RESEARCH REVIEW JOURNALS
Volume-04
Issue-02
February-2019

ISSN: 2455-3085 (Online)
RESEARCH REVIEW International Journal of Multidisciplinary
www.rrjournals.com[UGC Listed Journal]

A New Improved Scheme for Securing AODV

Dr. Sima

Dept of Urban Planning and Architecture in the subject of Computer Science, State University of Performing and Visual Arts Rohtak

ARTICLE DETAILS

Article History
Published Online: 20 February 2019

Keywords
AODV, MAODV, RAODV, Encryption, Decryption, MANET

Corresponding Author
Email: simasingh.2009@gmail.com

ABSTRACT

In this paper a broad discussion of the new proposed protocol highlighting the disadvantage of the existing protocols is given. It also gives detailed assessment of how a new protocol proposes an effective and more secure route discovering of route maintenance for on-demand routing protocol. After assessing the working of the proposed scheme, the chapter concludes with highlighting certain possible achievements in secure routing.

1. Introduction

In specially appointed organization directing is a significant activity, being the establishment of information trade between remote gadgets. Every remote hub goes about as a switch and partakes in the directing convention. Steering depends on an implied trust relationship among taking an interest gadgets, however accomplishing a safe directing convention in the specially appointed remote organizations is testing a result of the restricted remote transmission range, broadcast nature of the remote medium, hub versatility, restricted power assets, and restricted actual security.[1]

Broad work has been done to make MANET directing got. It was observed that not one technique can accomplish the objective. Numerous mixes were attempted and it was observed that every convention acts distinctively in each proposed plan. New plan is joined on AODV [2] in light of the fact that the majority of the work has been done utilizing AODV as a base convention. Proposed Scheme is contrasted and existing AODV without malignant hubs, with vindictive hubs and results are broke down. It was observed malignant hubs are large issue in MANET directing. These malignant hubs drop the bundles by utilizing counterfeit courses and it is extremely challenging to recognize a pernicious hub.

In this paper two conventions for On-Demand steering in impromptu organizations are introduced.

Initial protocol use encryption and decryption for securing the data. It effectively encrypts the data and provides a good solution for securing the data from hackers. But the drawback of this scheme is that it is not able to detect and remove malicious nodes. Malicious nodes are not able to read the encrypted data but they can destroy the packets by providing fake route reply.

If malicious nodes enter in the network, they can provide fake route to the Source node and they can easily drop the packets.

The Objectives

As per the work conducted, the objectives to be achieved can be summarized as:

- Tackling problem of security
- To secure the routing on MANET using some encryption technique.
- Detecting and removing malicious nodes.
- Running the proposed scheme on a simulator.
- Comparing the scheme with other existing schemes.
- Carrying out performance evaluation using various metrics.
- Evaluating and generalizing the achievements w.r.t. other schemes.
- Carrying out secured transmission and evaluating cost factor.

An algorithm has been proposed for encrypting the information and it has been implemented in C language. This algorithm works on the basic theory of encryption and uses secret key or symmetric cryptography algorithm for it. The following algorithm explains the concept.

2. Algorithm 1

It is a security algorithm for securing 16 bit data packet and its implementation is done in C language. First a packet is entered. It (the algorithm) converts the whole packet in to its 16 bit binary equivalent. Then it (the algorithm) count number of zeros in the packet and generate the encryption key. Suppose there are 5 zeros in the entered packet (for encryption of this packet key will be 5), then it converts the key to its 16 bit binary equivalent (it converts 5 into its 16 bit binary equivalent).

Then it applies XOR operation on the original packet (original packet is the 16 bit binary version of entered packet) along with its generated key (generated key is the 16 bit binary version of 5). Encrypted packets traverse from Source to Destination. On the receiving end it applies decryption process for decrypting the encrypted packet.

2.1 Encryption Algorithm

This is an encryption algorithm which encrypts a 16 bit data packet by using XOR operation as an encryption technique. Encryption is acted in four stages.

Step 1: Activate and Instate the Parcel Pi//Pi is the name of the group

Step 2: Generate an Irregular Key KR by analyzing number of 0s in Parcel.
//KR is the name of the key

(a) Develop a day by day timetable to remember bits for the Information Parcel
(b) Set N: = Count (Pi)//Include Number of 0's in the Information Parcel.
(c) Set KR: =N//Store N in Irregular Number KR

Step 3:Apply XOR (Select OR) Activity
(a) (a) Set EK: = Pi KR
(b) The Encoded Parcel EK is made using XOR Activity.

Step 4: Packet ready for Transmission

Step 1:Activate and Initialize the Packet Pi //Pi is the name of the bundle
Step 2:Generate a Random Key KR by dissecting number of 0s in Packet.
//KR is the name of the key

(a) Develop a daily schedule to include bits in the Data Packet
(b) Set N: = Count (Pi) //Count Number of 0's in the Data Packet.
(c) Set KR: =N //Store N in Random Number KR

Step 3: Apply XOR (Exclusive-OR) Operation
(a) (a) Set EK: = Pi $\oplus$ KR
(b) The Encrypted Packet EK is created utilizing XOR Operation.

Step 4: Packet prepared for Transmission

All The Steps of Algorithm are Explained Below

Step 1: Generates a packet maximum of 16 bit length (This algorithm can be extended for 32 bit packet but for simplicity algorithm 1 is designed for 16 bit packet) and converts this packet in to its 16 bit binary equivalent.

Step 2: Count Number of zeros in the packet. Suppose the entered packet in its binary form is 0000110110001100. There are ten zeros in the packet. Then it converts ten in to its 16 bit binary equivalent and generates a random key which is sixteen bit binary equivalent of ten i.e.: 0000000001010. So the generated key will be: 0000000000001010.

Step 3: For encryption it applies XOR operation on the generated key i.e. 0000000000001010 along with that packet (0000110110001100).

Step 4: Generates Encrypted packet which is ready for transmission. After encryption the packet will be 0000110110000110.

This algorithm provides a secure and efficient encryption scheme for preventing data from hackers. It has been successfully implemented using C language. On the receiving end it receives the encrypted packet along with the key.

Example of Encryption Routine

```
**************************************
Enter The bundle/packet :3468 //Here user can enter any number
**************************************
Original packet is: 0000110110001100
Key is: 0000000000001010

 Encrypted Packet is: 0000110110000110
**************************************
```


3.1 Decryption Algorithm

After receiving an encrypted packet from the Source, Destination requires to decrypt the encrypted packet. The following algorithm decrypts the received encrypted packet.

Step 1: Receive the Encrypted Packet EK // from the Source
Step 2: Receive the Binary key
Step 3: Apply XOR
Step 4: DEK: = EK $\oplus$ KR "Decryption Successful"
Step 5: Accept the Packet

All the Steps of Algorithm are as under explained

Step 1: In first step it receives the encrypted packet which is in binary form.
Step 2: Then it receives the key which is also in binary form. Suppose the encrypted packet is 0000110110000110. Key for decryption is 0000000000001010.
Step 3: For decryption it apply XOR gate on the encrypted packet 0000110110000110 along with that key i.e. 00000000001010.

After applying XOR gate the decrypted packet is 0000110110001100. The decrypted packet is the original packet sent by the Source.

Example of Decryption Routine

- **********
- **Key is:** 0000000000001010
- **Encrypted Packet is:** 000011011000011
- **********
- **Decrypted Packet is:** 0000110110001100
- **********

After the implementation of this protocol an effective encryption technique has been developed. This technique can be implemented on various On-Demand protocols like and Dynamic Source Routing (DSR)[3] and Ad-Hoc on Demand Distance Vector (AODV).[4]

References

[1] *Available at:- http://www.docstoc.com/docs/82983365/MOBILE-AD-HOC-NETWORK , Retrieved on 13-Oct-12.*
[2] *Sunil Taneja and Ashwani Kush "A Survey of Routing Protocols in Mobile Ad Hoc Networks", International Journal of Innovation, Management and Technology, Volume 1, Issue 3, August 2010, pp. 279-285*
[3] *David B. Johnson and David A.Maltz, "Dynamic Source Routing in Ad Hoc Wireless Networks". http://tools.ietf.org/html/draft-ietf-manet-dsr-1 , July-2004. Retrieved on 10-Oct-12.*
[4] *Charles E. Perkins, "Ad Hoc On Demand Distance Vector (AODV) Routing", http://tools.ietf.org/html/draft-ietf-manet-aodv-13, February 2003. Retrieved on 7-Oct-12.*

