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 12th Nov 2018. Link
:http://www.ijiemr.org/downloads.php?vol=Volume-07&issue=ISSUE-12

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

Volume 07, Issue 12, Pages: 52–57.
Paper Authors

SARA ALI
Mewar University Gangrar, Chittorgarh, India,hyderabad,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
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

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

SARA ALI
Ph.D Research Scholar,Dept of CSE, Mewar University Gangrar, Chittorgarh, India,hyderabad,India
saraali101@gmail.com

Abstract—Ad hoc on-Demand distance vector routing(AODV) is one of the most commonly used protocol in Mobile Ad Hoc networks(MANETS).However the protocol suffers from security concerns and is open to many security threats.In this paper we propose a novel VPNAODV protocol which uses techniques like Virtual Private Network,Observer nodes and Digital signature in order to safeguard the protocol from attacks like wormhole,blackhole,flooding and Sybil attack.The proposed protocol not only enhances the basic AODV protocol but it also successfully retains the underlying functionality of the algorithm.We have simulated the results using Network Simulator-2 and have compared the results of AODV with our proposed algorithm

Keywords—VPN,Observer,Cluster,Digital Signatures

I.INTRODUCTION

Ad Hoc Distance Vector routing protocol is one of the most frequently used protocol for routing purposes in the MANETS.The nature of the protocol is Reactive which indicates that the updates are shared between the nodes on-demand and not in a periodic manner[1,2].It is very useful in the functioning of the MANETS as each and every node present in the network can behave like a specialized router and can retrieve routes as and when needed.The routes which are provided by the protocol are free of loops .In case of any disintegrated nodes in the network the protocol does not require any advertisements due to which the bandwidth usage is considerable low.The exclusive condition which is applicable to the broadcast medium is the capability of the neighbouring nodes to have the faculty of detecting one anothers broadcast messages.

The principal objective of the algorithm are

- The route discovery packets are broadcasted only when required
- Differentiation must be established between regular topology maintenance ,neighbour discovery and local connectivity management.
- Ability to provide information related to the change in local connectivity to the neighbouring nodes .

II.SECURITY CONCERNS IN AODV

The major security challenge which is faced in the AODV protocol[3] is due to the mutable information present in the control packets.The control packets contain information like the Sequence number and the hop count which are uniquely used to

identify the freshness of the packet.These fields are mutable and expose the protocol to various security attacks,notifications related to improved routes are another feature which can be taken advantage of by the malicious nodes.

A. Destination Sequence Number

when a fresh control packet is received the destination sequence number is compared against the existing destination sequence value present in the route entry table,if the value is found to be greater than the existing one the value in the route entry table is updated and all the nodes are notified of this better route to the destination.This value can be incremented by the malicious node to give an appearance of a better route due to which the route entry table is modified and all the packets get diverted through this fallacious node.

B. Hop Count

The algorithm gives a preference to the packets having a larger value of sequence number and lesser hop count value.This feature can be exploited by the malicious nodes in order to advertise a false path with a smaller hop count by decrementing the current value of hop count.

III. ATTACKS ON AODV PROTOCOL

A. Wormhole Attack

A wormhole attacks [4,5] creates a disturbance in network routing, the nodes get an impression that the advertised link is one or two hops shorter as compared to multiple hops, which may also lead to flooding and packet dropping. These attacks are therefore very dangerous and also are difficult to realise as the wormhole tunnels are private and out of bound in nature hence won't be visible to the network.

B. Blackhole Attack

In this attack the malicious node[6] does not relay the received routing messages but drop them with an intent of reducing the routing information available with the other nodes. The attack is passive in nature .This attack can be launched either randomly,selectively or in bulk thus making the destination unreachable or downgrading the network communication.

C. Sybil Attack

In this kind of attack the malicious node[7] generates false identity for additional nodes in place of a single node. The Identity can be duplicate Id or a fake identity. These fabricated identities acquired by the nodes are called Sybil nodes.

D. Flooding Attack

This is a very serious attack and is very easy to launch . This can be implemented by the node choosing a IP address which is not present in the network. After the attacking node enters the network it sets up a path between existing nodes, after the path gets established the malicious node injects a huge amount of invalid data packets in the network. These packets can end up congesting the network.

IV.PROPOSED ALGORITHM

A.Key Management Configuration

a)Mobile Adhoc Network is constructed with ‘n’ number of nodes.

b)Assign Private key and public key for all nodes

c)Nodes are aware of their direct neighbors. The one-hop neighbors of all the mobile nodes are identified

d)For a sender node 'S', relay node is selected, by checking the distance to the destination node 'D'.

e)Sender Node 'S' checks for next hop node and forwarding node.

f)Assign threshold for UB−THRESHOLD=7

Read the RSS while sending data packets from source node addNewRss (Address, rss, time−recv)

g)BEGIN SUB

h)IF Address is not in the Table THEN

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

Bcast−Detection−Update(Address)

j) ELSE Add−to−Table(Address)

END−IF

END SUB

k)Check private key and accept packet

l)The source Send packets to destination node

B.VPNAODV Configuration and Security Setup

a)Source node sends a RREQ packet to the neighbours for identifying route.

b)Neighbour node will check RREQ packet for future process to reach destination

c)Discovery node distance to identify neighbour nodes and to identify optimal hop by hop communication.

d)In order to avoid the duplicate RREQ packets at neighbour nodes, VPNAODV determines the routing packet by classifying relay value and forward value.

e)Relay value and forward values are changed based on information provided in the duplicate RREQ packets.

f)We modify RREQ packet format by organizing source address, destination address and previous interaction details

(P) (Last address).

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

h)The node on receiving a RREQ having a TTL=0 or receives a duplicate RREQ having the same broadcast ID it will review the P-address field in the RREQ.

i)If node address is same as the P-alueddress v in RREQ, then the Relay value of that node will be set to 1. It means that the node can now participate 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 provide the data integrity.The message digest produces a initial vector value IV which is present with the sender and receiver and this message digest will be transmitted to the receiving node which will decrypt it.The process to obtain the value of message digest as a key is as follows

a)When even a node initiates a RREQ,RREP or a RERR An initial vector value of a hash function h' is utilized 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'

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

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;
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 generated in the presence of attacks like Wormhole,Flooding,Blackhole and Sybil attacks. We can observe that the the Average throughput,End-to-end delay,Energy Consumption Packet drop rate is better in the case of our protocol VPNAODV in presence of the attacks mentioned above which is represented by a redline.

A.AverageThroughput

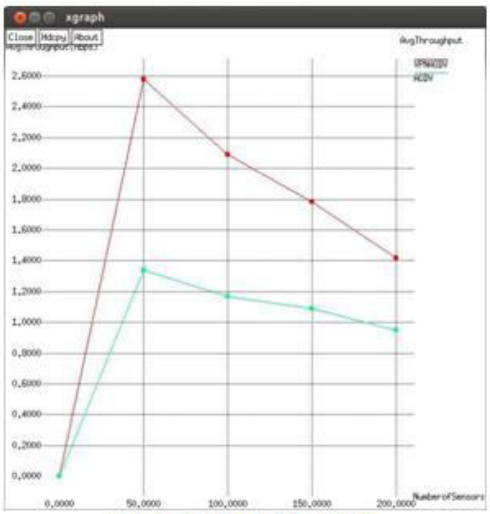

Fig. 1. Average Throughput

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

B. End to End Delay

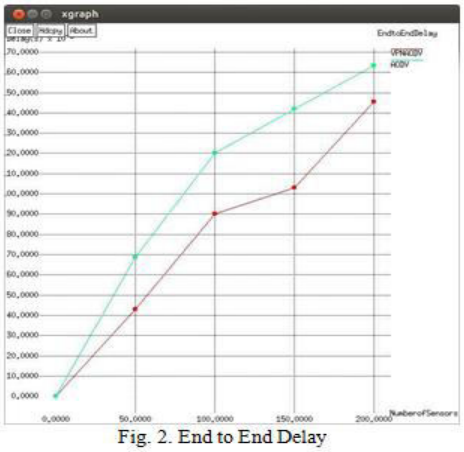

Fig. 2. End to End Delay

C. Energy Consumption

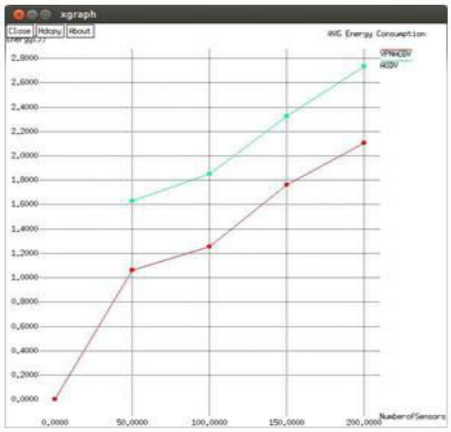

Fig. 3.Energy Consumption

D. Packet Drop Rate

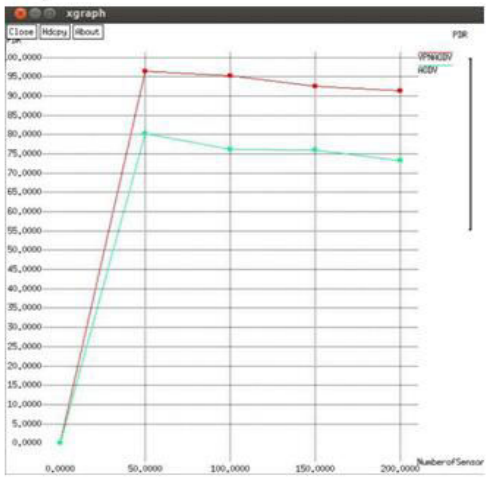

Fig. 4.Packet Drop Rate

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).