ISSN No. 0976-5697

Volume 4, No. 5, May 2013 (Special Issue)

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

Stable and Secure AODV protocol for MANET

A.Ravali
M.Tech(CSE)
School of IT, JNTUH
Hyderabad, India
ankamravali87@gmail.com

K. Suresh Babu
Assistant Professor in CSE
School of IT, JNTUH
Hyderabad, India
kare_suresh@yahoo.co.in

Abstract: This paper presents a new Stable and Secure Routing Strategy for AODV protocol. This has been designed to overcome the flaws in basic AODV protocol. The proposed scheme is based on modifications to existing AODV. Two parameters have been used, one for stability and other for security. Security has been achieved using one-way hash chains and stability by using Hello packets. Thus this strategy ensures stable and secure routing over the MANET.

Keywords: MANET, Routing, Secured, Stable

I. INTRODUCTION

A Mobile Ad hoc Network (MANET) is a collection of self configurable mobile node connected through wireless links. In MANET nodes which are within the range of each other can connect directly where as nodes which are not in the vicinity of each other rely on the intermediate node for communication Figure.1. Some special characteristics of MANET like dynamic topology, fast deployment, robustness make this technology an interesting research area. Each node in MANET can work as a sender, receiver as well as router Figure 1. Communication in the network depends upon the trust on each other. Communication can work properly if each node co-operate for data transmission.

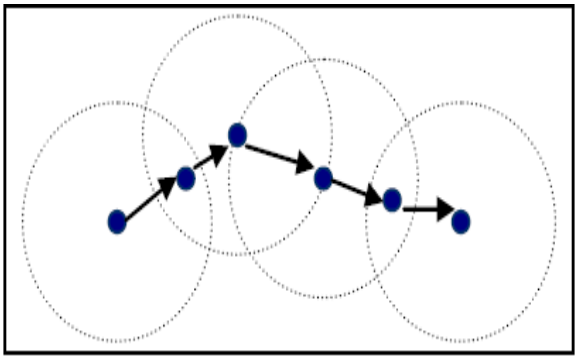

Figure1: Communication in Mobile Adhoc Networks

The following algorithm depicts the communication in any adhoc network:

1. Sender node sends the signal to the neighbouring nodes within the vicinity.
2. Neighbouring nodes communicate with the sender node
3. Sender node sends the message to the destination node.
4. If destination node is within the vicinity then message received by the destination node else an intermediate node receives the message.
5. Restart the process of forwarding the message from step no 1 till the destination node is reached.

As MANET has no fixed infrastructure, they are more prone towards the security threats as compared to the infrastructure wireless networks. Providing security in MANET is a difficult task to achieve due to its dynamic nature, lack of centralized monitoring, and limited resources like bandwidth and battery power.

This paper is divided into three major sections. First section will describe AODV protocol. Second section will describe Security issues in AODV. Third section describes about the proposed solution.

II. OVERVIEW OF AODV PROTOCOL

AODV is a reactive protocol, when a node wishes to start transmission with another node in the network to which it has no route; AODV will provide topology information for the node. AODV use control messages to find a route to the destination node in the network. There are three types of control messages in AODV which are discussed below.

Route Request Message (RREQ):

Source node that needs to communicate with another node in the network transmits RREQ message. AODV floods RREQ message, using expanding ring technique. There is a time to live (TTL) value in every RREQ message, the value of TTL states the number of hops the RREQ should be transmitted.

Route Reply Message (RREP):

A node having a requested identity or any intermediate node that has a route to the requested node generates a route reply RREP message back to the originator node.

Route Error Message (RERR):

Every node in the network keeps monitoring the link status to its neighbour's nodes during active routes. When the node detects a link crack in an active route, (RERR) message is generated by the node in order to notify other nodes that the link is down.

Route Discovery Mechanism in AODV:

When a node "A" wants to initiate transmission with another node "G" as shown in the Fig. 3 , it will generate a route request message (RREQ). This message is propagated through a limited flooding to a node that has a fresh enough route to the destination or destination node is located itself other nodes. This control message is forwarded to the neighbors, and those node forward the control message to their neighbors' nodes. This process of finding destination

CONFERENCE PAPER
"National Conference on Networks and Soft Computing"
On 26-27 Feb 2013
Organized by
Vignan University, India

node goes on until it finds. Once the destination node is located or an intermediate node with enough fresh routes is located, they generate control message route reply message (RREP) to the source node. When RREP reaches the source node, a route is established between the source node "A" and destination node "G". Once the route is established between "A" and "G", node "A" and "G" can communicate with each other. Fig. 2.4 depicts the exchange of control messages between source node and destination node.

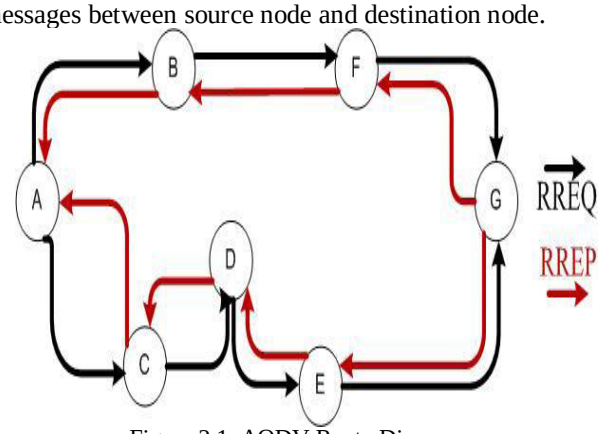

Figure 2.1 AODV Route Discovery.

When there is a link down or a link between destinations is broken that causes one or more than one links unreachable from the source node or neighbours nodes, the RERR message is sent to the source node. When RREQ message is broadcasted for locating the destination node i.e. from the node "A" to the neighbours nodes, at node "E" the link is broken between "E" and "G", so a route error RERR message is generated at node "E" and transmitted to the source node informing the source node a route error, where "A" is source node and "G" is the destination node. The scheme is shown in the Fig.2.5 below.

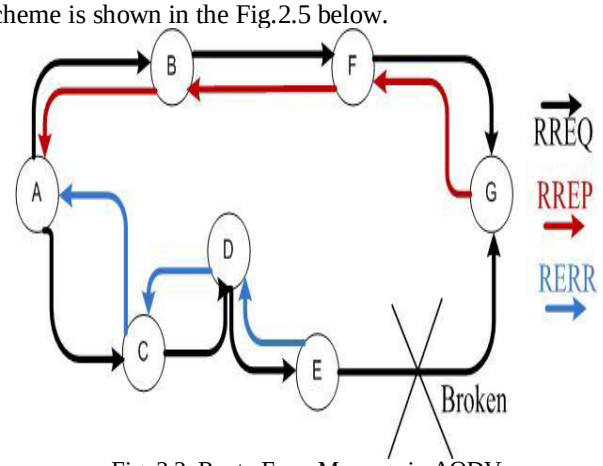

Fig. 2.2 Route Error Message in AODV

III. SECURITY FLAWS OF AODV

Since AODV has no security mechanisms, malicious nodes can perform many attacks just by not behaving according to the AODV rules. A malicious node M can carry out the following attacks (among many others) against AODV:

1. Impersonate a node *S* by forging a RREQ with its address as the originator address.
2. When forwarding a RREQ generated by *S* to discover a route to *D*, reduce the hop count field to increase the chances of being in the route path between *S* and *D* so it can analyze the communication between them. A variant of this is to increment the destination sequence number to make the other nodes believe that this is a 'fresher' route.
3. Impersonate a node *D* by forging a RREP with its address as a destination address.
4. Impersonate a node by forging a RREP that claims that the node is the destination and, to increase the impact of the attack, claims to be a network leader of the subnet *SN* with a big sequence number and send it to its neighbours. In this way it will became (at least locally) a black- hole for the whole subnet *SN*.
5. Selectively, not forward certain RREQs and RREPs, not reply to certain RREPs and not forward certain data messages. This kind of attack is especially hard to even detect because transmission errors have the same effect.
6. According to the current AODV, the originator of a RREQ can put a much bigger destination sequence number than the real one. In addition, sequence numbers wrap around when they reach the maximum value allowed by the field size. This allows a very easy attack in where an attacker is able to set the sequence number of a node to any desired value by just sending two RREQ messages to the node.
7. The originator of a RREQ can put a much bigger destination sequence number than the real one. In addition, sequence numbers wraparound when they reach the maximum value allowed by the field size. This allows a very easy attack in where an attacker is able to set the sequence number of a node to any desired value by just sending two RREQ messages to the node.

IV. PROPOSED STABLE AND SECURE ROUTING STRATEGY

The proposed scheme is based on modifications of existing AODV. Two parameters have been used, one for stability and other for security. The proposed protocol,ensures stable and secure routing over the adhoc network.

In AODV protocol, it is assumed that the malicious node has exceptionally large sequence number. Whenever a malicious node joins the network, the packets start dropping and link path breakage happens as shown in figure 4.1.

Whenever a link path breakage occurs, stable routing is achieved with an alternate route selection using neighbor nodes. If there is an attack on security of the network, the hash key chain mechanism is used to ensure secure routing. This has been shown in figure 4.2.

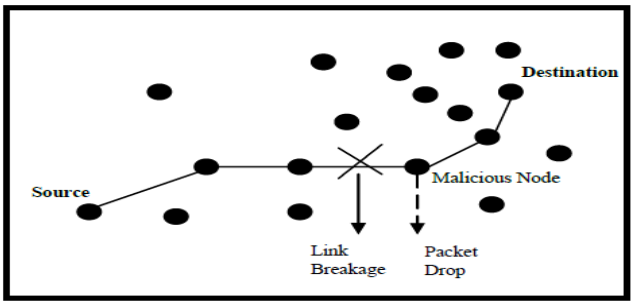

Figure 4.1.Route prior to malicious node entry in AODV

CONFERENCE PAPER
"National Conference on Networks and Soft Computing"
On 26-27 Feb 2013
Organized by
Vignan University, India

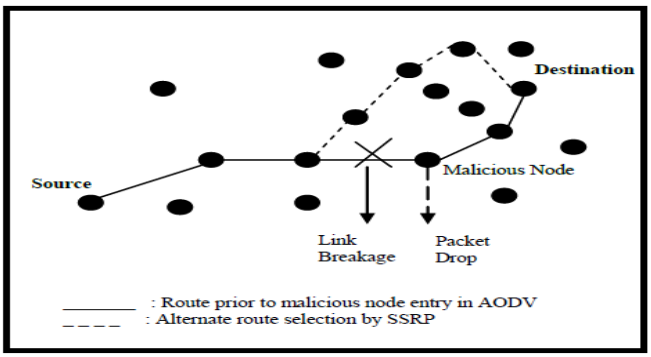

Figure 4.2.Route recovery using alternate path in SSRP

Steps to achieve Stability:

Following modifications are incorporated in AODV to make it stable.

1. In original AODV protocol, every node periodically broadcasts HELLO messages. Every node keeps counts of how many HELLO messages it has received from each of its neighbors.
2. RREQ packet is modified. It has one field known as "stability". When a node forwards RREQ, it adds the count of HELLO packets (that it received from predecessor) into stability field.
3. When destination receives RREQ, it calculates average stability as follows: Average stability = Cumulative stability value in RREQ / hop count.
4. Route Reply (RREP) is also modified to contain "stability" field. Destination copies average stability in "stability" filed and RREP is sent to source.
5. Source begins data transmission as soon as it receives first RREP. When it receives RREP with better "stability" value, it switches to new stable route.

Implementation of security:

Hashing technique is used to secure the adhoc networks. A unique way of using hash functions as 'one way hash chain' has been used in the proposed work. Hash key chains are constructed by using only symmetric cryptographic primitives, namely hash functions. Hash functions MD5, SHA1,etc can be used. A hash key chain is configured as a recursive chain, where the node first chooses a random key, K1. Subsequent keys are calculated by calculating the one-way hash over the key as given in equation.

K2=H [K1], K3=H [K2], ……, KN=H[KN-1].

Each node discloses each key of its one-way key chain in a particular order, which is exactly reverse of the order in which the keys were generated. The key disclosure schedule and key generation schedule should be reverse For example if the keys were generated by a node in the order KN; KN-1; ⋯..K1; K0 then the node disclose them in the order K0; K1; ...: KN. The rationale behind having the key disclosure schedule to be reverse of the key generation schedule is that KN of a node is known to all other nodes and in such a situation they should be able to authenticate any subsequent keys that are disclosed. The use of one way hash function allows K0; K1 ;… ;KN-1 to be authenticated using KN but KN cannot be authenticated using any other key value. Hence the key disclosure schedule and key generation schedule is reverse.

V. PERFORMANCE METRICS

RF C 2501 describes a number of quantitative metrics that can be used for evaluating the performance of a routing protocol for mobile wireless ad-hoc networks. Some of these quantitative metrics are defined as follow:

Packet Delivery Fraction (PDF): The packet delivery fraction is defined as the ratio of number of data packets received at the destinations over the number of data packets sent by the sources as given in equation. This performance metric is used to determine the efficiency and accuracy of MANET's routing protocols.

PDF = (Total Data Packets Received / Total Data Packets sent) X 100

Throughput: A network throughput is the average rate at which message is successfully delivered between a destination node (receiver) and source node (sender). It is also referred to as the ratio of the amount of data received from its sender to the time the last packet reaches its destination. Throughput can be measured as bits per second (bps), packets per second or packet per time slot. For a network, it is required that the throughput is at high-level. Some factors that affect MANET's throughput are unreliable communication, changes in topology, limited energy and bandwidth.

Throughput = Number of bits received/second

Packet loss rate: Packet loss occurs when one or more packets being transmitted across the network fail to arrive at the destination. It is defined as the number of packets dropped by the routers during transmission.

Packet Loss = Total Data Packets Dropped.

Packet Loss = Total Data Packets Sent –Total Data Packets Received.

Packet Loss (%age) = (Total Packets Dropped /Total Data Packets Sent) X 100.

*Average End-to-*End *Delay (AE2ED):* This is the average time involved in delivery of data packets from the source node to the destination node. To compute the average end-to-end delay, add every delay for each successful data packet delivery and divide that sum by the number of successfully received data packets as given in equation. This metric is important in delay sensitive applications such as video and voice transmission.

Average End to End Delay = ∑(Time Received - Time Sent) / Total Data Packets Received.

Normalized Routing Load (NRL): The normalized routing load is defined as the fraction of all routing control packets sent by all nodes over the number of received data packets at the destination nodes. In other words, it is the ratio between the total numbers of routing packets sent over the network to the total number of data packets received as given in equation. This metric discloses how efficient the routing protocol is. Proactive protocols are expected to have a higher normalized routing load than reactive ones. The bigger this fraction is the less efficient the protocol.

Normalized Routing Load = Total Routing Packets Sent / Total Data Packets Received.

VI. CONCLUSION

The existing routing protocols are typically attack-oriented. They first identify the security threats and then enhance the existing protocol to conquer such attacks. Since

CONFERENCE PAPER
"National Conference on Networks and Soft Computing"
On 26-27 Feb 2013
Organized by
Vignan University, India

the solutions are designed explicitly with certain attack models in mind, they work well in the presence of designated attacks but may collapse under unanticipated attacks. Therefore, the ultimate goal for adhoc network security is to develop a multifold security solution that results in in-depth protection that offers multiple lines of defense against both known and unknown security threats. AODV is vulnerable to various kinds of attacks as it based on the assumption that all nodes must cooperate and without their cooperation no route can be established.

In addition, when the malicious nodes enter into the network, various performance metrics begin decreasing for AODV. The objective of this project is to find a multifold security solution by developing a new on-demand stable and secure routing strategy.

VII. REFERENCES

[1] T. Karygiannis and L. Owens, "Wireless Network Security", NIST Special Publication, 2002.

[2] William Stallings, "Cryptography and Network Security: Principles and Practice", Prentice Hall,5th Edition, 2011.

[3] B. Dahill, B. N. Levine, E. Royer and C. Shields, "A secure routing protocol for adhoc networks", Technical Report UM-CS-2001-037,University of Massachusetts, Department of Computer Science,2001.

[4] P. Papadimitratos and Z. J. Haas, "Secure Routing for Mobile Adhoc Networks", SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), 2002.

[5] Adrian Perrig, D. B. Johnson, Yih-Chun Hu, "ARIADNE: A Secure On-demand Routing Protocol for Adhoc Networks", ACM, Proceedings of the Eighth Annual International Conference on Mobile Computing and Networking (MobiCom 2002), 2002.

[6] L. Zhou and Z. J. Haas, "Securing Adhoc Networks", IEEE Network Magazine, 13(6), pp. 24–30, 1999.

[7] S.Marti, T. J. Giuli, K. Lai and M. Baker, "Mitigating Routing Misbehavior in Mobile Adhoc Networks", Proceedings of the Sixth Annual International Conference on Mobile Computing and Networking, pp. 255–265, 2000.

[8] Bayya Arun, "Security in Ad-hoc Networks", Computer Science Department, University of Kentucky.

[9] Yih-Chun Hu, D. B. Johnson, and A. Perrig, "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Adhoc Networks", IEEE Workshop on Mobile Computing Systems and Applications(WMCSA), pp. 3-13, 2002.

[10] Manel Guerrero Zapata, N. Asokan, "Securing Adhoc Routing Protocol", WiSe 2002.

[11] Kush A., Hwang C., "Proposed Protocol for Hash-Secured Routing Adhoc Networks", Masaum Journal Of Computing (MJC), Volume 1, Issue 2, pp.221-226, 2009.

[12] Kush A., Gupta P., Hwang C., "Secured Routing Scheme for Adhoc Networks", International Journal of Computer Theory and Engineering (IJCTE),Volume 3. pp. 1793-1799, 2009.

CONFERENCE PAPER
"National Conference on Networks and Soft Computing"
On 26-27 Feb 2013
Organized by
Vignan University, India