International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

New Improved Secure Routing Technique for Securing MANET

Dept. of Urban Planning and Architecture in the subject of Computer Science
State University of Performing and Visual Arts Rohtak

Abstract
This gives detailed assessment of the proposed protocol and explains how the proposed protocol provides stable and secure routes and discovering route maintenance for on-demand routing protocol. After assessing the working of the proposed scheme the chapter concludes with highlighting certain possible achievements in secure routing.

Keywords: Proactive, Reactive, AODV, Security, RAODV

Introduction

In ad-hoc network routing is an important operation, being the foundation of data exchange between wireless devices. Each wireless node acts as a router and participates in the routing protocol. Routing relies on an implicit trust relationship among participating devices, but achieving a secure routing protocol in the ad-hoc wireless networks is challenging because of the limited wireless transmission range, broadcast nature of the wireless medium, node mobility, limited power resources, and limited physical security. [1]

Extensive work has been carried out to make MANET routing secured. It was found that not one method can achieve the target. Many combinations were tried and it was found that each protocol behaves differently in each proposed plan. New scheme is incorporated on AODV [2] because most of the work has been carried out using AODV as a base protocol. Proposed Scheme is compared with existing AODV without malicious nodes, with malicious nodes and results are analysed. It was found malicious nodes are big issue in MANET routing. These malicious nodes drop the packets by using fake routes and it is very difficult to identify a malicious node.

Existing MANET Protocols

Table-Driven Routing Protocols (Proactive) [3]

On Demand Routing Protocols (Reactive) [4]

A portion of the current table driven or proactive conventions are: DSDV [5], WRP[6] and OLSR[7]. In the Reactive convention a hub finds or keeps up with course to an objective if and provided that it is the initiator of the course to that objective or is a middle hub on a functioning course to that objective. Any other way, it doesn't keep up with steering data or directing action at the organization hubs in case there is no correspondence. The course revelation normally happens by flooding the course demand parcels all through the organization well known ones are: AODV[8], DSR[9] and TORA[10].

There exist a few recommendations that endeavor to designer a safe steering convention for specially appointed organizations, to offer security against the different attacks.

- **Authenticated Routing for Ad-hoc Networks (ARAN) [11]**
- **Security-Aware Ad-hoc Routing (SAR) [12]**
- **Secure Routing Protocol (SRP) [13]**
- **Secure and Efficient Ad-hoc Distance vector (SEAD) [14]**
- **Secure Link State Routing Protocol (SLSP) [15]**
- **Secure AODV (SAODV) [16]**
- **ARIDANE [17]**

The examination of the various recommendations demonstrates that the plan of a solid specially appointed directing

Reverse on Demand Distance Vector (RAODV)

This section, proposes a methodology RAODV for identifying malicious nodes with slightly modified MAODV protocol. The solution that proposes here is designed to detect the malicious nodes in the default operations of either the intermediate nodes or either that of the Destination node.

In RAODV every node has a sequence number. When a node wants to send data to any other node then RAODV set status of each node, participating in the routing process. It sets status of node as 'TRUE' whose sequence number is in between 'Source Node Sequence Number' and 'Destination Node Sequence Number'. Otherwise it set status of this node as 'FALSE'.

RAODV successfully detects and removes malicious nodes and generates a new path. This new path will be secured and will result in stable and secured routing. It starts with route request to search shortest path. Two arrays are used in this phase, first for malicious nodes and second for non malicious nodes. At the time of route request nodes are verified one by one for checking nodes status. If node status is 'TRUE' then this node enters in to the NonMalicious_Array and if node status is 'FALSE' then this node enters in to the Malicious_Array.

In Route Reply phase all the possible routes will be searched by RREP. Then available route will be selected by the RREP for broadcasting. It repeats procedure until it reaches to Source node. Source node will select the path for data transmission based on the shortest path algorithm, if more then one paths are available. After establishing a path transmission starts between Source node and Destination node.

When transmission starts between Source and Destination, RAODV verifies status of each node in the path whether they belongs to Malicious_Array or NonMalicious_Array.

If RAODV finds any node in the active route belongs to Malicious_Array then it generates a Route Error and stops the transmission. When a RERR is generated each intermediate node invalidates that particular route. After detecting RAODV marks this node as malicious node in the routing table and removes this node from the current route. After removing the malicious nodes RAODV tries to repair the route by releasing a local route request by an intermediate node. If the route is repaired then RAODV starts the transmission again between Source and Destination. If it is not able to repair the route then Source of the data receives the RERR, it invalidates the route and reinitiates route discovery. Then a new route is established by RAODV for data communication. After establishing this new route again it verifies

statusof each node in the route. This process repeats until RAODV establishes a stable and secure route between Source and Destination.
RAODV establishes a stable and secure route using various phases. Every phase performs a specified task.

RAODV has the following phases:

1. Route Request (RREQ)
2. Route Reply (RREP)
3. Data Transmission(DTRAM)
4. Detection of Malicious Nodes (DMALN)
5. Route Error (RERR)
6. Route Repair (RREPR)
7. Establishing New Path (ESTNP)

RREQ: When a Source has data to transmit to a Destination, it broadcasts a Route Request (RREQ) for that Destination. At each intermediate node, when a RREQ is received a route to the Source is created. If the receiving node has not received this RREQ before, is not the Destination node and does not have a current route to the Destination, it re-broadcasts the RREQ. In this phase RAODV also set status of each node participates in routing process. It sets node status with the help of 'Source Node Sequence Number' and 'Destination Node Sequence Number'.

It checks Node sequence number one by one that participates in the routing process. It sets each node status as 'TRUE' whose sequence Number is in between the 'Source Node Sequence Number' and 'Destination Node Sequence Number'. If it is found there is any node whose sequence number do not match with the given condition it sets status of that node as 'FALSE'.

It uses two arrays one for non malicious nodes and other for malicious nodes. Node whose status is 'TRUE' enters into NonMalicious_Array and node whose status is 'FALSE' enters into the Malicious_Array.

RREP: 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 node. When the Source receives the RREP, it records the route to the Destination and it can begin sending the data. If multiple RREPs are received by the Source, it selects the path on the basis of shortest path algorithm.

DTRAM: After establishment of a path between Source and Destination transmission starts between the Source node and Destination node. If a route is not used for some period of time, a node cannot be sure whether the route is still valid; consequently, the node removes the route from its routing table.

DMALN: As transmission starts from Source to Destination, RAODV checks status of every node in the active route. If RAODV finds any node in the current route that does not belong to NonMalicious_Array it declares this node as malicious node.

RERR: When RAODV finds any malicious node in the route it generates a RERR. As the RERR propagates towards the Source, each intermediate node invalidates that particular route.

RRPR: When a RERR is generated RAODV tries to repair the route locally by releasing a RREQ to find a new route to the Destination and if it is not able to repair the route it release RERR to the Source. Route Error (RERR) is sent to the Source of the data in a hop-by-hop fashion.

ESTNP: When the Source of the data receives the RERR, it invalidates the route and reinitiates route discovery. If more then one routes are available it selects the shortest route and establishes a path between Source and Destination. RAODV again verifies status of each node in the new Route. This process repeats until RAODV establishes a stable and secure path for data transmission between Source and Destination.

Conclusion:

The work carried out contributes in terms of proposed new protocol modification to the existing protocol and gives a new secure authentication scheme in routing to enhance security.

Proposed protocol has been developed for better performance in terms of security in different conditions like varying network size, varying pause time, varying number of nodes and varying speeds.

References

1. Samuel Jhun, available at: - http://wireless-network-system.blogpost.com/ Retrieved on 11-Jul-12.
2. Available at: - http://ars.els-cdn.com/content/image/1-s2.0-S1570870511-001697-gr1.jpg. Retrieved on 8-Aug-12
3. Sunil Taneja and Ashwani Kush "A Survey of Routing Protocols in Mobile Ad Hoc Networks", International Journal of Innovation, Management and Technology, Volume 1, Issue 3, August 2010, pp. 279-285.
4. Available at: - http://web.mit.edu/~lldai/www/images/wireless.gif, Retrieved on 11-Oct-12.
5. Yuan Zhou, Chunhe Xia, Haiquan Wang, Jianzhong Qi, "Research on Survivability of Mobile Ad-hoc Network", Journal of. Software Engineering and Applications, Volume 2, Issue 1, April 2009, pp. 50-54.
6. Aleksi Penttinen, "Research on Ad Hoc Networking: Current Activity and Future Directions", available at: - http://utopia.duth.gr/~vtsaousi/13-Aleksi.pdf , Retrieved on 5-Jul-12.
7. Available at: - http://www.ece.iupui.edu/~dskim/manet/images/adhocne-t.gif , Retrieved on 13-Dec-12.
8. Vikaram Patalbasi, Sonali Mote and Vijyalaxmi Kondal "Mobile Ad Hoc Networks: Opportunities and Future", available at: - http://www.hiray-.org.in-/data/-MobileAdhocNetworksChallengesand-Future.pdf ,Retrieved on 1-Feb-12.
9. Humayun Bakht "History of Mobile Ad hoc Networks", available at: - http://www.oocities.org-/humayunbakht/HMANET.pdf , Retrieved on 2-Nov-12.
10. S. Corson, J. Macker. Mobile Ad hoc Networking (MANET): "Routing Protocol Performance Issues and Evaluation Considerations". IETF RFC 2501, January 1999 available at: http://www.ietf.org/rfc/rfc2501.txt , Retrieved on 25-Oct-12.

11. M. Scott Corson, Joseph P. Macker and Gregory H.Cirincione "Internet-based Mobile Ad Hoc Networking" Preprint IEEE Internet Computing Magazine, July/Aug1999 pp.1-8, available at:- http://cs.itd.nrl.navy.-mil/pubs/docs/Internet-%20Comp%2099%20preprin-t.pdf , Retrieved on 1-Aug-12.
12. Available at:- http://en.wikipedia.org/wiki/Mobile_ad_hoc_network , Retrieved on 28-Mar-12.
13. G.Subhramanya Sarma, Ravi Kumar Kallakunta,, A.Ramakrishna, S.Swarna, A.somasekhar, "A Case Study on Pervasive Computing in MANET" International Journal of Scientific and Engineering Research, Volume 2, Issue 12, December 2011, pp.1-6.
14. Humayun Bakht, "Computing Unplugged, Wireless infrastructure, Some Applications of Mobile ad hoc networks", available at :- http://www.computingunplugged.com/issues-/issue200410/-0000139500-1.html,April-2003 , Retrieved on 6-Sept-12.
15. A.N. Al-Khwildi, S. Khan, K.K. Loo, H.S. Al-Raweshidy "Adaptive Link-Weight Routing Protocol Using Cross-Layer Communication for Manet", Wseas Transactions on Communications, Volume 6, Issue 11, November 2007, pp. 833-839.
16. Panagiotis Papadimitratos, Zygmunt J. Haas, Emin Gün Sirer , "Path Set Selection in Mobile Ad Hoc Networks", 2002 available at :- http://citeseerx.ist.psu.edu/showciting-?cid=5375906 , Retrieved on 22-Jan-12.
17. Sudhakar Pandey, Narendra Kumar Shukla, "Improved Node Failure Prediction Qos Routing Protocol With Classified Power Levels", International Journal of Engineering and Management Sciences, Volume 1, Issue 1, October 2010, pp. 66-68.