I J C T A, 9(11) 2016, pp. 5369-5376

SECURE REACH ROUTING ALGORITHM USING KEYLESS ENCRYPTION

Mr. Ch. Prem Kumar[*], Amit Verma[**] , Ravi Prakash[***]

Abstract: Development in Information technology has brought various threats and problems in communication apart from facilitating it. To prevent the data during this process from an outsider, proper means of security need to ensure before transmission. Cryptography which is the science of writing in secret code, is an inevitable part in the field of network security is used to protect the data. Cryptography is not a solution to all the attacks but is a way to prevent them. Internet routing protocols are subject to various attacks by the intruders Various algorithms have already been developed and implemented to address the problem but in this paper, we aim to solve the problem by using a keyless encryption approach to protect the routing data. Basically, the cryptography algorithms are categorized into two types on the basis of key management, which are key-oriented and keyless encryption algorithms. The proposed algorithm reduces the probability of attack as it does not require any explicit keys over the transmission medium. Moreover, the processing time of key generation is reduced considerably thus providing security against unauthorized attacks.

Key Words: Routing protocols, Cryptography, keyless encryption, Security, intruders.

1. INTRODUCTION

Security plays an inevitable role in the computers and communication systems by preventing against illicit attacks. In order to secure the transmitted data during communication, it becomes necessary to address the concern of confidentiality of this data. Encryption is the process of secretly encoding the data to prevent it from intruders ensuring its security. There are various algorithms for transforming the data sent by the receiver called the plain text into the cipher text. The principal objective of all the algorithms is the prevention of data against all unauthorized attacks and access [1].Cryptography is categorized as key oriented and keyless. Keyless encryption involves transformation of the data by the algorithm by maintaining the anonymity of the sender [4]. The advantage of keyless encryption is that it reduces the management of the bulky keys and reduces the processing time involved in key generation thus simplifying the entire process. Practically, in order to ensure security the algorithm must address concerns like performance and complexity [1]. In order to strike a balance between security and performance, the paper proposes a keyless approach for prevention of routing data .This would not only result in increase in the performance of communication channel but would also prevent the intruder from obtrusion into data.

[*] Assistant Professor, CIT Dept University of Petroleum & Energy Studies Dehradun, Uttarakhand State, India
Email: chpremkumar@ddn.upes.ac.in

[**] Student, University of Petroleum & Energy Studies Dehradun, Uttarakhand State, India
Email: amit.verma@ddn.upes.ac.in

[***] Email: rprakash@ddn.upes.ac.in

Routing Protocols are the key enablers of connectivity in the computing world. Routing Protocols are mainly responsible for establishing and maintaining routing paths among the hosts. For ensuring the reliability of these routing protocols, stability, fault tolerance and security must be incorporated .Routers can behave in a malicious manner by disrupting the communication- by creating routing loops or degrade network performance – by poisoning the routing tables. Thus, there is a critical need to secure the routing protocols from the threats which are the threats tending to cripple the communication. Efficiently securing the routing protocols is difficult [3]. The Open Shortest Path First (OSPF), a link state protocol is the most widely used interior gateway protocol routing protocol (IGP) for the Internet. Link-state routing protocols like OSPF generate routing updates only when a change occurs in the network topology with their nearest neighbours. It works on the fundamental principal of the Dijkstras algorithm by sharing the entire topology and calculating the path based on the shortest path. Despite its reliability and scalability, OSPF is vulnerable as an attacker can modify the link state advertisements of other routers resulting in incorrect routing table computation by the remaining routers thereby degrading network performance [3]. The routing data can also be attacked leading to a loss of business critical information. Thus, ensuring data integrity is an important requirements for securing the routing protocols.

The paper intends to create a keyless reach routing algorithm for the OSPF protocol in order to ensure safe transmission of data. For this purpose, a cipher algorithm has been proposed which can be easily integrated at all junction points of data transmission i.e. the points where information is sent or received in encrypted format. The algorithm uses keyless approach of encryption as stated above which is solely algorithm based implying a simple integration of both the encryption and routing algorithm would serve the basic requirement of safeguarding the data.

The main application of the encryption is required at the time of information broadcast done by the router stating its security protocols to adjacent nodes. So, the proposed concept utilizes the expansion, permutation and substitution methodology on the plain text and then uses the RSA algorithm to encrypt the data, further adding security. The data at first is made to input in matrix of format after which expansion of data is done to the size of the remaining data in the block. This results in a key with recognizable character pattern .In order to prevent the pattern to be concealed, RSA (Rivest Shamir Adleman) algorithm is applied for further encryption and is finally permuted [5]. The algorithm capitalizes on the fact that there is no efficient way to factor very large numbers. The reason to use RSA algorithm is that RSA algorithm uses mathematical values for its parameters which can be easily manipulated than a string key. Moreover, RSA is a simple encryption and verification technique supported by the industry providing security to the data faster [5]. This key is then added to the remaining block consisting of plain text, in order to obtain cipher text. Permutation and Substitution is then applied to the key to obtain the final cipher. The decryption methodology is simple and again requires to generate the key from the cipher text itself by storing it in the matrix. Expansion and Permutation generate the intermediate key which is subtracted from the cipher text to get the block of plain text. The decryption method is simple and straightforward with the method similar to that of encryption.

This cipher is sent for transmission via the OSPF protocol making it less vulnerable to attacks. It is implemented at first by initialization of the broadcast and encryption module. The message would act as an input for the encryption module which would encrypt the text to obtain cipher. The cipher would be broadcasted to prevent data obtrusion and then be decrypted at the receiver side integrated with the decryption module. The information obtained is sent further to other modules. The process in OSPF is run at all adjacent nodes for communicating the network layout. The entire process of generation of key with the text itself without requirement of the external key generation simplifies the entire cryptographic process of safe data transmission. The implementation of the

algorithm using RSA to encrypt the key and further derivation of cipher text at the receiver side in encryption module prevents the routing information from being invaded thus making the entire process private.

2. LITERATURE REVIEW

A Keyless User Defined Optimal Security (KUDOS) Encryption has been proposed by Akhil Kaushik, Satvika, Manoj Barnela, and Anant Kumar .It aims to remove the bulky keys from the process of cryptography by illustrating the a symmetric encryption algorithm called KUDOS. The KUDOS algorithm completely states a new approach of security with integrating the requirement of security and keyless cryptography [1].

Key exchange using 'keyless cryptography' by Bowen ALPERN and Fred B. SCHNEIDER from the Department of Computer Science, Cornell University, introduces the concept of describe key-distribution protocols that are based on keyless cryptography ,which hides the information by keeping the originator of the message a secret. Protocols to generate and distribute secret keys in a computer network are described, which allow two users to agree on the value of a secret key, while preventing passive wire tappers and other users from determining its value. [4].

A keyless JS algorithm has been implemented by Jiwan Pokharel, N. Saisumanth, Dr Ch. Rupa and T. Vijaya Saradhi. It solves the problem of secure data transmission between two parties by presenting a key-less "JS algorithm", which readily encrypts and decrypts the data. The paper has utilized the concept of using certain portion of its own data to create a protective coating from eavesdropper. Selection of appropriate number of rounds (up to 256) as per the security level is a major advantage associated with the algorithm. Overall, the paper illustrates with experimental analysis a methodology for secure data communication [2].

Routing Protocol Security Using Symmetric Key Based Techniques presented by Bezwada Bruhadeshwar and Kishore Kothapalli and M.Poornima addresses the security of routing protocols subject to attacks in the control plane as well as the data plane. It states the importance of routing protocols among network hosts and the need for their reliability as well as stability. The vulnerabilities involved can reduce the trust by degrading performance in a malicious manner. The paper focuses on an integrated approach of symmetric key protocols for addressing the security at both the control and data [3].

Implementation of RSA algorithm using elliptic curve algorithm for security and performance enhancement by Prasant Singh Yadav, Pankaj Sharma, and Dr K. P Yadav introduces the concept and implementation of RSA algorithm for security purpose and to enhance the performance of software system [5].

3. SYSTEM MODEL

The keyless encryption-decryption algorithm is implemented in the routing protocol Open Shortest Path First Algorithm (OSPF) in order to address its security concerns. OSPF is the underlying base algorithm integrated with the proposed encryption algorithm. As OSPF is the most widely implemented routing protocol for transmission using Dijkstra' s Algorithm in order to calculate the loop free shortest path, a high level of security is incorporated .The cipher is obtained using block level encryption of size 128 to 512 bits. The alphanumerical dictionary is used for encryption. Encryption model is initiated at the very time of information broadcast done by the router stating its security protocols to adjacent nodes. The block level encryption algorithm

considers the text as a 2D Matrix. The entire system level block diagram uses the process illustrated in the diagram:

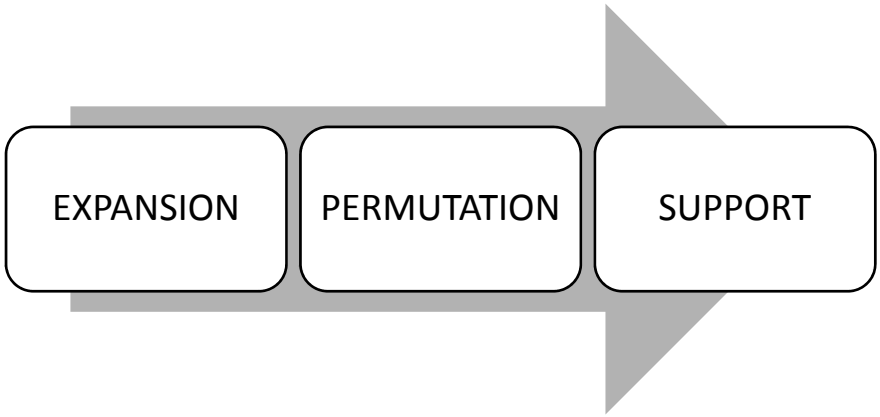

Fig 1. Process Oriented Block Diagram

The encryption and decryption algorithm later used by the routing protocol use the above illustrated process. At first, expansion is used to derive the unencrypted intermediate key (I_K) from the block of size 4*4 using the key placement algorithm and is made of the size of the remaining text of the entire block. In order to remove similarity, RSA algorithm is used to encrypt I_K after which permutation is applied to obtain the encrypted key. The final cipher text is

$$C_L = [(P_L\text{-}K_L) + I_K)] \, P_2$$

Decryption module follows the same model of decryption. The key obtained from the cipher text is used to retrieve I_k. The decrypted key after subtracting from the cipher recovers the plain text.

$$PL = [(CL\text{-}KL)\text{-}IK]$$

The data transmission by the routing protocol is protected at both ends by the encryption and decryption module. The integration of both the algorithms at the sender and receiver side prevents the broadcasted message from being leaked, thus maintaining data integrity. The model at the routing protocol is illustrated below.

Fig 2. Routing Model

Notations:

E_1: Expansion-Box

P1: Permutation-Box

S1: Support-Box

IK: Unencrypted Intermediate Key

KL: Encrypted Key obtained after using I_k

CL: Cipher Text obtained after Encryption using Keyless

RSA: Rivest Shamir Adleman Algorithm

PL: Plain Text

4. PROBLEM DEFINITION

Data being transmitted over the internet is both confidential and sensitive. Transmission of data by maintaining data integrity is a major challenge. Security in transmitting the sensitive data over internet has become a major challenge. Routing protocol specifies the communication details to routers and exchanges routing state updates enabling them to compute routes towards various destinations. Routing Protocols are subject to various attacks and are difficult to secure efficiently [3]. There are various routing algorithms which determine the specific choice of route and aim in safe transport of the routing information. Traditional cipher algorithms cannot be used for securing today's information as security is the main concern [1]. The data being transmitted via these protocols is subject to attacks like injection or modification of routing messages, which may lead to incorrect computation of routing paths or forwarding the message to the routers that benefit the attacker. An attacker may also attempt to exploit mechanisms in the routing protocol, such as those intended to quickly spread new routing information, to instead consume large amounts of network and router resources. In the most commonly used routing protocol OSPF where the information is broadcasted, attacker can modify the link state advertisements of other routers. This results in incorrect routing table computation by the remaining routers thereby degrading network performance.

The growing significance of internet among various organizations and public services, has made the security of routing protocols a significant issue. Hence an algorithm which relieves the user of all the hassles of securing the data an algorithm is required which minimizes human error and makes the data more secure. To make the transmission of data secure as well as simplified, an algorithm which does not require the user to produce any key is used instead of bulky external key which increases the time complexity .Keyless Encryption makes the communication process easier and prevents the attacker from encroachment of the key leading to loss of critical data [2]. Thus the messages including the routing updates, being broadcasted via the OSPF routing protocol must be protected before transmission to avoid encroachment and in order to ensure data integrity.

5. ALGORITHM

Encryption

Fetch Plain-Text and Load first 512 bits (64 bytes) into the P_L Matrix

1. Take out the block of size 4x4 (0...4,0..4) derive the key using Column major operations apply expansion-Box (E_1), then P-Box (P_1) and finally S-Box(S_1) to the key. Now size of remaining text: 384 bits, therefore a key is required of that size to be added to the key.
2. Obtain the Intermediate Key- IK (Unencrypted) by key placement algorithm.
3. The Key has a recognizable Character pattern. To remove that we will apply the basic operations of cryptography, i.e., Confusion and Diffusion. To achieve this, RSA is used to

encrypt the key and then apply a randomization sequence. The reason to use RSA algorithm is that RSA algorithm uses mathematical values for its parameters which can be easily manipulated than a string key.

4. Add the intermediate key to the remaining plain text to get Cipher, C_L
5. In C_L place the K_L using formula: C_L (i, j) =K_L, where the place is selected such that only a position after a+r is selected where a=0, a=a+1 and r=1.
6. $CL = [(P_L\text{-}K_L) + I_K)]$ P2->P_2- P-Box<-1.

Decryption

The decryption methodology is simple and straight forward.

1. The cipher text is stored in 2D-Array and the key placement algorithm is then run on this text and the key is extracted.
2. The key is simply sent through E_1 Box and P_1 Box sequentially which gives I_K.
3. The Intermediate key is the final requirement which is subtracted from the Cipher text resulting in the 384-Bit Plain text.
4. At last the key is placed in the text and decrypted text is obtained.

Decryption PL = $[(C_L\text{-}K_L)\text{-}I_K]$

Routing:

1. Initialize Broadcast module and encryption module.
2. Inside Broadcast module ret () the broadcast message as the input for encryption module
3. The encryption module follow the steps accordingly and get () the text to Broadcast module
4. The Broadcast module then Broadcasts this message
5. This message when received at an adjacent node is sent to its Receiver module which receives the encrypted message.
6. This receiver module is integrated with decryption module which get () the text and is processed with decrypting modules following the steps accordingly.
7. The decrypted information is sent to receiver module which is further sent to other modules which has the required data for routing modules to update their routing tables and other relevant configuration.
8. This whole process is run at all adjacent nodes in conjunction to each other giving a full network layout.

Example

Message: India is my country and I love my country more than anything in this world.

Encryption-Key-Less

Taking an 4*4 block out of the above message and applying column major operations, a matrix consisting of plain text is illustrated by the below figure

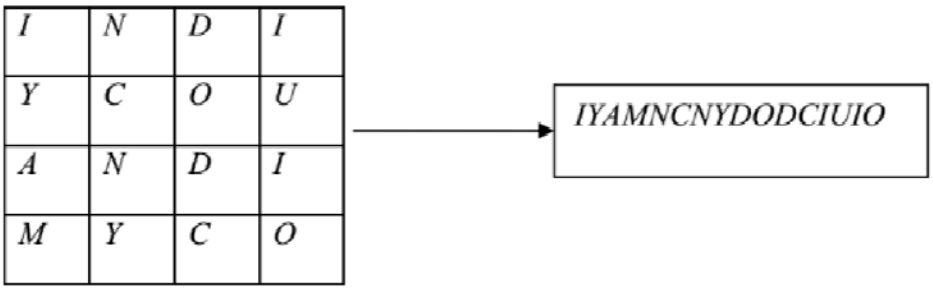

Fig. 3: Extracting 4x4 Block of data from the message

Applying the key placement algorithm in order to obtain the unencrypted key which is the primary requirement for the algorithm is illustrated in the figure below.

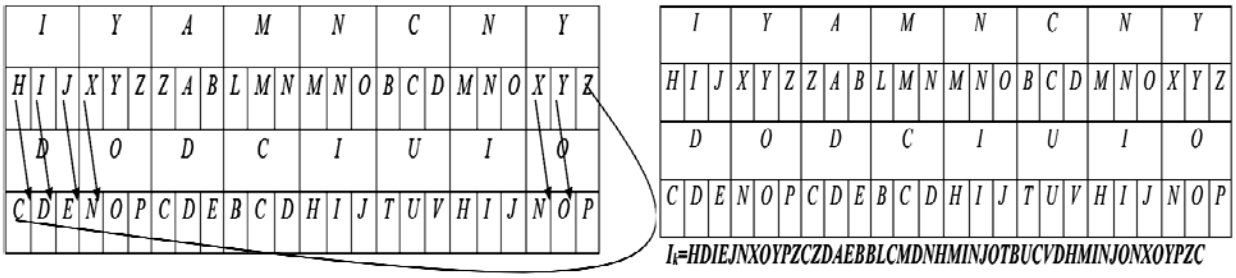

Fig 4: Extracting the Unencrypted initial Key

6. CONCLUSION

The keyless encryption and decryption algorithm saves the transmitted data routed by the OSPF protocol from being attacked simply by adding an encryption module. The overhead of transportation of the key via the channel is reduced thereby reducing the encroachment by eavesdropper. Moreover, the non-requirement for any specific key allows lesser time for the entire process reducing the time complexity involved for key generation as well as transportation. The user at the receiver end has no idea about the location from which the message is sent or broadcasted and is also unaware that the encrypted text has been encoded by the internal key placement algorithm.

7. FUTURE WORK

A algorithm used to encrypt the initial intermediate key obtained after applying the key placement algorithm would be replaced with better encryption methodologies like triple DES enabling a cipher which is unbreakable and secure to be transmitted. Implementing such algorithms would make the internet routing protocols achieve a higher level of security.

References

[1] Akhil Kaushik, Satvika, Manoj Barnela, and Anant Kumar, “Keyless User Defined Optimal Security Encryption”, International Journal of Computer and Electrical Engineering, Vol.4, No.2, April 2012

[2] Jiwan Pokharel, N. Saisumanth, Dr. Ch. Rupa, T. Vijaya Saradhi, “A Keyless JS Algorithm”, International Journal Of Engineering Science & Advanced Technology Volume-2, Issue-5, 1397 – 1401.

[3] Bezawada Bruhadeshwar and Kishore Kothapalli and M.Poornima and M. Divya, “Routing Protocol Security Using Symmetric Key Based Techniques”, IEEE, March 2009.

[4] Bowen Alpern and Fred B. Schneider, "Key Exchange Using Keyless Cryptography", Information Processing Letters 16 (1983) 79-81 North-Holland Publishing Company, 26 February 1983.

[5] Prasant Singh Yadav, Pankaj Sharma, Dr K. P Yadav, "Implementation Of RSA Algorithm Using Elliptic Curve Algorithm For Security And Performance Enhancement", International Journal of Scientific & Technology Research Volume 1, Issue 4, May 2012.