RESEARCH ARTICLE OPEN ACCESS

Resilient Key Sharing Approach Based on Multimode Authentication Scheme

[1]A.Senthilkumar, [2]R.Divya

[1]Asst.professor, Dept.of.Computer science, Tamil University (Established by the Govt.of.Tamilnadu), Thanjavur.

[2]Research Scholar, Dept.of.Computer Science, Tamil University, Thanjavur.

----------**********----------

Abstract:

The history of Information Security begins with the study of computer security. Security concern arises from various parameters to safeguard physical location, hardware and software from the outside threats. The research work carries out essential security needs and adoptions of security policies based on Resilient Key Distribution Mechanisms (RKDM) to safeguard information transmissions over networks. The adoption of sender and receiver whom are called as 'clients' should register themselves initially. The registration work of them clients are maintained in separate databases maintained for them, and whenever each user makes a login request, thereby an individual private key is created by the clients themselves. To know their own authentication, a centralized server which is called as an 'Authentication Server (AS) is maintained to monitor the data transaction of the clients and the application which runs between them. After confirming the registration ,the server issues resilient key (Public keys) for each of the user for their data transactions in the networks. The authentication server issues resilient key only after verification of each client who register themselves within it.

.

Keywords **— Information security, Resilient key distribution mechanisms(RKDM) private key, authentication ,authentication server, resilient key(public keys) ,RSA algorithm ,object set , user set, node awareness ,multimode.**

----------**********----------

I. INTRODUCTION

Authentication is referred as 'User identity who claims any resources in the network'. Authentication plays a key role in preventing unauthorized and corrupted messages to safe the data transmission in wireless networks (WN). For this reason, many authentication schemes have been proposed in literature to provide message authenticity and integrity verification for wireless networks (WNs). Message authentication schemes can largely be divided into two categories: public-key based approaches and symmetric-key based approaches. The symmetric-key based approach requires complex key management, lacks of scalability, and is not resilient to large numbers of node compromise attacks since the message sender and the receiver have to share a secret key. An intruder can compromise the key by capturing a single sensor node. In addition, this method does not work in multicast networks. The idea of this scheme is to implement resilient key sharing based on RSA algorithm which considers secret sharing, where the key sizes are determined initially from 1024 bits.

This approach offers information-theoretic security of the shared secret key when the number of messages transmitted as specified by the algorithm key size. The intermediate nodes verify the authenticity of the message through an evaluation. The message is transmitted along with the Server issued resilient keys. Every nodes in the network can share files to other nodes only after verifying their identities. The Research proposal includes registration module for user registrations, authentication module to verify the users and key sharing and file sharing and secured module where the algorithm is implemented and the node status to identify the awareness of the user which narrates the user, object , the file and all the user's

authentication. The file shared to node and verify the keys and generate the resilient key. The number of local hosts connected in this work remains limited and can be scaled according to the organization or network in future. While achieving compromise resiliency, flexible-time authentication and source identity protection.. Both theoretical analysis and simulation results demonstrate that our proposed scheme is more efficient than the RSA algorithms under comparable security levels. The advancement of wireless communication technologies and rooted computing, are being widely adapted into many applications through networks and many active researches on related subject are being carried out. Several nodes are connected to build the wireless networks. The large numbers of devices are the interconnected to form a network. The WN make use of a number of nodes within or neighboring the area of event to not only collect and integrate but also process and relay the information. The . registration of clients or data transaction but also confirms one of the security policies named Authentication.

PROBLEM DESCRIPTION

Existing system:

”The existing system based on RSA has not fixed network limitation ’’.the symmetric-key based approach needs complex key management, lacks of scalability, and is not resilient to large numbers of node compromise attacks since the message sender and the receiver have to share a secret key. The sender generate message Authentication Code (MAC) for each transmitted message by using the shared key. However, for this basis, the authenticity and integrity of the message can only be checked by the node with the secret key, which is usually shared by a group of nodes. The existing system provides the use of RSA algorithm with not specifying the user awareness status, which is difficult for any user to locate the identity this research proposal solves the issues by Identifying the user , node of the file to be kept secret. For a public-key based approach, each message is transmitted along with the digital signature of the message which is generated using the sender’s private-key. Every intermediate forwarder and the final receiver can authenticate the message using the sender’s public-key. The drawbacks of the public-key based approach is the high computational overhead.

PROBLEM DEFINITION

User authentication plays a key role in preventing unauthorized and corrupted messages to safe the data transmission in wireless networks (WN). For this reason, many authentication schemes have been proposed in literature to provide message authenticity and integrity verification for wireless networks (WNs). user authentication schemes can largely be divided into two categories: public-key based approaches and symmetric-key based approaches. In this research proposal on a server called a “Resilient key”.

The symmetric-key based approach requires complex key management, lacks of scalability, and is not resilient to large numbers of node compromise attacks since the message sender and the receiver have to share a secret key. The shared key is used by the sender to generate a message authentication code for each transmitted message. The authenticity and integrity of the message can only be verified by the node with the shared secret key, which is generally shared by a group of nodes. . The here public key server as authentication server, issues resilient keysecret RSA based message authentication scheme. The idea of this scheme is similar to secret sharing, where the is determined by the degree of the RSA This approach offers information-theoretic security of the shared secret key when the number of messages transmitted by user. The intermediate nodes verify the authenticity of the message through a RSA evaluation.

3.2 PROPOSED SYSTEM

For the public-key based approach, each message is transmitted along with the digital signature of the message generated using the sender’s private key. Every intermediate forwarder and the final receiver can authenticate the message using the sender’s public key. One of the limitations of the public-key based scheme is the high computational overhead. The recent progress on RSA algorithm shows that the public key schemes can be more advantageous in terms of computational complexity, memory usage, and security resilience, since public-key based approaches have a simple and clean key

management. Our scheme enables the intermediate nodes to authenticate the message so on. In this work are used five modules that can used Registration, authentication, file sharing ,node status and last one performance analysis . Registration module suggests the client or node based on their own login name or password. , authentication server checks the secret key of the user name , file sharing this module file or any application is chosen it going to be shared. Node status the node in idle or busy state or secured. Both theoretical analysis and simulation results demonstrate that our proposed scheme is more efficient than the RSA algorithms used encryption, decryption security levels**4.**

METHODOLOGY

Design steps:

1. Let the nodes be assumed as n1, n2,n3
2. Server is notated as 'AS1'
3. Given the nodes initialize then according to their private key assumptions say ln1,pw1 for node 'n1' ln2,pw2 for node'n2', ln3,pw3 for node 'n3'.
4. Repeat the initialization procedure if added up clients are there in network.
5. Call the authentication procedure for the initial nodes
6. Here As1 verifies for authentication by the nodes private key ln1,ln2 for all clients.
7. Authentication server rejects the invalid node if they do not possess secrete keys
8. Call resilient key authentic procedure, let the resilient key be R1,R2… Rn
9. Allocate resilient key r1 for n1, r2 for n2 and r3 for n3 ;
10. Allocate until the resilient keys of authentic server ends up
11. Call the file sharing procedure for security implementations
12. Let the file, or node or application to run on node 1 be initialized say f1 = 1, a1 =1, n1=1,n2=1 and so on
13. Let the file n1 =f1 (file f1 is in use) by the note n1
14. Call the security procedure call sec();
15. Calculate the private key &public key computations.
16. Call the encrypt procedure if file is in node 1 or application is in node 1
17. Call the decrypt procedure and return back to produce plaintext
18. Check the node status procedure to print the usernames, network boundaries , key sizes and other too
19. Call the perform analysis procedure for all files, user and applications
20. Thus multimode authentication schemes are utilized in this research work.

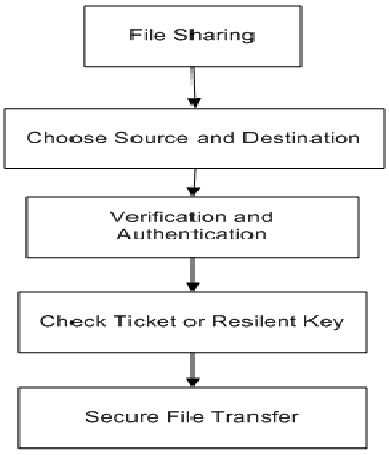
1) Registration:

Registration module suggests the clients or node registration based on their own login name or password. Initially it occurs for a single user and for a single receiver and updates to more no of users at the end. The login name or password generated is assumed to be their secret key.

2) Authentication Module:

In the authentication module, the authentication server checks the secret key of the user namely (l name, pw) and validates the user. This can be a repeated process for additional clients also say node2 or node3 and so on.

In the authentication module (Sub module) as another part, the server provides or issues Resilient keys which is the Public key to the registered Users. The server database maintains all the **registered users who are validated** based on their private key (l name, pw) and the public key (resilient key1….resilient key2) up to the node limit.



3)File Sharing:

In this module, the file or any application say f1 or a1 is chosen. If it is going to be shared, the file must be secured USING RSA Algorithm before sharing the file, the clients records, RSA algorithm the security for authentication purpose.

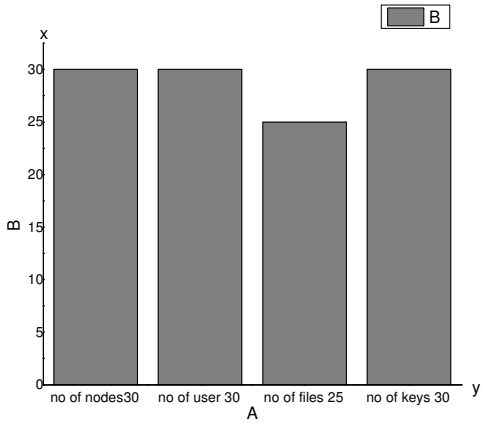
For example, if a content or a word is chosed in a sample file, it must be encrypted using RSA formula, $c = m^e \bmod n$ where m is the plaintext, e to the power and must be decrypted $m = c^d \bmod n$.

4)Node Status:

The RSA algorithm proposes the study of network security but it does not analyzed the study of network limitation, but the research work proposed suggests the network boundary since nodes or clients must be framed in a boundary to achieve information security very fastly. This can be scalable in future according to the organizational needs. In this module, the work checks which user say u1, is viewing which file, say f1 and up to which network boundary say u_n , is in what status [the node is in idle state or busy state or secured].

5)Results Analysis and Performance Efficiency:

Performance analysis module suggests the research work carried to how much extent or an average the user or file or nodes got secured. For this the nodes can be arranged in a linear fashion next to next. The files secured based on the keys must be matched up with the nodes. The nodes with file must be equally secured proportionally to the maximum limit. For example if node1 checks 5 files means (1: 5) , secondly node 2 checks 10 files(1:10) secured or the contents secured.



7. CONCLUSION

In this research proposal analysis the total number of client with the RSA algorithm implement the secure files. In we used five modules which initially login the client of the look successfully concludes the concept Of authentication principle in a elaborated manner of an is provided in a multimode fashion. User authentication scheme. improve the security in wireless Networks. An efficient Source anonymous message authentication schemeAn intermediate nodes are authenticate and allow to transmit a message, does not have the network boundary limitation that is unlimited number of messages are secret key verified than server compare based scheme Proposed scheme is more efficient than the RSA-based scheme such as memory and security .

8. FUTURE ENHANCEMENT

The number of nodes at the initial stage can be limited. in future, the nodes of the research proposal can be extended to maximum number of nodes.

Security analysis showed that the proposed protocol fulfils the security benefits that a secure user authentication scheme should provide and can resist to various possible attacks such as SSL/TLS man-in-the-middle attack, offline dictionary and brute force attack, and message modification or insertion attack. Future scope in this work is to investigate the possibility of using cloud computing technology to improve the portability and recovery of our scheme. We also plan to provide a secure design for user's session management. While the proposed scheme needs public key cryptography, then we will further focus on elliptic curve cryptography which offers faster computations and less power use. The application uses can be enlarged as per any organization wish with regard to number of nodes increased to scale in the future.

7.REFERENCES

[1]B. Pang, L. Lee, and S. Vaithyanathan, "Thumbs up? Sentiment classification using machine learning techniques," in *Proc.EMNLP*, Philadelphia, PA, USA, 2002, pp. 79–86.

[2]B. Snyder and R. Barzilay, "Multiple aspect ranking using the good grief algorithm," in *Proc.*

HLT-NAACL, New York, NY, USA, 2007, pp. 300–307.

[3]L. Tao, Z. Yi, and V. Sindhwani, "A non-negative matrix tri-factorization approach to sentiment classification with lexical prior knowledge," in *Proc. ACL/AFNLP*, Singapore, 2009, pp. 244–252.

[4]T. Wilson, J. Wiebe, and P. Hoffmann, "Recognizing contextual polarity in phrase-level sentiment analysis," in *Proc. HLT/EMNLP*, Vancouver, BC, Canada, 2005, pp. 347–354.

[5]J. Yu, Z.-J. Zha, M. Wang, and T. S. Chua, "Aspect ranking: Identifying important product aspects from online consumer reviews," in *Proc. ACL*, Portland, OR, USA, 2011, pp. 1496–1505.

[6] Bo Pang1 and Lillian Lee2Foundations and Trends in Information Retrieval Vol. 2, Nos. 1–2 (2008) 1–13

[7] S. Zhou, S. Zhang, and G. Karypis (Eds.): ADMA 2012, LNAI 7713, pp. 577–588, 2012.c_Springer-Verlag Berlin Heidelberg (2012)

[8] Baccianella, Stefano, Andrea Esuli, and Fabrizio Sebastiani. (2010).SentiWordNet 3.0: An enhanced Lexical resource for sentiment analysis and opinion mining. In Proceedings of the Seventh Conference on International Language Resources and Evaluation (LREC'10), pages 2200–2204, Valletta.

[9] Kessler, B., Nunberg, G., and Schutze, H. 1997. Automatic Detection of Text Genre. In Proc. of 35th ACL/8th EACL.