IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Volume 11, PP 27-30

Network Performance Improvement in AODV with Improved Weighted Clustering

Supriya Dicholkar[1], Payal Mohadikar[2], Deepthi Sekhar[3], Payal Varangaonkar[4]
Poonam Chaudhari[5]

[1](Electronics And Communication Dept., Atharva College Of Engineering/ Mumbai University, India)
[2](Electronics And Communication Dept., Atharva College Of Engineering/ Mumbai University, India)
[3](Electronics And Communication Dept., Atharva College Of Engineering/ Mumbai University, India)
[4](Electronics And Communication Dept., Atharva College Of Engineering/ Mumbai University, India)
[5](Electronics And Communication Dept., Thakur Polytechnic/ Mumbai University, India)

Abstract : *Mobile Ad-Hoc Network Is Integral Part Of Growing Wireless Communication Network .Different Protocols Available In MANET Are DSDV, DSR, AODV, TORA. MANET Is Infrastructure Less Mobile Network Without Centralized Administration So Security Is Main Concern In MANET. Research Work Is Carried Out MANET Security As It Is Used For Most Crucial Military Operations And Rescue Operations. In This Paper We Are Focusing On Different Attacks On AODV And Security Measures Taken Against Them For Network Performance Improvement.*

Keywords – *Mobile Ad-Hoc Network, Wormhole Attack, Ad-Hoc On Demand Distance Vector*

I. INTRODUCTION

A Mobile Ad Hoc Network (MANET) Is A Network Consisting Of A Set Of Mobile Hosts Communicating With Each Other Without Centralized Administration. MANET Consists Of Mobile Nodes That Can Dynamically Self Organize Into Arbitrary Ad-Hoc Network Topologies. MANET Can Be Used In Disaster Recovery Environments Where Preexisting Communication Infrastructure Is Not Available Or Preexisting Network Infrastructure Requires Wireless Extensions[1].

There Are Three Types Of Routing Protocols- Proactive Protocols, Reactive Protocols And Hybrid Protocols. Proactive Protocols (Table-Driven Protocols) Maintain Routing Table For All Nodes, Including Nodes To Which No Packets Are Sent So They Can Easily Adopt Topology Changes. Reactive Protocols (On Demand Protocols) Determine The Routes Between Hosts Only When There Is Demand For Data Transmission Reducing Routing Overhead. Hybrid Protocols Are Combination Of Both Proactive And Reactive Protocol Properties. MANET Has Limited Resources Such As Energy And Bandwidth. So Adaption Of Suitable And Efficient Routing Protocol Is Very Essential [2].

II. AD-HOC ON DEMAND DISTANCE VECTOR

Ad-Hoc On Demand Distance Vector (AODV) Is A Well-Known Reactive Protocol With Less Bandwidth Requirement Than Other Proactive Protocols. It Is A Modification Of DSDV. It Enables Multi-Hop, Self-Starting And Dynamic Routing In Manets. AODV Is Very Efficient In Networks With Large Number Of Mobile Nodes As It Relies On Dynamically Establishing Route Table Entries At Intermediate Nodes. Source Node That Wants To Communicate With A Destination Node Relies On Sequence Numbers For Route Discovery. After A Specific Interval Of Time, Each Node Broadcasts A HELLO Message To Keep Track Of Its Neighbors. Thus A Node Keeps Track Of Only Its Next Hop For A Route Instead Of Entire Route. Node Use A Route Request Packet Called RREQ Which Contains RREQ ID, Destination IP Address, Destination Sequence Number, Source IP Address, Source Sequence Number And Hop Count When Wants To Communicate With A Node That Is Not Its Neighbor. Route Table Is Updated Continuously For Node Receives RREQ, RREP Or RRER With Latest Sequence Number For The Nodes In The Network. Hop Count Represents The Distance In Hops From The Source To Destination.

When A Node Receives An RREQ, It Checks That Whether It Has Already Received An RREQ With The Same Source IP Address And RREQ ID Within PATH_DISCOVERY_TIME. If Yes, It Discards The Newly Arrived RREQ. If Not, It Increments The Hop Count Value In RREQ By One. The Route Table Entry For The Destination Will Be Updated With The New Sequence Number If:

1. Destination Sequence Number Received From RREQ Is Greater Than The Existing Value In The Route Table Entry.
2. The Sequence Numbers Are Equal, But The Incremented Hop Count Is Smaller Than Existing Hop Count.
3. The Sequence Number Is Unknown [7].

III. SECURITY ATTACKS AGAINST AODV

Manets Being Unwired Network Are Vulnerable To MANET Attacks. These Attacks Are Broadly Divided Based On Protocol Layer And Functionality. In Protocol Layer Each Layer Is Undergoing Attack. Denial Of Service (Dos) Attacks And Preventing Signal Jamming Are Security Attacks At Physical Layer. Network Layer Has To Deal With Security Of Ad-Hoc Routing Protocol. End To End Data Security With Encryption Methods And Authentication Are Security Concern At Transport Layer. Prevention, Worms, Malicious Codes, Application Abuses As Well As Virus Detection Are Security Threats At Application Layer.

Depending On Functionality, There Are Two Kinds Of Attacks Passive And Active. In Passive Attack, There Is No Change In The Functionality Of The Network. Attacker Sneaks Data Without Altering It. Active Attacks Can Be Carried Out Either By Nodes Within The Network Or By Nodes Outside The Network. Modification, Impersonation And Fabrication Are Some Of The Most Common Active Attacks That Cause A Big Security Concern For MANET.

3.1 Attacks Using Modification

AODV Uses The Hop Count Parameter To Determine The Shortest Path. A Node May Attack By Altering Hop Count Values In The Protocol Field Messages Or Routing Messages With False Values. Redirection Of Network Traffic Is Carried Out By A Malicious Node By Setting The False Hop Counts Or False Value Of Route Sequence Numbers. A Dos Attack May Be Launched By Modifying Source Routes As Well. Dos Attack Is Easy To Carry Out But It Is Difficult To Detect.

3.2 Attacks Using Impersonation

A Malicious Attacks In MANET Are Carried Out By Impersonating A Node (Spoofing),. For Example, Traffic That Belongs To The Impersonated Node May Be Redirected To The Malicious Node. Spoofing May Also Be Used To Create Loops. The Malicious Node May Take Up Identity Of Multiple Nodes; It Does Not Need To Impersonate Any Node Of The Network.

3.3 Attacks Using Fabrication

Fabrication Attacks Are Carried Out By An Intruder. An Intruder Generates False Routing Information Such As False Route Error Messages (RERR). When Route Updation Will Start, It Will Disturb The Network Operations Or Consume Node Resources.Well-Known Fabrication Attacks Are As Below:

3.3.1Black Hole Attacks

In Black Hole Attack, A Malicious Node (Black Hole) Falsely Replies For Route Requests From An Active Route And Tries To Become An Element Of An Active Route. Black Hole Then Try To Disrupt Data Packets Being Sent To The Destination Node Or Obstructing The Route Discovery Process. Many Neighbor Black Holes Cooperates With Each Other Can Cause Cooperative Black Hole Attack. Black Hole Attack May Be Internal Or External.

3.3.2 Gray Hole Attacks

In A Gray Hole, A Malicious Node Sometimes Forwards All Packets To Certain Nodes But May Drop Packets Coming From Or Destined To Specific Nodes. A Gray Node May Behave Maliciously For Some Time But Later On It Behaves Absolutely Normally. These Types Of Attacks Are More Difficult Compared To Black Hole Attack Due To Uncertainty In Behavior Of Gray Hole.

3.1.3 Wormhole Attacks

In Wormhole Attack, The Attackers Disturb The Usual Flow Of Routing Packets. "Wormhole Link" Is Used By Two Or More Attackers To Connect Existing Network. They Capture Packets At One End And Replay Them At The Other End Using Private High Speed Network. Wormhole Attacks Can Be Easily Deployed And Can Cause Great Damage To The Network[11].

IV. OPERATION OF WORMHOLE ATTACK IN AODV

Wormhole Attack Is A Most Challenging Replay Attack In MANET. Even If, The Routing Information Is Confidential, Encrypted Or Authenticated, It Can Be Very Effective And Damaging. An Attacker Sends A Request Packet RREQ Directly To The Destination Node Without Increasing The Hop-Count Value. Thus It Prevents Any Other Routes From Being Discovered. AODV Would Be Unable To Find Routes Longer Than One Or Two Hops. It Is Easy For The Attacker To Make The Tunneled Packet Arrive With Better Metric Than A Normal Multi-Hop Route For Tunneled Distances Longer Than The Typical Transmission Range Of A Single Hop. Malicious Nodes Can Retransmit Eavesdropped Messages Again In A Channel That Is Exclusively

Available To Attacker. Destination Node Does Not Receive Packets If Wormhole Attack Is Merged With The Message Dropping Attack.

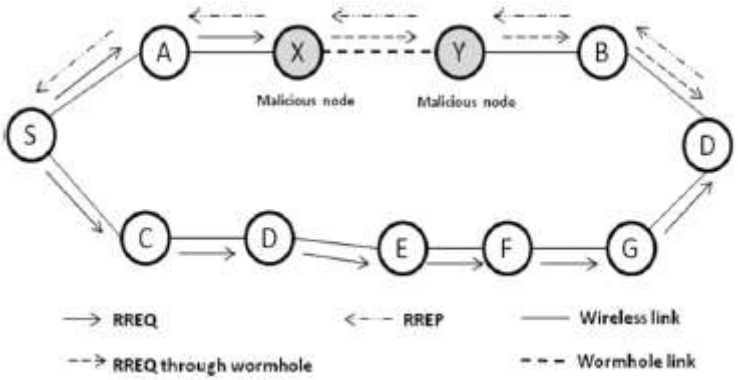

Figure- Wormhole Attack On AODV In MANET

Wormhole Attack Is Carried Out With Two Remote Malicious Nodes Shown As X And Y In Figure. X And Y Both Are Connected Via A Wormhole Link. During Path Discovery Process, If Malicious Nodes X And Y Wants To Attack On Source S. Initially Source S Broadcasts RREQ To A Destination Node D. Neighbors Of S Namely A And C Receive RREQ And Forward RREQ To Their Neighbors. After Receiving RREQ Forwarded By A, Malicious Node X Records RREQ And Tunnels The RREQ Via The High-Speed Wormhole Link To Its Partner Y. Malicious Node Y Forwards RREQ To Its Neighbor B. Finally, B Forwards It To Destination D. Thus, RREQ Is Reaching Destination D Via S-A-X-Y-B-D Very Fast As Compared To RREQ From S-A-X-Y-B-D Reaches Destination To D. Thus, Setting Wormhole Attacks In MANET Is Very Easy And Affect MANET Network At Large Extent.Hence Detection Of Wormhole Attacks And Securing AODV Against Them Still Remains A Big Challenge In Mobile Ad-Hoc Networks.

V. WEIGHT CALCULATION ALGORITHM FOR SECURITY OF AODV

In Weight Calculation Algorithm Three Parameters Namely Energy, Connectivity And Buffer Length Of Nodes Is Considered.WCA Algorithm Is Divided In Two Steps Primary Weight Calculation And Cluster Head Selection. In First Step Of Weight Calculation Process, Depending On Energy, Mobility And Buffer Size Weight For Each Node Is Calculated.

In Cluster Head Selection Process, Memory, Buffer, Connectivity And Mobility For Each Node Is Calculated. Weights For All The Nodes Are Found Out. If Node Weight Is Maximum Than Cl-Head =1 Else Cl-Head=0. In This Way Decide Cluster Head. Cluster Head Decides Threshold For Network.

If At The Time Of Receiving Request From Another Node If Any Node Send RREQ Packets More Than Estimated Threshold Then Add These Nodes To Blacklist And Do Not Receive Any Request From This Node[13].

VI. CONCLUSION

MANET With Mobile Nodes Is Fastest Growing Wireless Solution Where Existing Network Is Unavailable Different MANET Protocols Such As DSDV, TORA, AODV Are Available For Management Of Mobile Nodes. AODV Is Well Known Reactive Protocol With Less Bandwidth Requirement. Spoofing, Fabrication, Black Hole Attacks, Grey Hole Attack, Worm Hole Attacks These Are Some Threats To AODV Protocol. Worm Hole Attack Is Most Frequent And Dangerous Attack Among All. Weighted Calculation Algorithm Is Used For Security Against Worm Hole Attack. In Worm Hole Attack Depending On Energy, Mobility And Buffer Length Threshold Weight For Path Is Calculated And If Any Node Send RREQ Packets More Than Estimated Threshold Add That Node In Blacklist And Preserve Security Of Network.

REFERENCES:

Journal Papers:

[1] Salim M Zaki, Mohd Asri Ngadi, Shukor Abd Razak," A Review Of Delay Aware Routing Protocols In MANET", Computer Science Letter,Vol.1,2009

[2] Lee, S., Gerla, M., (2001), "Split Multipath Routing With Maximally Disjoint Paths In Ad Hoc Networks", Communications, ICC 2001. IEEE International Conference On, Pp. 3201-3205, Vol.10. [21]

[3] K. J. Lee, M. S. Kim, S. Y. Cho, B. I. Mun, (2005), "Delay-Centric Link Quality Aware OLSR", Proceedings Of The IEEE Conference On Local Computer Networks 30th Anniversary, Pages: 690 – 696.

[4] Rajiv Misra And C.R. Mandal, "Performance Comparison Of ADOV/DSR On-Demand Routing Protocols For Ad Hoc Networks In Constrained Situation"

[5] Khin Sandar Win," Analysis Of Detecting Wormhole Attack In Wireless Networks", World Academy Of Science, Engineering And Technology 48, Pp. 422-428, 2008
[6] Mohd Anuar Jaafar And Zuriati Ahmad Zukarnain,"Performance Comparisons Of AODV, Secure AODV And Adaptive Secure AODV Routing Protocols In Free Attack Simulation Environment", European Journal Of Scientific Research, Pp. 430-443, 2009
[7] Luke Klein-Berndt, "A Quick Guide To AODV Routing"
[8] Charles E. Perkins And Elizabeth M. Royer, "Ad-Hoc On-Demand Distance Vector Routing"
[9] Yih-Chun Hu, Adrian Perrig And David B. Johnson,"Wormhole Attacks In Wireless Networks", IEEEJOURNAL ON SELECTED AREAS IN COMMUNICATIONS, Pp.370-380,2006
[10] Komala CR, Srinivas Shetty, Padmashree S., Elevarasi E., "Wireless Ad Hoc Mobile Networks", National Conference On Computing Communication And Technology, Pp. 168-174, 2010
[11] Rutvij H. Jhaveri, Ashish D. Patel, Jatin D. Parmar Bhavin I. Shah "MANET Routing Protocols And Wormhole Attack Against AODV", IJCSNS International Journal Of Computer Science And Network Security, VOL.10 No.4, April 2010.
[12] Emmanouil A. Panaousis, Levonnazaryan, Christos Politis,"Securing AODV Against Wormhole Attacks In Emergency MANET Multimedia Communications", Mobimedia,London, U.K., Vol - 09, Pp (7-9), Sept 2009
[13] Basant Kumar Verma, Binod Kumar, "An Improved Weighted Clustering For Ad-Hoc Network Security New, International Journal Of Computer Sciences And Engineering Open Access", Vol. 3. Issue 3,2015,51-55