P.Periyasamy *et al*, International Journal of Computer Science and Mobile Applications,

Vol.3 Issue. 8, August- 2015, pg. 43-49 **ISSN: 2321-8363**

Traffic Analysis and Prevent Pattern in MANET using AODV Protocol with AES Algorithm

P.Periyasamy[1], R.Anbuselvi[2]

[1]Research Scholar, Bishop Heber College Trichy, periyasamyps1@gmail.com

[2]Assistant Professor, Bishop Heber College Trichy

Abstract:

The Mobile Ad-hoc Network is an autonomous system of movable nodes, this type of a wireless network where the movable nodes dynamically form a network to exchange information without utilizing any pre-existing fixed network infrastructure. In this self-configuring type of network, any type of internal as well as external attacks is possible. When the source node has to transmit the data to the destination node, shortest path will be established between source and destination. The secure and the shortest path between the sender and the receiver ensure reliable data transmission. AODV is the reactive routing protocol which is used to found the shortest path (except malicious node), on the origin of hop counts. In self-configuring type of network, a lot of malicious (data loss) nodes may exits which are responsible for packet dropping. The malicious node impersonates a destination node by sending a spoofed route reply packet to a source node which initiates a route discovery (advertises itself that it is has the shortest path) causes attack. In this paper, we propose the secured solution and detection against attack by finding the optimum path in AODV protocol and providing high secured data transmission using AES Algorithm.

Index Terms: MANET, reactive routing protocol, statistical traffic analysis, AES algorithm.

1. INTRODUCTION

A Mobile Ad-hoc Network (MANET) is the collection of wireless nodes that can be dynamically set by anywhere at any time without the need of any fixed infrastructure**.** In this self-configuring type of network, any type of internal as well as external attacks are possible like Black hole attack, Denial-of-Service Attack, Man-in-the-Middle Attack, Worm hole attack, Gray hole Attack, etc. In AODV protocol, attacks are the major drawbacks which causes problem for data transmission.

A. Applications of Mobile Ad-hoc Networks

There are a number of applications of MANET such as disaster recovery operations, battle field communications, data sharing in conference halls, Sensor Networks, Personal Area Networks, Vehicular Ad-Hoc Networks, Civilian Environments, Emergency Operation, [2] et.

B. MANET Characteristics and Challenges

Some of the MANET characteristics are Dynamic network topology, Multi-hop communications, Bandwidth constraints and variable link capacity, Limited Security, Distributed operation, Autonomous terminal, Light-weight terminals. The major MANET challenges are dynamic topology, limited security, limited bandwidth and routing.

Vol.3 Issue. 8, August- 2015, pg. 43-49 **ISSN: 2321-8363**

2. AODV ROUTING PROTOCOL

Ad-Hoc On-demand Distance Vector routing protocol is a reactive protocol in which the network is established only when the source node desires to transmit data packets to the destination. [6]AODV is capable for both unicast and multicast routing. AODV protocol uses sequence numbers to know the freshness of the route. AODV protocol comprises of mainly two phases. They are Route Discovery phase and Route Maintenance Phase.

A. Route Discovery Phase

When a source node has to transmit to an unknown destination, it broadcasts a Route Request (RREQ) for that destination node. Each intermediate nodes, when a RREQ is received a route to the source is created. If the receiving nodes have not established this RREQ earlier than, is not the destination and does not have an reorganized route to the destination, it re-broadcasts the RREQ. [2]

If the receiving node is the destination or has a current route to the destination, it generates a Route Reply (RREP). As the RREP propagates, each intermediate node creates a route to the destination. When the source receives the RREP, it updates the route to the destination and starts sending the data. If multiple RREPs are received by the source, the routing method with the shortest hop count will choose.

Each and every node in the network maintains the routing table which updates the freshness of the route. If a route is not used for some episode of time, the node closed the route from its routing table. AODV uses sequence numbers to establish an up-to-date path to a destination. Each and every entry in the routing table is associated with a sequence number. If the numbers act as a route timestamp of the sequence, ensuring originality of the path. Leading and receiving a RREQ packet, an intermediary node compares its sequence number with the sequence hop count in the RREQ packet. The sequence number already registered is greater than that in the packet; the existing route is more up-to-date.

Table: AODV RREQ Packet Format

Source Ip Address	Destination Ip Address	Source Sequence Number	Destination Sequence Number	Broadcast Id	Hop Count

Table 2: AODV RREP Packet Format:

Source Ip Address	Destination Ip Address	Destination Sequence Number	Broadcast Id	Hop Count	Life Time

B. Route Maintenance Phase

When a break occurs, a Route Error (RERR) is that is sent to all sources using the broken link through hop-by-hop fashion. [3]The Route Error packet erases all routes using the link along the way. If a resource receives a Route Error packet and a route to the target is still required, it initiates a new path discovery process. Paths are also canceling from the routing table if they are unused for a certain amount of period.

3. SECURE PROCESSING

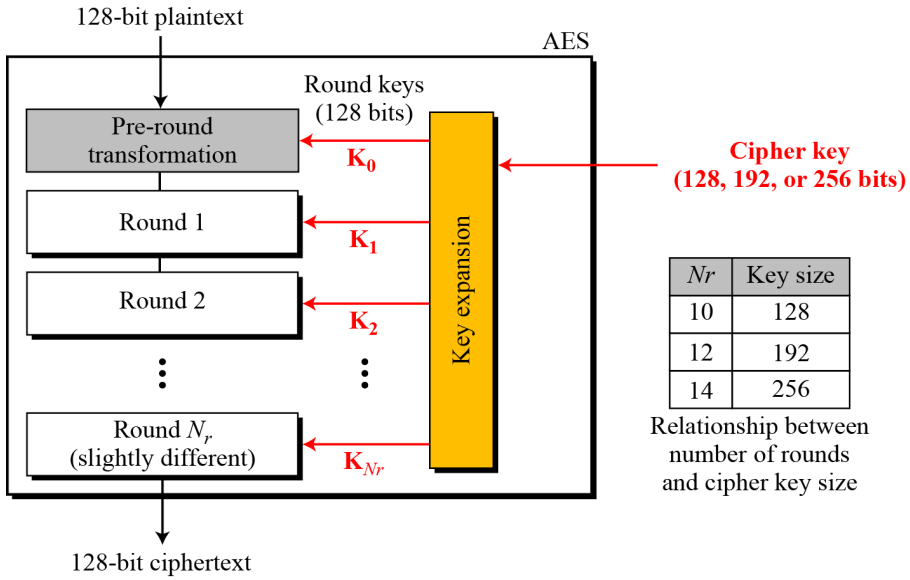
The two processes, encryption and decryption together form the cryptographic process. For ensuring security, the Data are encrypted by the sender before transmitting them and are decrypted by the receiver after receiving them so that only the sender and the intended person can see the content in the image. AES algorithm which uses a key of variable size up to 256 bits. AES symmetric block cipher algorithm encrypts block data of 64-bits at a time.

AES Algorithm

The Advanced Encryption Standard (AES) is a symmetric-key block cipher published by the National Institute of Standards and Technology (NIST).

The criteria defined by NIST for selecting AES fall into three areas:

1. Security
2. Cost
3. Implementation.



Nr	Key size
10	128
12	192
14	256

Relationship between number of rounds and cipher key size

Figure 1: AES algorithm process flow

AES is a non-Feistel cipher that encrypts and decrypts a data block of 128 bits. It uses 10, 12, or 14 rounds. The key size, which can be 128, 192, or 256 bits, depends on the number of rounds.

AES has defined three versions, with 10, 12, and 14 rounds.

Each version uses a different cipher key size (128, 192, or 256), but the round keys are always 128 bits.

To provide security, AES uses four types of transformations: substitution, permutation, mixing, and key-adding

AES, like DES, uses substitution. AES uses two invertible transformations.

Sub Bytes

The first transformation, Sub Bytes, is used at the encryption site. To substitute a byte, we interpret the byte as two hexadecimal digits.

Transformation Using the GF (2^8) Field AES also defines the transformation algebraically using the GF(28) field with the irreducible polynomials ($x^8 + x^4 + x^3 + x + 1$).

Vol.3 Issue. 8, August- 2015, pg. 43-49 **ISSN: 2321-8363**

Permutation

Another transformation found in a round is shifting, which permutes the bytes. Shift Rows In the encryption, the transformation is called Shift Rows Inv Shift Rows In the decryption, the transformation is called InvShiftRows and the shifting is to the right

Mixing

We need an inter byte 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.

Mix Columns

The Mix Columns transformation operates at the column level; it transforms each column of the state to a new column

Inv Mix Columns

The Inv Mix Columns transformation is basically the same as the Mix Columns transformation.

Key-adding

Add Round Key precedes one column at a time. Add Round Key adds a round key word with each state column matrix; the operation in Add Round Key is matrix addition.

To create round keys for each round, AES uses a key-expansion process. If the number of rounds is N_r , the key-expansion routine creates $N_r + 1$ 128-bit round keys from one single 128-bit cipher key.

4. RELATED WORK

In paper [9], every node maintains an authentic table of neighboring nodes along with the routing table. Authentic table contains two entries node name and 1 bit field named authentic which is set to 1 if neighboring node is authentic and 0 if neighboring node is not authentic. Source node first sends a Light-Weight Packet (LWP) to destination node encrypted by its own private key KPRs and public key of destination KPUd. Since only the destination can decrypt this LWP, destination in reply sends a LWP to source encrypted by its own private key KPRd and source's public key KPUs through multiple paths.

If source node receives this LWP from destination then source node marks neighboring node as authentic (by marking 1 in its authentic table) and sends the data packets through the neighboring node to destination. This paper presents a method to detect colluding black hole attack in AODV routing protocol using digital signature. In paper [10], VBOR is taken as the base protocol. The VBOR protocol consists of two phases namely, Route maintenance and Route discovery with the use of variable bit rate. In this paper, the message authentication code is generated during route discovery phase. Then, these data are exchanged between the nodes. VBOR and MAC algorithm is to provide more security in route discovery and data are exchanged to the MANETs.

In paper [11], the proposed solution can be used to detect malicious nodes in the network and find secured routes for the transmission of data from source to destination. The solution involves two additional changes in the AODV protocol. First change is the addition of two parameters in the routing table of each node in the network. These parameters are DATA_PCK_SENT and DATA_PCK_REC. DATA_PCK_SENT will count the total number of data packets sent to its next hop node, whereas, DATA_PCK_REC will count the data packets received from the next hop node. Secondly, an additional routing table known as Routing Information Table (RIT) is to be maintained at source node.

5. PROPOSED SOLUTION

In the proposed solution, we mainly focused on two criteria. The first criteria are to detect and remove the suspicious malicious node. The second criteria are to transmit the data in highly secured manner. The below algorithm provides the way to achieve the above two criteria.

A. Algorithm

Step 1: Choosing the source node and destination node in the network.
Step 2: Source node sends RREQ packet until the destination receives it through the neighbors.
Step 3: Destination node sends back the RREP packet to the source through the neighbors.
Step 4: Finding the possible paths for data transmission.
Step 5: Determining the optimum path

Criteria for optimum path:

1. Hop count should be low.
2. Destination sequence number should be high.

Step 5.1: Among the possible paths, in AODV protocol, the shortest path can be identified by the hop count and destination sequence number.

Step 5.2 : Choosing any node's destination sequence number randomly which is in the routing table and compare with the other node's destination sequence number (+10 or -10) and eliminate the node which have the highest destination sequence number. (Due to the suspecting of malicious node, mostly the malicious node only sends back the RREP packet with this above criteria**).**

Step 5.3: Sort out the possible paths from source to destination.

Step 5.4: Choose the topmost path which have the lowest hop count and reject the topmost path.

Step 5.5: Choose the topmost among the obtained path having lowest hop count, highest destination sequence number and minimal consumed time to do data transfer and do step 7. **(**This path satisfies the criteria as well as it is secure to transfer the data and there is no chance that this path may contain malicious nodes**).**

Step 6: Applying Secure Process (like Encryption and Decryption algorithm AES)
Step 6.1: Even though we detecting the existence of malicious node before data transfer, we need to secure the data during data transmission..
Step 6.2: Encrypt the original data file using AES and do step 7.
Step 6.3: Decrypt the received file using pass code and get back the original data file
Step 7: Do data transfer.

After deriving the routing table for all nodes, we randomly choose any node's destination sequence number among all the nodes and compare with the remaining other nodes destination sequence number that comes within the range of +10 or -10 of chosen destination sequence number and eliminate the node which has the highest destination sequence number. Here, is node 2, which has the highest destination sequence number as 60 (Refer Routing table for every nodes for the destination-6 to find the sequence number)which is out of range of all other node's destination sequence number.(1-20, 3-22, 4-15, 5-20, 6-30). So, we eliminate the node 2 from the network and we find the possible paths with the remaining nodes except node2.

After finding the possible paths, we eliminate the path 4 because it has the lowest hop count as per the algorithm proposed. Finally, we choose the optimum path which is path 1 that has the lowest hop count and highest destination sequence number among the remaining 3 paths. Finally, we do data transfer using the Path 1. Here, the sender encrypts the data file using pass code and conceals the encrypted data using audio file called Steganography and the receiver will receive the audio file. Then, the receivers decrypt the audio file using the pass code and obtain the original data file. Hence, two goals have been achieved that the malicious node is removed and the data packet is transferred in highly secured manner.

Table 3: Optimum Path Selection

Path No.	Path 1→6	Hop count	Destination Seq No.	T I M e (in secs)	Optimum path
1	**1→3→5→6**	**3**	**20+22+30=72**	**5**	**Optimum path having lowest hop count, highest sequence number and minimal consumed time.**
2	**1→4→5→6**	**3**	**20+20+30=70**	**6**	
3	**1→3→4→5→6**	**4**	**20+22+30=72**	**4**	
4	**1→3→6**	**2**	**20+22+30=72**	**3**	**eliminate the path, having lowest hop count**

6. CONCLUSIONS

In this paper, the suspected malicious node has been detected and removed by finding the optimum path in AODV protocol. And the data packet is transmitted in highly secured manner using AES algorithm. Finally, the attack has been detected and data packets are highly secured from the malicious node. As a future work, our aim is to do simulation of proposed algorithm and compare it with existing solutions for optimality.

REFERENCES

[1] N.H. Saeed, M.F. Abbod, H.S. Al-Raweshidy, "Modeling MANET, Utilizing Artificial Intelligent," Second UKSIM European Symposium on Computer Modeling and Simulation, 2008, pp. 117-122.

[2] Neha Kaushik, Ajay Dureja,, ―Performance Evaluation of Modified AODV Against Black Hole Attack in MANET‖, European Scientific Journal June 2013 edition vol.9, No.18 ISSN: 1857 – 7881 (Print) e - ISSN 1857- 7431, 182

[3] C.E.Perkins, E. M. Belding-Royer, and S. Das, Ad hoc On-Demand Distance Vector(AODV) Routing, RFC 3561, jUly 2003.

[4] C.E.Perkings and E. M. Royer. The Ad hoc On-Demand Distance VectorProtocol, In C.E. Perkins, editor, Ad hoc Networking, pages 173-219, Addison-Wesley, 2000.

[5] H. Deng, W. Li, and Dharma P. Agrawal, "RoutingSecurity in Ad Hoc Networks,"IEEE CommunicationsMagazine, Special Topics on Security in Telecommunication Networks, Vol. 40, No. 10, October2002, pp. 70-75.

[6]Sheenu Sharma, Roopam Gupta, ―Simulation Study of BlackHole Attack in the Mobile Ad-hoc Networks‖, Journal of Engineering Science and Technology, Vol. 4, No. 2 (2009) 243 - 250© School of Engineering, Taylor's University College 243, 1SOIT, RGPV Bhopal, India, 2UIT, RGPV Bhopal, India.

[7]www.garykessler.net/library/steganography.html

[8] www.webopedia.com/TERM/S/steganography.html

[9]Akshat Jain, Shekher singh Sengar, Vikas Goel, ―Colluding Black Holes Detection in MANET‖, International Journal of Engineering Research & Technology (IJERT), Vol. 2 Issue 1, January- 2013, ISSN: 2278-0181

[10] K.Pazhanisamy, Dr. Lathaparthiban, ―Secure Route Discovery in Mobile Ad-Hoc Network Using MACBased Group Key Management Protocol‖, International Journal of Advanced Research inComputer Science & Technology (IJARCST 2014), Vol. 2 Issue Special 1 Jan-March 2014, ISSN : 2347 - 8446 (Online), ISSN : 2347 – 9817.

[11] Neha Kaushik, Ajay Dureja, ―Performance Evaluation of Modified AODV against black hole attack in MANET‖,European Scientific Journal June 2013 edition vol.9, No.18 ISSN: 1857 – 7881 (Print) e - ISSN 1857- 7431

