International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

COPY RIGHT

ELSEVIER SSRN

IJIEMR Transactions, online available on 6th Jun 2019. Link :http://www.ijiemr.org/downloads.php?vol=Volume-08&issue=ISSUE-06

Title: AN ENHANCED VIRTUAL PRIVATE NETWORK AUTHENTICATED AD HOC ON-DEMAND DISTANCE VECTOR ROUTING

Volume 08, Issue 06, Pages: 288–292.

Paper Authors

SARA ALI, DR C. D KUMAWAT

Mewar University Gangrar, Chittorgarh, India

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

AN ENHANCED VIRTUAL PRIVATE NETWORK AUTHENTICATED AD HOC ON-DEMAND DISTANCE VECTOR ROUTING

[1]SARA ALI, [2]DR C. D KUMAWAT
[1]PhD Research scholar Dept of CSE ,Mewar University Gangrar, Chittorgarh, India
[2]Professor ,CSE Department ,Mewar University Gangrar, Chittorgarh, India

Abstract— The most commonly used protocol in the MANETS Mobile Ad Hoc networks is the Ad hoc on-Demand distance vector routing (AODV). This has exposed the protocol to a range of security threats. In this paper we have proposed a novel Virtual Private Network Authenticated Ad hoc On-Demand Distance Vector Routing(VPNAODV) protocol which uses techniques like Virtual Private Network ,Observer nodes and Digital signature to secure the protocol against attacks like flooding ,wormhole, blackhole , and Sybil attacks. The protocol proposed by us has enhanced the fundamental AODV protocol while preserving the underlying functionality of the algorithm. Network Simulator-2 is used to compare the results of our protocol and the existing protocol and have found our proposed algorithm to be superior.

Keywords—VPN,Observer,Cluster,Digital Signatures

1 Introduction

Ad Hoc Distance Vector routing protocol is one of the widely used network protocol for routing data in the MANETS. The protocol is Reactive in its functionality i.e. the updates are exchanged between the network nodes in an On-demand method while not in a periodic manner [1,2].The functionality of the MANETS allows all nodes which are a part of the network to act as a specialized router ,which can recover the routes as and when required. These routes provided by the protocol are free of loops. The usage of bandwidth is considerably low as in the case of any node which is disintegrated the protocol does not require any further advertisements. The neighbour nodes have the exclusive ability of detecting one another's other's broadcast messages.The principal objectives of our proposed algorithm are

A. Destination Sequence Number

On receiving a new control packet the destination node compares its sequence number with the existing destination sequence value available in the route entry table, if this value is found greater than the existing value then the data in the route entry table is updated followed by the process of notifying all the nodes of this updated route to the destination. However this value can be altered by the malicious node to give an impression of a better route which may lead to all the packets getting diverted through this route due to the modification in the route table entry..

B. Hop Count

The protocol gives preference to the packets having a greater sequence number value and lesser value of hop count. This feature can be used to present a false path with a smaller

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

hop count by the malicious nodes by decrementing the current value of hop count

2 Security Concerns in AODV

A security threat which is faced by the AODV protocol [3] is due to the presence of mutable data present in the control packets. Information like the Sequence number and the hop count is present in the control packets used to distinctively identify the packet freshness .These fields are changeable which has exposed the protocol to various security attacks. Route notifications associated to a superior path is another aspect which can be used by the malicious node to launch an attack..

3 Attacks on AODV Protocol

A. Worhole Attack

A wormhole attack [4, 5] causes disruption in the network routing, the nodes get a false indication of the advertised link having hop count which is one or two hops shorter than the path which is in current use, this may also lead towards flooding the network and packet dropping. The attack is therefore highly dangerous and also is difficult to realise as these malicious wormhole tunnels are out of bound and concealed in nature consequently and invisible to the network.

B. Blackhole Attack

The malicious node[6] In this attack does not broadcast the inward routing messages but drops them with a purpose of reducing the information related to routing available with the other nodes. This attack is passive in nature .The attack can be launched either selectively, arbitrarily or in mass, making either the destination inaccessible or downgrading the network communication.

C. Sybil Attack

The malicious node[7] In this attack generates fake identity of added nodes in place of a single node. This Identity can either be a replica Id or a false identity. These fabricated identities used by the nodes are called Sybil nodes.

D. Flooding Attack

The malicious node launches this attack by selecting an IP address not present in the network. After the malicious node enters the network it establishes a path between the existing nodes, after establishing the path the attacking node injects a large amount of fake data packets in the network. These packets can result in congesting the network

IV.PROPOSED ALGORITHM

A. Key Management Configuration

MANET is constructed with ‘n’ nodes.

b) Each node is assigned a Private key and a public key.

c) The Nodes have knowledge of their direct neighbours. All the nodes which are present at one-hop distances are recognized as neighbours.

d) For a sending node ‘S’, one relay node is selected, by calculating the distance to the destination node ‘D’.

e) The Sender Node ‘S’ checks the next hop node and forwarding node.

Threshold for UB−THRESHOLD id assignedRead the RSS while sending data packets from source node add a new RSS with Address, rss, time−recv

f)IF Address is not found in the Table THEN

.g) IF rss >= UB−THRESHOLD, then Add−to−Malicious−list(Address

Bcast−Detection−Update(Address)

h) ELSE Add−to−Table(Address)

k) Check private key and accept packet

l) The source Send packets to destination node

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

B. VPNAODV Configuration and Security Setup

a) Source node sends a RREQ packet to the neighbouring node for route identification.

b) Neighbour node verifies RREQ packet.

c) Node distance is calculated to identify neighbouring nodes and to identify optimal hop by hop communication.

d) To stay away from the duplicate RREQ packets at the neighbour nodes the VPNAODV determines the routing packet by classifying relay value and forward value.

e) Relay value and forward values are altered depending on information provided by the duplicate RREQ packets.

f) RREQ packet is modified by organizing source address, destination address and previous interaction details

g) The last address field maintains the last transaction of the forwarded node.

h) The node on reception of a RREQ having a TTL=0 or a duplicate RREQ with the same broadcast ID will result in the review the P-address field in the RREQ.

i) If node address is same as the P-valueddress v in RREQ, then the Relay value of that node will be set to 1. It indicates that the node can now take part in the search of the destination.

j) Else, the node won't participate in the route discovery process.

C.Message Encryption

Message Digest having a hash value of IV is used to supply the data integrity. The message digest produces an preliminary vector value IV which is present with the sending and receiving node. This message digest will be transmitted to the receiving node which will decrypt it.The procedure to obtain the value of message digest as a key is as follows

a) Whenever a node initiates a RREQ,RREP or a RERR An initial vector value of a hash function h' is used to create the message digest

b) The initial vector sets the value of the Hash-Function='h'

c) The initial vector value is used as a key which is available to all nodes.

d) The next data transmission uses the initial vector value of the message digest where 'h' the hash function is a result of function 'h' applied on 'x'

e) When even a node initiates a RREQ,RREP or a RERR it needs to verify the validity of the message by using the initial vector value in order to decrypt the message digest which was available with the target node initially ,the hash value is used to decrypt and verify of the received value is equal to the Message-Digest field of received AODV message present in the Message Digest field.

D.Sending Node

Assumption: Initial Vector (IV) value is available with sender and receiver.

a) When even a node Initialize Counter to IV (for first time only);

b) While (a packet is available to be sent) do;

c) If (first packet);

d) i=0;

e) Encrypt packet using IV as a key;

f) C= E (M, IV);

g) Send packet(C);

h) Continue;

i) Else (second packet onwards)

j) i++;

k) IV'= IV+i;

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

l) H= SHA3 (IV');
m) Encrypt packet using H as a key;
n) C= E (M, H);
o) Send packet(C);
p) Continue;

V.Receiving Node

a) Verify destination of Packet and accept it only if intended destination;
b) Initialize Counter to IV (for first time only);
c) While (there is a packet to be sent) do;
d) If (first packet);
e) i=0;
f) Decrypt packet using IV as a key;
g) M= D (C, IV);

h) Send packet (M);
i) Continue;
j) Else (second packet onwards)
k) i++;
l) IV'= IV+i;
m) H= SHA3 (IV');
n) Decrypt packet using H as a key;
o) M= D(C, H);
p) Send packet (M);
q) Continue;

VI.SIMULATION RESULTS

The results are simulated in the existence of attacks like Wormhole, Flooding, Blackhole and Sybil attacks.We can examine that the Average throughput, End-to-end delay, Energy Consumption Packet drop rate is superior in the case of our protocol VPNAODV even in presence of the attacks mentioned above which is represented by a redline.

A.Average Throughput

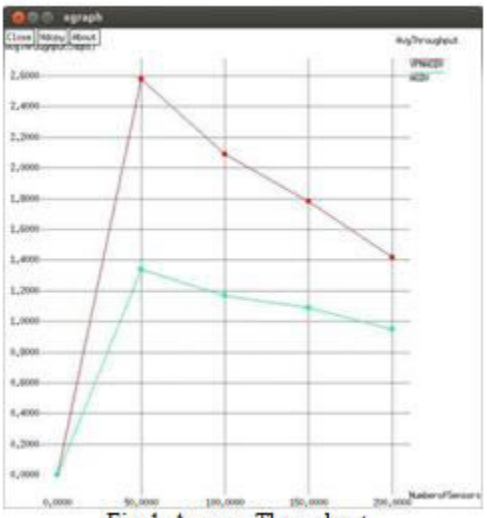

Fig. 1. Average Throughput

B. End to End Delay

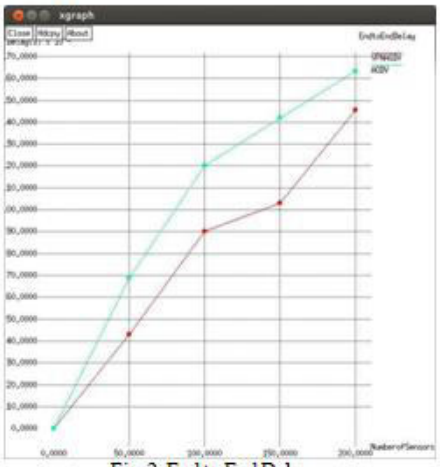

Fig. 2. End to End Delay

C. Energy Consumption

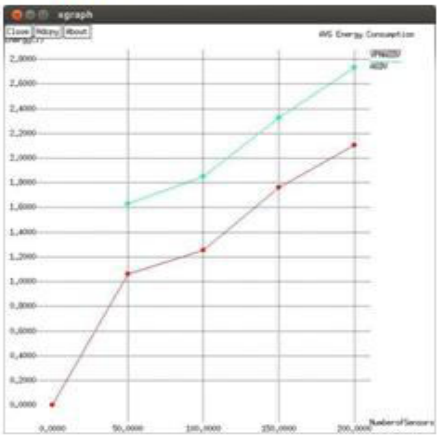

Fig. 3.Energy Consumption

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

D. Packet Drop Rate

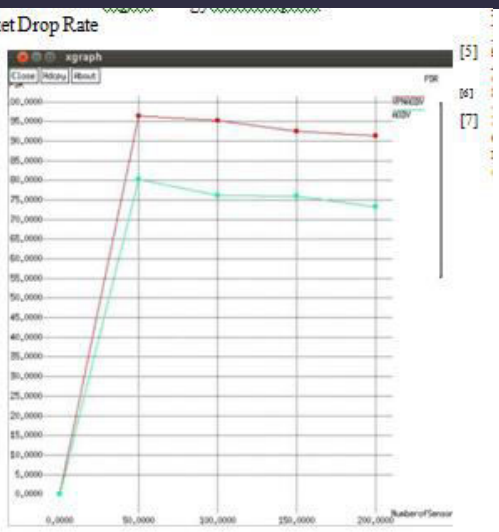

Fig. 4 Packet Drop Rate

ACKNOWLEDGMENT (Heading 5)

I would like to thank Dr.S Krishna Mohan Rao for his constant guidance and support. I would also like to thank all the authors whose work has helped me immensely in my current research.I would like to thank my parents and my family for their support.

REFERENCES

[1] Perkins, C. E. Ad-hoc On-Demand Distance Vector Routing Charles E. Perkins Sun Microsystems Laboratories Advanced Development Group Menlo Park, CA 94025.

[2] Perkins, Charles E. "Ad-hoc On-Demand Distance Vector Routing Charles E. Perkins Sun Microsystems Laboratories Advanced Development Group Menlo Park, CA 94025."

[3] Miss Morli Panday, Ashish Kr. Shriwastava, "A Review on security Issues of AODV routing protocol for MANETs", IOSR Journal of Computer Engineering(IOSR-JCE), vol. 14, no. 5, pp. 127-134, Sep.-Oct. 2013, ISSN 2278-0661

[4] Sharma, P., Sinha, H. P., & Bindal, A. (2014). Detection and Prevention against Wormhole Attack in AODV for Mobile Ad-Hoc Networks. International Journal of Computer Applications,95(13).

[5] Goyal, S., & Rohil, H. (2013). Securing MANET against Wormhole Attack using Neighbor Node Analysis. International Journal of Computer Applications,81(18), 44-48.

[6] Stallings, W. (2006). Cryptography and network security: principles and practices.Pearson Education India.

[7] Singh, U. K., Goswami, D. N., Phuleria, K. C., & Sharma, S. (2014). An analysis of security attacks found in mobile ad-hoc network. International Journal of Advanced Research in Computer Science,5(5).