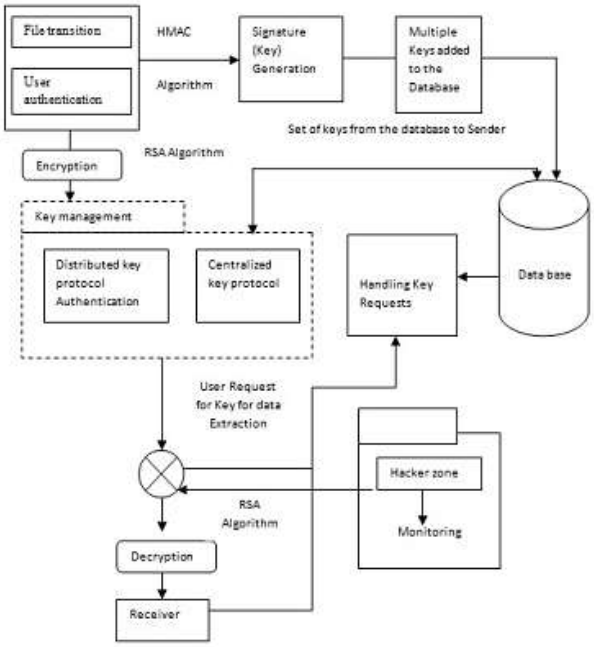

Fig.1 System Model

IV. System Analysis

A detailed study of the system is done by making use of various techniques. Analysis refers to the process of finding facts and details about requirements that are needed for the system development. The data's collected are gathered and then we arrive at the final conclusion. This conclusion is the system function which is the existing system. After making the study we identify the problems and the proposed system is presented to the user.

A. Algorithm Specification

1) RSA algorithm: RSA is a cryptographic algorithm which met the requirements for public-key system, and is widely used for securing sensitive data, particularly when being sent over an insecure network such as the internet. This scheme uses a public key and private key for encryption and decryption techniques.

Key Generation: Whoever wants to receive secret messages creates a public key (which is published) and a private key (kept secret). The keys are generated in a way that conceals their construction and makes it 'difficult' to find the private key by only knowing the public key.

2) HMAC Algorithm: An iterative hash function breaks up a message into blocks of a fixed size and iterates over them with a compression function. For example, MD5 and SHA-1 operate on 512-bit blocks. The size of the output of HMAC is the same as that of the underlying hash function (128 or 160 bits in the case of MD5 or SHA-1, respectively), although it can be truncated if desired.

$$HMAC(K, m) = H((K \oplus opad)||H((K \oplus ipad)|| m))$$

where,
H is a cryptographic hash function,
K is a secret key padded to the right with extra zeroes to the input block size of the hash function, or the hash of the original key if it is longer than that block size,
m is the message to be authenticated,
e.g.,

```
SecretKeySpec key = new
SecretKeySpec((keyString).getBytes("UTF-8"), algo);
Mac mac = Mac.getInstance(algo);
mac.init(key);
byte[] bytes = mac.doFinal(msg.getBytes("ASCII"));
StringBuffer hash = new StringBuffer();
for (int i = 0; i < bytes.length; i++)
{
String hex = Integer.toHexString(0xFF & bytes[i]);
 if (hex.length() == 1)
 {
  hash.append('0');
 }
  hash.append(hex);
 }
```

3) SHA-1 Algorithm: The SHA is used for generating message digest which is used for authentication.SHA-1 is based on MD5. SHA-1 produces a 160-bit (20-byte) hash value known as a message digest. A SHA-1 hash value is typically rendered as a hexadecimal number, 40 digits long.

$W_t = ROTL^1(W_{t-3} \oplus W_{t-8} \oplus W_{t-14} \oplus W_{t-16})$ for $16 \leq t \leq 79$

In which $ROTL^n(x) = (x << n)\ v\ (x >> w - n)$.

B. Module Description

The modules which are to be used in the proposed schemes are:

1) ***Network Authentication:*** In this module, the login process has additional level of security. Apart from user account name and password, when the user has been registered with the database, a set of keys will be generated for more authentication. These keys will provide more security while sending the data from one system to another system. The keys which have generated in the database will act as an onetime password while data transfer.

2) ***Sender/File transmission:*** Sender holds the key values which has been generated by key generation. Protected key gives more security to the data transmission. A set of protected keys are available. The sender should select one key at a time, same key cannot be selected again to send data. The Protected key allows the user to send data to the receiver. The key will be updated while sending data in the network and the file transmission will be processed through Routers and reach the destination (receiver).

3) ***Signature (Key) Generation:*** The set of keys are generated in the database at the time of registration. The keys are generated with the help of HMAC-SHA1 algorithm. Sender holds the key values (signature) which has been generated by key generation. The keys generated by the hmac-sha1 algorithm are the private keys for sending the information from one user to another. The file encryption and decryption is performed by the RSA algorithm.

Signature (Key) Management - We present two new symmetric key approaches to secure mechanism: Pre-key distribution approach, centralized key distribution approach.

Pre-Key distribution - The users are given a substantial number of keys to avoid frequent key update. Periodic rekeying method, the keys are changed at the beginning of each period which is sufficiently long. Where the individual router is responsible for key distribution, and to secure the updates. In the key distribution protocols the center node maintains a set of "k" keys.

Centralized Key Distribution - Where a central authority is responsible for key distribution. In this approach, the cost of signature generation for a router is only one signature, i.e., the route attestation that is added by this speaker. The cost of signature generation is lower. In this approach, the cost of signature generation is low, that each router only needs to add its own signature to the update.

4) ***Hackers Zone:*** The node which is present in the different network or individual system accessing the data in the false name of a node which is present in the router network is called as hackers. The randomly generated key is not allocated to the hacker system.

Monitoring access - Monitoring Access module takes care of the data sending through the network using the key. It accesses the database to check the validation for proper and improper user. It also monitors the hackers if anybody accessing the data, who does not belong to the network.

5) ***Receiver:*** Some of the node is acting as a sender and all the remaining nodes are the receivers. If a node sends a message that includes a signature from each of the keys it has and the receiver verifies the signatures based on the common keys then it can conclude that the message is authentic. The receiver has to request for the key to extract the data. Keys will not be updated at the time of transmission.

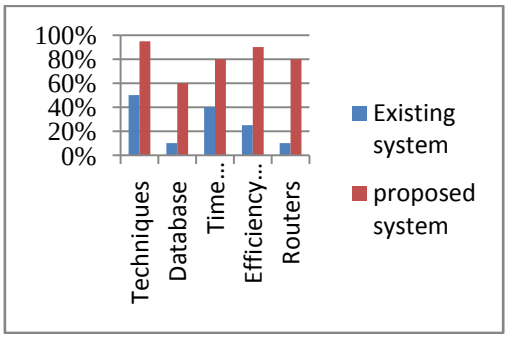

Fig .2 Comparison Graph

V. Conclusion And Future Enhancement

We make three key contributions in this paper. First, we show that the right trade-off between efficiency and security for information could be achieved by adding little bit of trust on routers. We present a new flexible threat model where for any path of length k, at least one router is trustworthy. Second, we present two new symmetric key approaches for securing information: the centralized key distribution approach and the distributed key distribution approach. Third, we evaluated the efficiency of the two approaches with previous approaches for securing the data. The evaluation results show that our approaches are significantly more efficient than previous approaches. Also, we have discussed the

deployment issues and important concerns like key management and interoperability to illustrate the feasibility of our protocols.

REFERENCES

1] Eduru Hariprasad, J.S.V.R.S.Sastry, N. Subhash Chandra, " Vastly Efficient Key Pre Distribution and Authentication scheme for Wireless Sensor Networks." in SSRG-IJCSE, Volume 1, Issue 5, July 2014, IJCSE-V1I7P105.

2] H. Zhou, L. Huie, and L. Lai, *"Key generation in two-way relay wireless channels,"* in Proc. 17th Annu. Conf. Inf. Sci. Syst., Baltimore, MD, USA, Mar. 2013, pp. 1–6.

3] R. Wilson, D. Tse, and R. Scholtz, *"Channel identification: Secret sharing using reciprocity in UWB channels,"* IEEE Trans. Inf. Forensics Security, vol. 2, no. 3, pp. 364–375, Sep. 2007.

4] C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, and N. B. Mandayam, *"Information-theoretically secret key generation for fading wireless channels,"* IEEE Trans. Inf. Forensics Security, vol. 5, no. 2, pp. 240–254, Jun. 2010.

5] L. Lai, Y. Liang, and H. V. Poor, *"A unified framework for key agreement over wireless fading channels,"* IEEE Trans. Inf. Forensics Security, vol. 7, no. 2, pp. 480–490, Apr. 2012.

6] T.-H. Chou, A. M. Sayeed, and S. C. Draper, *"Impact of channel sparsity and correlated eavesdropping on secret key generation from multipath channel randomness,"* in Proc. IEEE Int. Symp. Inf. Theory, Austin, TX, USA, Jun. 2010, pp. 2518–2522.

7] Gori Mohamed .J, M. Mohammed Mohideen, Mrs.Shahira Banu. N, *"E-Mail Phishing - An open threat to everyone,"* International Journal of Scientific and Research Publications, Volume 4, Issue 2, February 2014, ISSN 2250-3153.

8] U. Padmavathi, C.Mohammad Gulzar, " Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage." in SSRG-IJCSE, volume 2 issue 6 June 2015, IJCSE-V2I6P103.

Ms. MOHANAVALLI .S was born in Madurai, in 1993. She received her B.E. degree Computer Science and Engineering from Mohamed Sathak AJ College of Engineering, Chennai, in 2014 and she is pursuing M.E. degree in Computer Science and Engineering from Mohamed Sathak AJ College of Engineering.

Mr. GORI MOHAMED .J was born in Aduthurai, in 1984. He received his B.Tech. degree in information technology from Anna University, Chennai, in 2006 and he received his M.Tech degree from Dr.MGR University in 2008. He started his career as an Assistant Professor in 2007 in C.Abdul Hakeem College of Engineering & Technology, Melvisharam, and worked there till 2011 September. Since September 2011 he has been with Mohammed Sathak.A.J college of Engineering, Chennai, where he is currently an Assistant Professor.