International Journal For Technological Research In Engineering
Volume 2, Issue 8, April-2015 *ISSN (Online): 2347 - 4718*

EFFICIENT KEY VERIFICATION AND ONE TIME SUPERVISION MECHANISM FOR PEER TO PEER NETWORKS

Uma Shanakar Prasad[1], Shravan Kumar[2], Dr.K.P.Kaliyamurthie[3]
[1,2]B.Tech Final Year, Department of Computer science Engineering, Bharath University, Chennai.
[3]Professor & Head, Department of Computer science Engineering, Bharath University, Chennai.

ABSTRACT: We propose an efficient key generation theme that achieves a considerably larger key rate than that of an immediate channel mimic approach. in contrast to existing schemes, there's no want for the key generating terminals to get related to observations in our theme. Secure key distribution schemes for cluster communications permit establishing a secure multi forged communication between a bunch manager and group members through an unreliable broadcast channel. The improved potency for key management is accomplished by sporadically refreshing all public non-public key pairs additionally as any multicast keys all told the nodes victimization just one freshly generated perform broadcasted by the key generator entity. The article stratify, peruse and collate the foremost important key distribution schemes, by gazing the selective key distribution algorithms, at the predistributed secret knowledge management, and at the self-healing technique. It reviews polynomial-formed algorithms, exponential arithmetic based algorithms, hash-rooted techniques, and others. Propose classification of schemes supported the applied cryptologic primitives.

I. INTRODUCTION

In the field of networking, the realm of network security consists of the provisions and policies adopted by the network administrator to stop and monitor unauthorized access, misuse, modification, or denial of the pc network and network-accessible resources. The main objective of our project is to boost the network security. because the network usage will increase day by day, the quantity of threats display by intruders and hackers will increase. to beat these threats and knowledge loss and supply a secure network that overcomes these threats we've to supply a complicated safety technique. therefore this project proposes a mechanism is to advertise the routing path info for informatics prefixes. Improve the protection that versatile communication infrastructures which offer a various set of operations. Improvement in signature verification and signature generation. In the extant system the command and management server could be a single system, this improves the probabilities of being attacked by the hacker by observance the quantity of traffic round the command and management server. during this project we have a tendency to overcome this defect by dynamically ever-changing the server from time to time. Secure cluster communication depends on secure and sturdy distribution of cluster keys [1]. One trigonal key noted solely to the cluster members will effectively shield a multicast group[2]. However, solely legitimate users ought to have access to the cluster communication so as to realize privacy. so the cluster key (session key) should be updated on every occasion once new users be part of or recent users leave the cluster and firmly decentralised to the prevailing members of the cluster. this is often noted as cluster rekeying. The recently joint users mustn't be ready to derive the previous cluster keys, although they're ready to derive future cluster keys with afterwards distributed keying info. Similarly, the revoked users mustn't be ready to derive the longer term session keys, although they're ready to cypher the previous session keys with antecedently distributed keying info. Providing authentication theme and providing a key management [3] protocol square measure the desired first steps of coming up with and implementing system security in SG[4] according to recent work key management mechanisms for securing the good grid ought to be supported by Public Key Cryptography (PKC)[5] and a Public Key Infrastructure (PKI), as they need lower key management prices than those of trigonal cryptography[6].

II. RELATED WORKS

Wireless sensing element network (WSN) consists of an oversized variety of little, low value sensing element nodes that have restricted computing and energy resources. because the wireless medium is characterised by its lousy nature, reliable communication is tough to assume within the key distribution schemes. Therefore, self-healing could be a sensible property for key distribution in wireless applications. a way to establish secure session keys is one in every of the central tasks for wireless sensing element network communications. General Key distribution schemes for ancient pc networks couldn't be directly shifted to wireless sensing element network environments. A self-healing key distribution theme permits an oversized cluster of sensing element nodes to ascertain a session key dynamically over an unreliable, or lousy wireless network. the most plan of self-healing key distribution theme is that users square measure capable to recover lost session keys on their own, while not requesting further transmission from the cluster manager that saves the extra communication value over the network and reduces the network traffic, although throughout an exact session some broadcast messages square measure lost owing to network faults. In the paper the author planned a brand new self-healing key distribution theme. The planned theme permits an oversized and dynamic cluster of users to ascertain a session key for secure communications over an unreliable wireless network. The theme conjointly

permits a user to recover, from one broadcast message. The long personal key schemes square measure provided by Staddon J. and Blundo C.[7,] [8]. However, they are doing not properly suitable sensible applications owing to the terribly restricted communication resources. the private key may be reused with none alternation[9.] theme planned up here has reserved forward security and backward security, that square measure crucial properties for cluster key distributions. The Border entry Protocol (BGP), that is employed to distribute routing info between autonomous systems(ASes), could be a vital part of the Internet's routing infrastructure. it's extremely at risk of a spread of malicious attacks, owing to the dearth of a secure suggests that of collateral the believability and legitimacy of BGP management traffic. Sir Leslie Stephen Kent in his paper describes a secure, scalable, deployable design (S-BGP) for AN authorization and authentication system that addresses most of the protection issues related to BGP. this paper provides a comparison of this design to different approaches that are planned, analyzes the performance implications of the planned countermeasures, and addresses operational problems. Ratul mahajan in his paper bestowed the primary quantitative study of BGP misconfiguration. Over a 3 week amount, he analyzed routing table advertisements from twenty three vantage points across the web backbone to observe incidents of misconfiguration. for every incident he polled the ISP operators concerned to verify whether or not it absolutely was a misconfiguration, and to be told the explanation for the incident. he conjointly actively probed the web to work out the impact of misconfiguration on property. In his paper he examined another supply of unreliability: the misconfiguration of the routers that talk BGP.he knew from varied studies of extremely reliable systems, like craft, bank databases, and therefore the telephone network, that human operator error will account for 20-70% of system failures. These studies have shown that as systems become more reliable, the human issue becomes more and more vital to overall responsibleness. he expected a similar to be true of the web. There's substantial anecdotal proof that BGP configuration errors do occur, with serious consequences. Chong Hee KIM planned a brand new public key trace and revoke theme secure against adjustive chosen ciphertext attack. His theme is a lot of economical than the DF theme steered by Y. Dodis and N. Fazio. His theme reduced the length of sanctioning block of the DF theme by (about) [half]. in addition, the procedure overhead of the user was not up to that of the DF scheme; instead, the procedure overhead of the server was augmented. the overall procedure overhead of the user and therefore the server was a similar as that of the DF theme, and so, his theme was a lot of sensible, since the computing power of the user was weaker than that of the server in several applications. A paper was planned by ratna dutta that explains Security of cluster communication for giant mobile wireless sensing element network hinges on economical key distribution and key management mechanism. because the wireless medium is characterised by its lossy nature, reliable communication can't be assumed within the key distribution schemes. Therefore, self-healing could be a sensible property for key distribution in wireless applications. In his paper he planned 2constructions for scalable self-healing key distribution with revocation capability. The novelty of his constructions square measure that he applied a unique and a lot of economical self healing mechanism compared to those within the literature exploitation unidirectional key chain. His planned key distribution mechanism considerably improves the communication and computation prices over the previous approaches with none increase within the storage complexness.

Donggang Liu in his paper bestowed the self-healing key distribution approach (with revocation capability) that was developed by staddon [17]. The technique by staddon uses secret sharing [16]supported two dimensional polynomials to distribute cluster keys, sanctioning cluster members to recover lost session cluster keys as long as they need received one broadcast rekey message before and one once the on top of session. Compared with the approaches mentioned earlier, an advantage of each and his techniques was that the computation, communication, and storage overheads needed to revoke cluster members and reach self-healing capability are freelance of the cluster size, and so appropriate for terribly massive teams. though this paper had several advantage compared to others it has some disadvantages that it absolutely was not appropriate for giant wide scale network.

Table 1
Comparision table for various methods/technique used

Title	Algorithm /technique	Advantages	disadvantages
Sensor network key distribution scheme[10]	key distribution	easy maintenance, low costs, high scalability.	*reliable communication is difficult .*
Secure border gateway protocol[11]	Route Propagation Algorithm	Maintain data more securely	cause problems such as misdelivery .
Understanding BGP misconfiguration[12]	Cumulative distribution function	Network traffic is reduced .	Increases routing load
Self healing key distribution [13]	self-healing mechanism	Can recover lost session keys	Packet loss and collusion attack
Pubic key trace [14]	Hmac	secure against adaptive chosen ciphertext attack	Implementation cost is high
Group key distribution with revocation[15]	Group key distribution	reduce the broadcast message size in situations.	no network infrastructure support,,not suitable for wsn.

III. SYSTEM DESIGN

In this section we introduce our proposed efficient key management scheme based on PKI for peer to peer networks in which Functionality of the scheme is decomposed into three separate aspects, namely: selective key distribution mechanism, predistributed secret data management and self-healing mechanism, which are used to classify and compare schemes. We introduce a three-dimensional classification, based on each aspect of the scheme separately, which allows

for more flexibility for secure transmission of data in which Communications security is achieved by message encryption and authentication using shared symmetric secret group key.

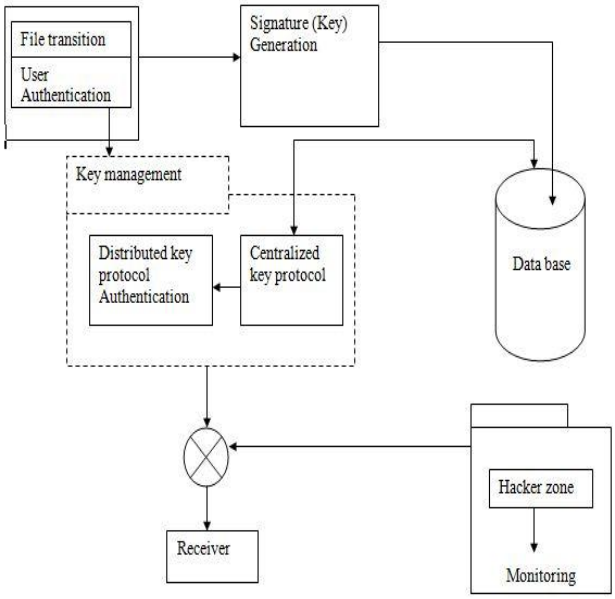

FIG: 2 OVERVIEW ARCHITECTURE OF OUR SYSTEM.

IV. SYSTEM MODULE:

There are totally five modules used in our project which is listed below. Each module has specific usage in the project and is description is given below followed by the list of modules.

1. Login /New User:

In this module, the login process itself has lots of security. Usually the user account name and appropriate password of that account is enough to do the validation and login process, but here some more actions are given to make more security during the login process. New User Creation process entitled that to collect some of the details to maintain the file transfer/Key Management

2. Sender/File Transmission:

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 file search process is used to select the file to be send.The keys which have generated in the database will act as a onetime password while data transfer.

3. Signature (Key) Generation:

Sender holds the key values (signature) which has been generate by key generation. The keys are in two categories private, public to give more security to the data transmission. The private key allows sending the selected data to the particular location or system. The public key allows sending to all users whom all are currently available in the network. And the file transmission can be able, to process through Routers and reached the destination(receiver).

4. Signature (Key) Management :

we have added two new symmetric key approaches to secure mechanism: Pre-key distribution approach, centralized key distribution approach.

4.1. 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, to secure the updates. In the key distribution protocols the center node maintains a set of "k" keys.

4.2. Centralized Key Distribution:

In this step a central authority is liable 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. During this approach, the value of signature generation is low, that each router only needs to add its own signature to the update.

5 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.

5.1Monitoring 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 any body accessing the data, which does not belong to the network.

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.

V. ALGORITMS USED

RSA Algorithm:

RSA is one in all the primary practicable public-key cryptosystems and is wide used for secure knowledge transmission. In such a cryptosystem, the encoding secret is public and differs from the cryptography key that is unbroken secret. In RSA, this spatiality relies on the sensible problem of factorisation the merchandise of two giant prime numbers, the factorisation drawback. RSA involves a public key and a personal key. the general public key may be far-famed byeverybody and is employed for encrypting texts. texts encrypted with the normal general key will solely be decrypted in an exceedingly affordable quantity of your time victimization thepersonal key. The keys for the RSA rule area unit generated the subsequent way:

Choose two well defined prime intezers p and Q. For security functions, the integers p and Q ought to be chosen willy-nilly, and may be of comparable bit-length. Prime integers may be expeditiously found employing a property check. Compute n = pq. n is employed because the modulus for each the general public and personal keys. Its length, typically expressed in bits, is that the key length.

Compute φ(n) = φ(p)φ(q) = (p − 1)(q − 1) = n - (p + Q -1), wherever φ is Euler's totient perform.

Choose associate number e such one < e < φ(n) and gcd(e, φ(n)) = 1; i.e., e and φ(n) area unit co prime.

e is discharged because the public key exponent.

e having a brief bit-length and little overacting weight ends up in additional economical encoding– most typically 216 + one = sixty five,537. However, abundant smaller values of e (such as 3) are shown to be less secure in some settings.

Determine d as d ≡ e−1 (mod φ(n)); i.e., d is that the reciprocal of e (modulo φ(n)).

This is additional clearly expressed as: solve for d given d.e ≡ one (mod φ(n))

This is commonly computed victimization the extended geometrician rule. victimization the pseudo code within the standard integers portion, inputs a and n correlate to e and φ(n), severally. d is unbroken because the personal key exponent.

HMAC Algorithm:

In cryptography, a keyed-hash message authentication code (HMAC) may be a specific construction for conniving a message authentication code (MAC) involving a crypto graphical hash perform together with a secret crypto graphical key. like any waterproof, it should be accustomed at the same time verify each the information integrity and the authentication of a message. Any crypto graphical hash perform, like MD5 or SHA-1, is also employed in the calculation of associate HMAC; the ensuing waterproof rule is termed HMAC-MD5 or HMAC-SHA1 consequently. The crypto graphical strength of the HMAC depends upon the crypto graphical strength of the underlying hash perform, the dimensions of its hash output, and on the dimensions and quality of the key. A repetitive hash performs breaks up a message into blocks of a set size and iterates over them with a compression perform. As an example, MD5 and SHA-1 care for 512-bit blocks. the dimensions of the output of HMAC is that the same as that of the underlying hash perform (128 or a hundred and sixty bits within the case of MD5 or SHA-1, respectively), though it may be truncated if desired.

VI. VI.EVALUTION

Though a number of techniques are used earlier for secure transmission of data we find some drawbacks that Security will be the problem while transferring the data from one system to another in the network due to the pattern recognition system. The hackers are extracting the secret key in between the data transfer in the network. so in this paper our proposed scheme overcome this drawbacks as Self-healing group key distribution schemes can be used in multicast networks with centralized management, which are established over an unreliable broadcast channel, such as system to systems, and enclosed networks, cellular networks and wireless networks. Communication security is achieved by message encryption and authentication using shared symmetric secret group key. our proposed system is suitable for WSN and has advantages as Individualized encryption Robust network connectivity, Efficiency is increased., Hacker cannot easily detect the server. And The proposed system is harder to monitored, hijacked and shutdown.

VII. CONCLUSION

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 the 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 to 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 to securing 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 protocol.

REFERENCES

[1] 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.

[2] 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.

[3] 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.

[4] 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.

[5] 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.

[6] A. Sayeed and A. Perrig, "Secure wireless communications: Secret keys through multipath," in Proc. IEEE Int. Conf. Acoustics, Speech, Signal Process., Las Vegas, NV, USA, Apr. 2008, pp. 3031–3016.

[7] Blundo C., D'Arco P., Santis A., and Listo M., Design of self-healing key distribution schemes, Design Codes Cryptography, 32, 15- 44 (2004

[8] Staddon J., Miner S., Franklin M., Balfanz D., Malkin M., and Dean D., Self-healing key distribution with revocation, IEEE Symposium Security Privacy, 224-240 (2002)

[9] Dutta R. and Mukhopadhyay S., Improved self-

healing key distribution with revocation in wireless sensor network, Wireless Communication Networking, 2963-2968 (2007) ..

[10] Patel Jay Kumar Shantilal " Self-Healing Sensor Network Key Distribution Scheme for Secure Communication"158-161,2013

[11] Stephen Kent, Charles Lynn, and Karen Seo" Secure Border Gateway Protocol (S-BGP).

[12] Ratul Mahajan ,David Wetheral,l Tom Anderson.."understanding BGP misconfiguration..

[13] Ratna Dutta, Ee-Chien Chang, and Sourav Mukhopadhyay3 Efficient Self-healing Key Distribution with Revocation for Wireless Sensor Networks UsingOne Way Key Chains"

[14] Chong Hee KIM, Yong Ho HWANG, and Pil Joong LEE" An E±cient Public Key Trace and Revoke Scheme Secure against Adaptive Chosen Ciphertext Attack"

[15] Donggang Liu, Peng Ning, Kun Sun"Efficient SelfHealing Group Key Distribution with Revocation Capability"

[16] A. Shamir. How to share a secret. Communications of the ACM, 22(11):612–613, 1979.

[17] J. Staddon, S. Miner, M. Franklin, D. Balfanz, M. Malkin, and D. Dean. Self-healing key distribution with revocation.In Proc. of 2002 IEEE Symp. on Security and Privacy, pages 224–240, 2002.

