Two Fish Cryptography For Data Security In Network Communication

Divya, R. Gobinath

Abstract*: The study of secure communication techniques is known as cryptography which plays important role in wireless ad hoc network. Cryptography is required to secure the data communication which enables two or more parties to communicate over insecure channel. Many cryptographic algorithms such as RSA, Bluefish, DES, etc. are implemented in many fields such as data communication, electronic commerce, chip based payment cards, digital currencies, computer passwords and military communications. This paper particularly presents the development of ADODV protocol with data security using Twofish cryptography and short overview about all block cipher methods used in network routing.

***Keywords* : Data security, network simulation, AODV routing, Twofish.**

I. INTRODUCTION

Simulation is the process of learning by doing. Network Simulator is the popular simulation can be used for both wired and wireless network. Several network categories such as MANET, VANET, etc., network protocols such as TCP, UDP and network routing algorithms are simulated and implemented using NS (Network Simulator).

The process of studying the information security with many protocols is called cryptography which protects the sensitive data from unauthenticated users over insecure wireless channels. Symmetric key consisting of encryption and decryption key is the fastest technique used in several advanced cryptography. Among several cryptographic algorithms Twofish cryptography is
one of the fastest and efficient techniques to secure the data while routing over the wireless network. Twofish works on 128 bit block of plaintext. Dividing input bit into 4 parts, performing XOR operation between bit inputs with a key and processing the input bits in 16 times Feistel network are the steps to be followed in Twofish algorithm. Data security and confidentiality of data is achieved by implementing Twofish algorithm when the data is transferred over the network. Succeeded data can be encrypted or decrypted. The speed of the encryption process is 3 times longer than the decryption process.

To schedule the packet and timer expiration events a packet level simulator Ns – 2 is used which is also denoted as centralized discrete event scheduler. An events occurring one by one can only be handled by the centralized event scheduler. Therefore events occurred at the same time cannot be accurately emulated. The events are often transitory therefore it is not a serious problem in network simulator. The two simple assumptions of wireless extension are as follows:

(1) When the packets are transmitted or received by the high rate and low speed nodes, it does not move significantly over the length of time.

(2) When compared to the speed of the light, the velocity of the node is insignificant.

II. LITERATURE REVIEW

Many papers have been surveyed for carrying out the current work. The evaluation of Ad-hoc routing protocols with abstract, methodology and parameters are discussed as follows:

The complement of AODV protocol is represented in paper [1]. The source node could not receive the route reply due to change in the topology, i.e. the node gets a reply message from the source node only after sending the route request message many times, which leads to increase in communication delay and power consumption. At the same time it also leads the packet delivery ratio to be decreased.

An implementation of AODV routing protocol that depicting changes to the route table while routing the data over wireless network is focused in this paper [2].

A reverse of AODV(R-AODV) protocol with multiple route reply messages are proposed in this paper [3]. Using NS2 simulation tool the R-AODV is implemented which results in good packet delivery.

An IP network protocols such as Int Serv, Diff Serv and RSVP are glanced in this paper [4]. This paper is mainly focused on QoS routing for MANets.

An Optimized Power Reactive Routing (OPRR) is proposed in this paper [5]. This type of routing will avoid the new route discovery approaches which improve network stability.

The 802.11 series with QoS schemes in the MAC layer is focused in this paper [6]. Multihop scheduling and mobile handoff over wireless network is mainly addressed in this paper.

An improved AODV routing protocol based on 802.11 has been proposed in this paper

Revised Manuscript Received on July 05, 2019.

Miss V Divya*, Research Scholar, Department of Computer Science, VISTAS, Pallavaram, Chennai & Assistant Professor, Prince Shri Venkateshwara Arts and Science College, Chennai.
Email: divyavenkatraman1992@gmail.com
Dr. R. Gobinath, Associate Professor, Department of Computer Science, VISTAS, Pallavaram, Chennai.

[7]. This implementation is computed using NS2 simulation which depicts the comparison between IEEE 802.11 series and IEEE 802.15.4 series.

This article [8] studies the QoS routing issues and compares the existing QoS base modification on AODV protocol.

The paper [9] focuses on mobile ad hoc network with the voice call problem employs IEEE 802.11b standard. An extended Ad-hoc On-Demand Distance Vector (AODV) protocol uses Distributed Coordination Function to search the stable routing.

The focus of this paper [10] brings out the logic to accept CAODV for building the tunnel's network.

III. AODV ROUTING WITH TWOFISH SECURITY

Without the need of external infrastructure like cables, the Ad Hoc network can be set anywhere. The network topology requirement and restructuring the route is not achieved using multi hop routing protocol. Therefore without any route break, high error rate and eavesdroppers the confidential information can be transmitted over wireless medium using Ad Hoc network. To achieve the data security along with route repair Twofish cryptography algorithm is used with AODV routing protocol.

An encryption algorithm generally used in cryptography and steganography is twofish cryptography. This type of encryption algorithm works based on the existing Blowfish algorithm. Block ciphering and single key with variable length of 256 bits are used by twofish algorithm. To balance the performance speed of the cryptography, timing for key setup and the size of the code are implemented. This algorithm manages the attack on six rounds which undergoes 2^{41} chosen plaintexts and 2^{232} efforts.

The general design criteria of twofish cryptography are as follows;

- 128, 192, and 256 bits of key length.
- A symmetric block cipher with 128-bit.
- Efficient on Intel Pentium Pro.
- Weak keys are avoided.
- Additional key length.
- Easy analysis and implementation.

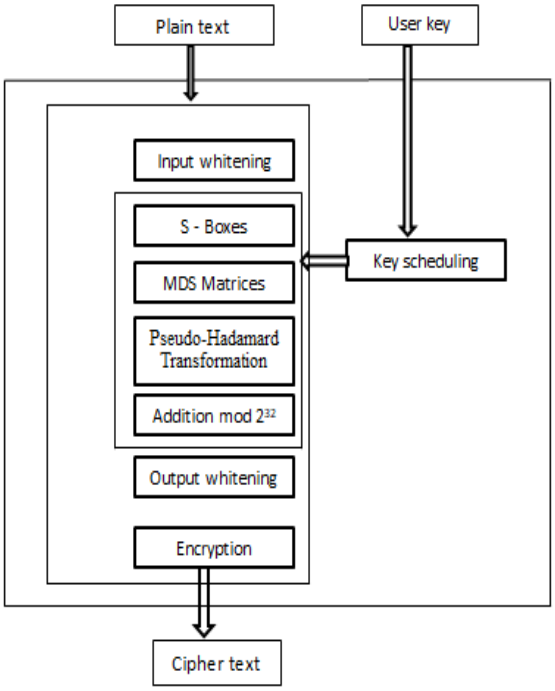

Fig. 1 Flow of Twofish cryptography

IV. ELEMENTS OF TWOFISH CRYPTOGRAPHY

The design elements of twofish algorithm are;

- The S-boxes with key-dependent
- The MDS Matrix
- The PHT
- The Feistel Networks

A. The S-Box with key dependent

The key design elements of Twofish algorithm is s-box. The characteristics of S-boxes are:

- 2 or 4 bytes of key assignment is made for each s-box.
- Each S-box outputs one byte.
- Few or no key pairs should be generated in identical S-boxes.
- A minor change in the key results in extremely different S-boxes.
- High-probability differential or linear characteristics are due to weak s-boxes caused by the keys.

.

B. MDS Matrix

The four S-boxes outputs four bytes, for this purpose the diffusion mechanism MDS Matrix is used. To achieve this, the output is multiplied with the MDS Matrix, which undergoes following attributes:

- Any input change can be guaranteed for modifying the output bytes.
- When two input bytes are changed,

then minimum three types of outputs will be changed.

- Though the rotation is made in the round function, there is a possibility to preserve the number of bytes modified.
- Includes fixed number of coefficients.
- Four lookup tables are used to implement the multiplication; therefore each lookup table contains 256 32-bit words.
- For decrypting, the matrix inverse is not used by twofish algorithm.

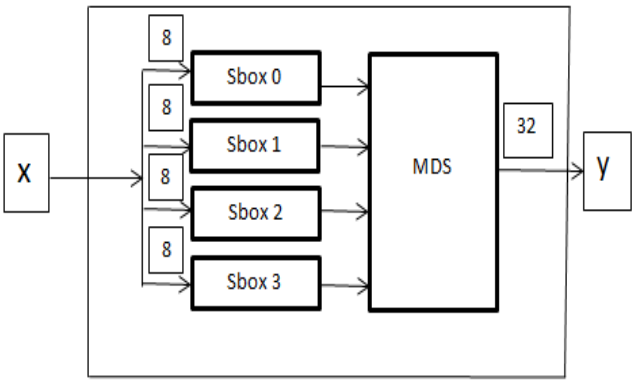

Fig. 2 MDS matrix representation in Twofish

C. Pseudo-Hadamard Transformation

The **PHT** is a cryptographic diffusion provided by the opposite bit transformation of the string. The variable *a* and *b* are the two classification of bit strings with the same lengths of *n* bits.

For any given key, the encryption process and decryption process can be compiled which optimize the performance of twofish algorithm. The eight key dependent S-boxes can be used instead of four and 8 X 8 MDS matrix can be used instead of a 4 X 4, which is considered to be the alternate for PHTs. But this alternative is much slower to implement the twofish, therefore PHTs are often used for implementing twofish cryptography. To compute the PHT transform, consider a and b are the two given inputs. The PHT can be denoted as;

$$a' = a + b \pmod{2^n} \quad (1)$$

$$b' = a + 2b \pmod{2^n} \quad (2)$$

D. Feistel Network

To transform a function into a permutation is the common the method used. The type of function is used in the DES. The Feistel routine is used to map the string of inputs as the string of outputs. This type of network works based on the Feistel routine which is denoted as F function, where often the value of F is not the linear and surjective;

$$F : \{1,0\}^{n/2} \times \{1,0\}^{N} \rightarrow \{1,0\}^{n/2}$$

The source block, which is the input and the output of *F* is EXORed with the destination segment. For the second round both the source and target blocks swap their places. The process is iterated repeatedly in order to create the strong encryption. After completing one cycle (two rounds in fiestel network) every bit of the text segment bits are altered. The frequency of levels is directly proportional to the algorithm strength. A strong cryptography undergoes more rounds (Twofish is a 16-level encryption network).

Steps for Twofish algorithm are as follows;

Step 1: QRY packets are encrypted

Step 2: QRY packets should be transmitted to the nearby neighbour nodes.

Step 3: If the authorized node receive the QRY packet then the following is performed;

i) Using hash code, the QRY packet is decrypted.
ii) Based on the QRY packet, the UPD packet is constructed.
iii) UPD packet is encrypted as in first step.
iv) UPD packet is forwarded to the source node.

Step 4: If the black hole receives the QRY packet then the node of black hole or grey hole will perform the following;

i. UPD message will be generated.
ii. The generated UPD packet is forward to the source.

Step 5: The received UPD is checked and the following is performed;

1. The received UPD packet is decrypted.

2. The hash code set the flag as 0 which indicates that the UPD packet is transmitted only by the authorized node. Therefore the packet is correctly decrypted.

3. Else, the UPD packet has come from a black hole node which in turn sets the flag as 1.

4. The black hole node affects the information if the hash code is changed while decrypting the packet.

Step 6: The value of trust index is computed as follows;

Trust index = correct transmissions / total number of transmissions

Step 7: Network link is established from the sender to link as follows;

i. Path is selected based on links computed by trust index.
ii. From the communication path the black hole is excluded.

iii. Links having low trust indexes are avoided.

Step 8: Repeat Step 4 to 7 when the node becomes a black hole.

V. SIMULATION RESULT

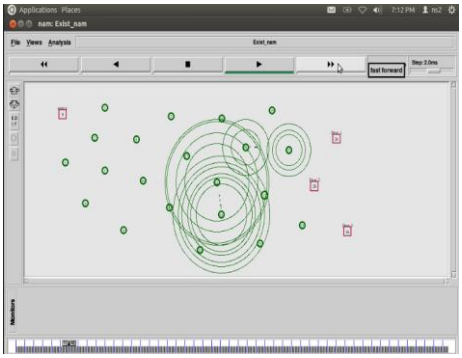

Fig. 3 Node connectivity in NS2

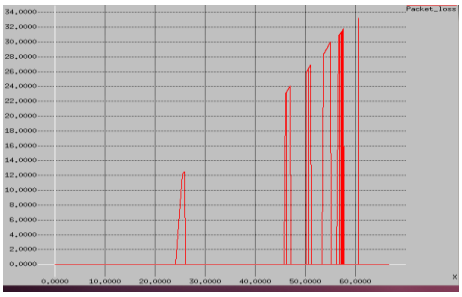

Fig. 4 Packet loss in AODV protocol

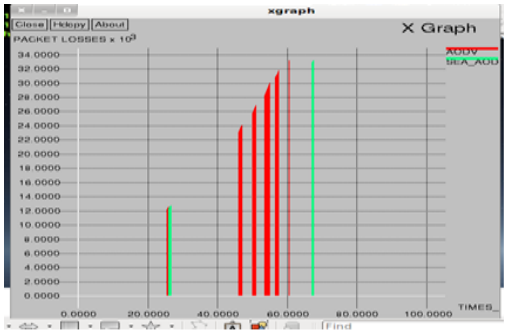

Fig. 5 Packet loss in AODV and M-AODV

VI. CONCLUSION

Twofish is one of the most advanced AES standard algorithm used secure symmetric block ciphers. Twofish operates on the set of plaintext with the length of 128 bit. Twofish algorithm is used for the data security purpose including encryption and decryption. Twofish algorithm implementation can be used to secure the data. The encryption and decryption are used for succeeding the data. This work is implemented to maintaining the data sensitivity during data transmission through wireless network.

REFERENCES

1. Adeyinka, O. 2008. Internet Attack Methods and Internet Security Technology. Second Asia International Conference on Modelling and Simulation, pp.77-82, 13-15 May 2008. W.-K. Chen, *Linear Networks and Systems* (Book style). Belmont, CA: Wadsworth, 1993, pp. 123–135.
2. Kautzar, M.G. 2007. Studi Kriptografi Mengenai Triple DES dan AES. ITB. Bandung. B. Smith, “An approach to graphs of linear forms (Unpublished work style),” unpublished.
3. Schneier, B. 1996. Applied Cryptography 2nd Edition. Wiley & Sons. Inc., New York.
4. Kantham, L., Ravi, S. 2014. Enhancing Data Security Using DES with Hardware Implementation. Journal of Theoretical and Applied Information Technology (JATIT), May 2014, Vol. 63 No. 2.
5. Schneier, Bruce, John Kelsey, Doug Whiting, David Wagner, Chris Hall, Niels Ferguson. 1998 "Twofish : A 128-bit block chiper".
6. Menezes A.J., Oorschot, P.C., and Vanstone, S.A. 1996. Handbook of Applied Cryptography, CRC Press, Boca Raton, New York.
7. Munir, R. 2006. Pengantar Kriptografi. ITB, Bandung.
8. Hassouna, M. 2013. An End to End Secure Mail System Based on Certificateless Cryptography in the Standard Security Model. International Journal of Computer Science Issues (IJCSI); Mar2013, Vol. 10 Issue 2.
9. Muslim, M.A., Kurniawati, I., Sugiharti, E., 2015. Expert System Diagnosis Chronic Kidney Disease Based on Mamdani Fuzzy Inference System. Journal of Theoretical and Applied Informations Technology (JATIT), Vol. 78 No. 1.
10. Gandomani, T.J., H. Zulzalil, A.Z.A. Ghani & A.A.MD. Sultan. 2013. Important Considerations For Agile Software Development Methods Governance. Journal of Theoretical and Applied Informations Technology (JATIT), Vol. 55 No. 3.
11. PRESSMAN, R.S., 2001, SOFTWARE ENGINEERING: A PRACTITIONER'S APPROACH, 6TH EDITION, THE MCGRAW-HILL COMPANIES, INC, SINGAPORE.