IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 2, Ver. I (Mar-Apr. 2014), PP 06-08
www.iosrjournals.org

Multiple Routing Configurations for Fast IP Network Recovery Using AES Algorithm

P.Lokana, P.Mohanambal,A.Manjula
Department of Computer Science, SNR Sons College, Coimbatore, India.

Abstract: *Internet takes an increasingly central role in our communications infrastructure, the slow convergence of routing protocols after a network failure becomes a growing problem. To assure fast recovery from link and node failures in IP networks, we present a new recovery scheme called Multiple Routing Configurations (MRC). Our proposed scheme guarantees recovery in all single failure scenarios, using a single mechanism to handle both link and node failures, and without knowing the root cause of the failure. MRC is strictly connectionless, and assumes only destination based hop-by-hop forwarding. MRC is based on keeping additional routing information in the routers, and allows packet forwarding to continue on an alternative output link immediately after the detection of a failure. It can be implemented with only minor changes to existing solutions. In this paper we present MRC, and analyze its performance with respect to scalability, backup path lengths, and load distribution after a failure. We also show how an estimate of the traffic demands in the network can be used to improve the distribution of the recovered traffic, and thus reduce the chances of congestion when MRC is used. To provide security for data transmission algorithm used is Advanced Encryption Standard(AES).*

Keywords; *AES, Backup Configuration, Weight Optimization Load distribution, Avoid Congestion*

I. INTRODUCTION

The main idea of MRC is to use the network graph and the associated link weights to produce a small set of backup network configurations. The link weights in these backup configurations are manipulated so that for each link and node failure, and regardless of whether it is a link or node failure, the node that detects the failure can safely forward the incoming packets towards the destination on an alternate link. MRC assumes that the network uses shortest path routing and destination based hop-by-hop forwarding. Cryptography is the science of information and communication security.

Cryptography is the science of secret codes, enabling the confidentiality of communication through an insecure channel. It protects against unauthorized parties by preventing unauthorized alteration of use.The packets are encrypted and decrypted using AES algorithm and transmitted.

II. PROPOSED SYSTEM

- Multiple Routing Configurations (MRC) is a proactive and local protection mechanism that allows recovery in the range of milliseconds.
- MRC allows packet forwarding to continue over preconfigured alternative next-hops immediately after the detection of the failure
- Using backup configuration algorithm it takes up the backup of nodes and links .
- Using MRC as a first line of defense against network failures, the normal IP convergence process can be put on hold.
- The shifting of traffic to links bypassing the failure can lead to congestion and packet loss in parts of the network. This limits the time that the proactive recovery scheme can be used to forward traffic before the global routing protocol is informed about the failure, and hence reduces the chance that a transient failure can be handled without a full global routing re-convergence.

AES Algorithm:

A term associated with AES is "the State," an 'intermediate cipher,'11 or the ciphertext before the final round has been applied. AES formats plaintext into 16 byte (128-bit) blocks, and treats each block as a 4x4 State array. It then performs four operations in each round. The arrays contains row and column information used in the operations, especially
MixColumns() and Shiftrows().

A.Encryption Algorithm

Step 1:Take the plain text as input and convert it into the state,scramble each byte(SubBytes).
Step 2:Perform Scramble each row (ShiftRows) function to shift rows to left in a table.

Step 3: Perform Scramble each column (MixColumns) to mix the columns in the table.
Step 4:Using addroundkey method encrypt the given plain text.

B.Decryption Algorithm

Step 1:Take the cipher text as input,perform inversesubbyte function.
Step 2:Perform inverse of shiftrows function to shift rows to the correct position.
Step 3: Perform inverse mixcolumns function to mix the columns in the table.
Step 4:.AddRoundKey()does not require an inverse function, as it simply XORs the state with the subkey (XOR encrypts when applied once, and decrypts when applied again).

III EXAPMLES

State

The text is first converted into state.

Text	A	E	S	U	S	E	S	A	M	A	T	R	I	X	Z	Z
Hexadecimal	00	04	12	14	12	04	12	00	0C	00	13	11	08	23	19	19

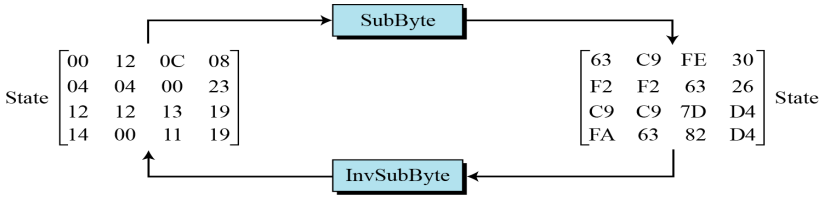
$$\begin{bmatrix} 00 & 12 & 0C & 08 \\ 04 & 04 & 00 & 23 \\ 12 & 12 & 13 & 19 \\ 14 & 00 & 11 & 19 \end{bmatrix} \text{State}$$

SubBytes &InvSubbytes

The first transformation, Sub Bytes, is used at the encryption site. To substitute a byte, we interpret the byte as two hexadecimal digits For decryption the inverse of subbytes is carried out. AES also defines the transformation algebraically using the GF(28) field with the irreducible polynomials *($x^8 + x^4 + x^3 + x + 1$).*

Subbyte: $d=x(s_{r,c})^{-1} \oplus y$

Invsubbyte: $[x^{-1}(d \oplus y)]^{-1}=[x^{-1}(x(s_{r,c})^{-1} \oplus y \oplus y)]^{-1}=[(s_{r,c})^{-1}]^{-1}=s_{r,c}$



ShiftRows& Invshiftrows:

In the encryption, the shiftrows transformation is used to shiftrows in the matrix to left side.

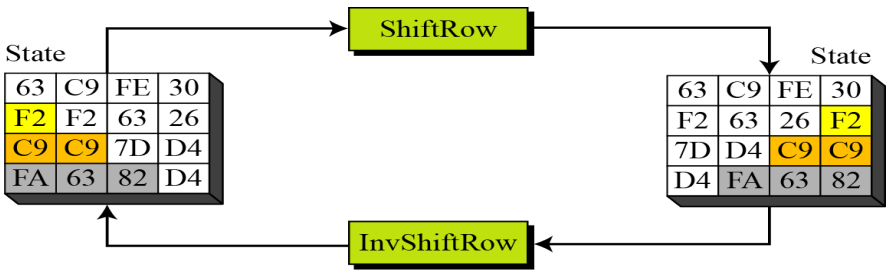
Rules for shiftrows:

- The first row is kept as usual.
- In second row one byte is shifted to left.
- In third row two byte is shifted to left.
- In third row three byte are shifted to left.

In the decryption, the shiftrows transformation is used to shiftrows in the matrix to right side.

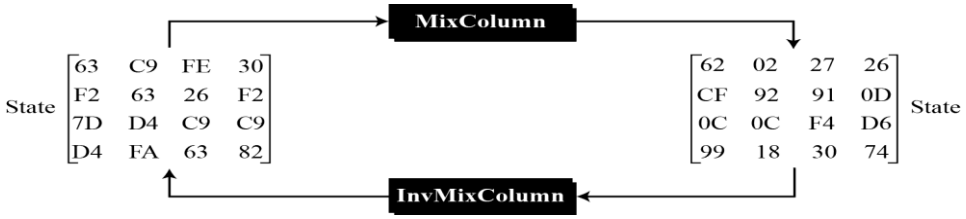
Rules for Invshiftrows:

- The first row is kept as usual.
- In second row one byte is shifted to right.
- In third row two byte is shifted to right.
- In third row three byte are shifted to right.



MixColumns ,Invcolumn

We need an interbyte transformation that changes the bits inside a byte, based on the bits inside the neighboring bytes. We need to mix bytes to provide diffusion at the bit level.The MixColumns transformation operates at the column level; it transforms each column of the state to a new column. InvMixColumns transformation performs the inverse function of
Mixcolumn .



AddRoundKey

AddRoundKey proceeds one column at a time. AddRoundKey adds a cipher key word with each state column matrix; the operation in AddRoundKey is matrix addition.Using the cipher key convert the cipher text to plain text. It adds key for every round of conversion. For 128 bits it goes through ten round totally forty keys generated. It may vary upon number of bits it passes. The cipher text is converted into plain text using the cipher key.

IV. APPLICATION

ADVANTAGE OF AES ALGORITHM

- The result cannot be easily identified.
- Brute attack, Statistical Attacks, Differential and Linear Attacks cannot crack the cipher text

V. CONCLUSION

MRC is based on providing the routers with additional routing configurations, allowing them to forward packets along routes that avoid a failed component. MRC guarantees recovery from any single node or link failure in an arbitrary bi-connected network. By calculating backup configurations in advance, and operating based on locally available information only, MRC can act promptly after failure discovery. MRC operates without knowing the root cause of failure, i.e., whether the forwarding disruption is caused by a node or link failure. This is achieved by using careful link weight assignment. We implemented AES algorithm to provide security for data transmission.

REFERENCE

[1] Advanced Encryption Standard (AES), Nov.26, 2001.
[2] Atul Kahate(2009), *Cryptography and Network Security,*second edition,MCgRAW-Hill.
[3] A. Kvalbein, T. ˇ Ci˘cic´, and S. Gjessing, "*Post-failure routing performance with multiple routing configurations*," in *Proc. IEEEINFOCOM*, May 2007.
[4] A. Nucci, B. Schroeder, S. Bhattacharyya, N. Taft, and C. Diot, "*IGP link weight assignment for transient link failures,"* in *Proc. 18th Int. Teletraffic Congress*, Berlin, Germany, Aug. 2003.
[5] S. Nelakuditi, S. Lee, Y. Yu, Z.-L. Zhang, and C.-N. Chuah, "*Fast local rerouting for handling transient link failures*," *IEEE/ACM Trans. Networking*,vol. 15, no. 2, Apr. 2007.
[6] Y.Wang, Z.Wang, and L. Zhang, "*Internet traffic engineering without full mesh overlaying*," in *Proc. IEEE INFOCOM*, Apr. 2001.
[7] W. Lou and Y. Fang, "*A Multipath Routing Approach for Secure Data Delivery*," *Proc. IEEE Military Comm. Conf. (MilCom)*, 2001.