International Journal of Advanced and Innovative Research (2278-7844) / Volume 6 Issue 12

Creation of Latest Routing Protocol L-AODV over AODV with Security Enhancements for Ad Hoc Wireless Networks

Deepak Sharma[1], Sohan Garg*[2]

1. Research Scholar Computer Science Mewar University-Rajasthan

2. Sir Chhotu Ram Institute of Engg. & Technology, Meerut (U.P.)

sohangarg@rediffmail.com, * Corresponding Author

Abstract:
MANET is gradually emerging to be much essential in the growth of wireless technology. MANET is a wireless network comprises the collection of mobile nodes with no fixed infrastructure. They are associated powerfully in a self-assertive way. Every hub carries on as a router and participates in the revelation and upkeep of routes to others. The hubs can move uninhibitedly whenever, with the goal that network structure changes progressively because of mobility. One of the present strong protocols is Ad Hoc On-Demand Vector Routing (AODV) tradition which is an open routing tradition which is mandatory for ad hoc and mobile networks that keeps up routes just between center points that requirements to confer. There are various security issues to be considered in this protocol. Recollecting a definitive goal to offer security to AODV tradition, Latest Ad Hoc On Demand Vector Routing (L-AODV) can be utilized. L-AODV is an expansion of the AODV routing tradition that can be utilized to shield the route disclosure process by giving security qualities like integrity and authentication.

1 Introduction

Mobile Ad Hoc Network (MANET) [1,2] can be depicted as an independent gathering of mobile hubs (clients) that impart over moderately low limit wireless links, with no help of any settled foundation. In these networks, hub developments and the wireless correspondence links may lead to progressively changing and very unverifiable topologies. All the network related functions like routing, multi-hop packet delivery and mobility management are to be done with the help of member nodes .These nodes are proficient of doing this task individually or collectively. Therefore cooperation of all member nodes is a big factor for network performance. MANETs find applications in diverse areas. These are ranging from low-power military WSN with the large-scale civilian applications .MANET applications are also helps in emergency search/rescue operations.

The main challenges of MANETs are Limited bandwidth, Dynamic topology, Routing Overhead etc. There are some other also like Hidden terminal problem, Packet losses and the next and most common is mobility Battery constraints. Since mobile ad hoc networks have unmitigated a more visible number of vulnerabilities than the conventional wired networks, security is by and large more difficult to keep up than in the wired network. Once the opponent is in the radio level of someone of a kind fixation focuses in the mobile ad hoc network, it can visit with those fixations in its radio range and in this way join the network as necessities be. Thusly, the mobile ad hoc network does not give past what many would consider possible to shield the network from some maybe risky network gets to. Routing security is another basic issue in the security of MANETs. This is not 100% that every one of the hubs in a manet are associated in a one hop range. Secure routing is mandatory for security of MANETs.

There are a less number of routing protocols are there[74] and important of them are AODV, TORA, and DSDV etc. Although MANET secure routing protocols never gives a 100% satisfying solution for all the attacks on MANET. Their assumption is that any center point sharing in the MANET isn't intolerant and it will arrange to help particular framework functionalities which is not true all the times. ARAN – (Authenticated routing protocol) [3] is a solution which is a secure protocol. It is not possible to describe all routing protocols here but we are explaining some of them here which are as follows:

1. The AODV Protocol:

AODV is for dynamic link conditions in this there is a concept of routing tables which keeps all routes from start point to last point. The node checks with its routing table first if there is any entry for the route to the destination. If yes, then it uses that route

Type	N	Reserved for Next Node	Destination Count
Identification for Route Request (RREQ ID)			
Destination IP Address is NOT REACHABLE			
Destination Sequence Number is NOT REACHABLE			
It is for Node IP Address (SIP)			
Route Not Developed			

to send the packets to the destination. In case a route isn't open, by then within point begins a route presentation process. A RREQ (Route Request) packet is broadcasted by within point in the network. The center concentrations which get RREQ packets, first keep an eye in the inconceivable event that they are the objective group for that packet and if so then they returns back RREP packet. In case they are not the objective then the routing table is checked again to pick whether there is any route to the objective. If not, the nodes relay RREQ packets with the help of the process of broadcast to the neighbors.

Type	A	B	Reserved for Next Node	Prefix Size	This is for Hop Count
Identification for Route Request (RREQ ID)					
This is for IP Address of the Destination Node (DIP)					
This is for Sequence Number of Destination Node (DSQN)					
This is for IP Address of the Source Node (SIP)					
Route Developed					

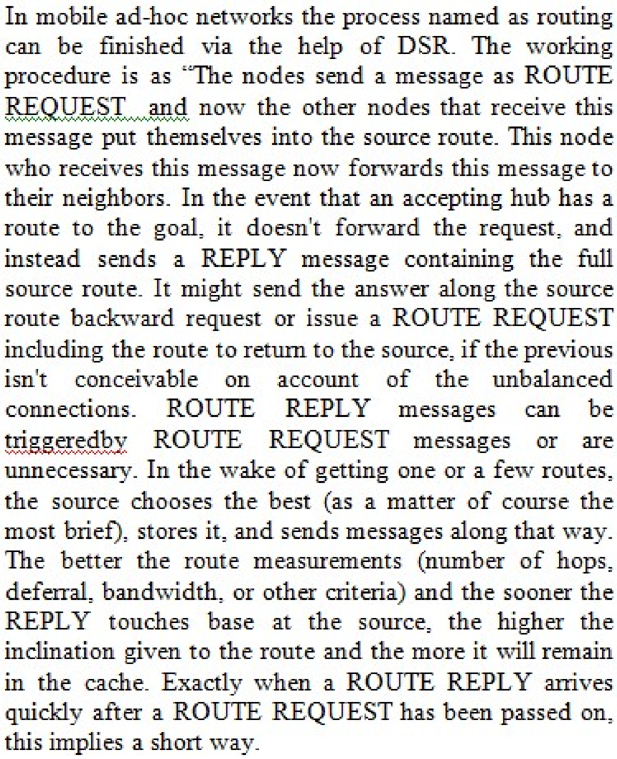
Type	A	B	C	D	E	Reserved	This is for Hop Count
Identification for Route Request (RREQ ID)							
It contains Destination Node IP Address (DIP)							
This is for Sequence Number of Destination Node (DSQN)							
This is for IP Address of the Source Node (SIP)							
This is for Sequence Number of Source Node (SSQN)							

Figure 1: RREQ Packet (Format for Route Request)

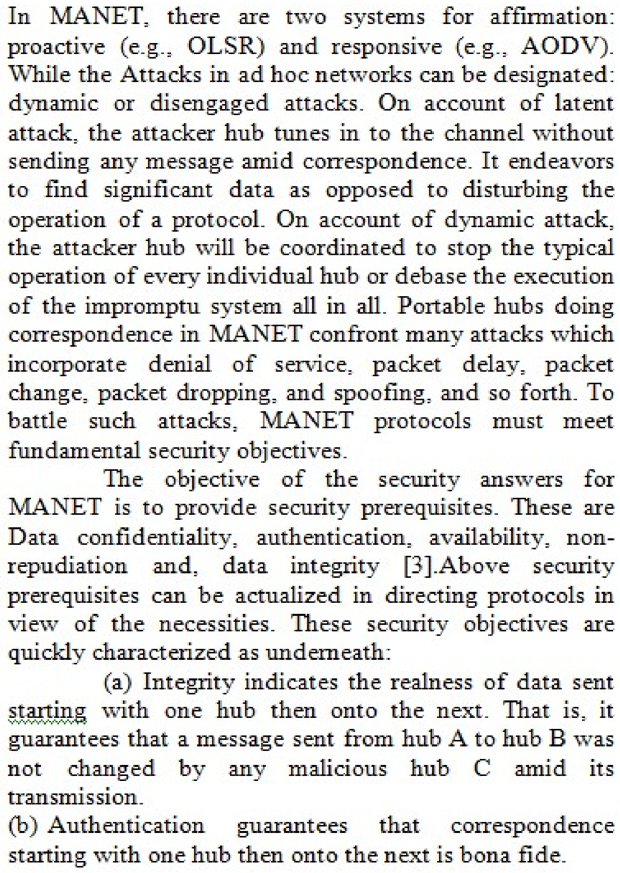
Figure 2: RREP Packet (Format for Route Reply)

Figure 3 RERR Packet (If there is any Error)

2. DSR Protocol Dynamic Source Routing:



In mobile ad-hoc networks the process named as routing can be finished via the help of DSR. The working procedure is as "The nodes send a message as ROUTE REQUEST and now the other nodes that receive this message put themselves into the source route. This node who receives this message now forwards this message to their neighbors. In the event that an accepting hub has a route to the goal, it doesn't forward the request, and instead sends a REPLY message containing the full source route. It might send the answer along the source route backward request or issue a ROUTE REQUEST including the route to return to the source, if the previous isn't conceivable on account of the unbalanced connections. ROUTE REPLY messages can be triggeredby ROUTE REQUEST messages or are unnecessary. In the wake of getting one or a few routes, the source chooses the best (as a matter of course the most brief), stores it, and sends messages along that way. The better the route measurements (number of hops, deferral, bandwidth, or other criteria) and the sooner the REPLY touches base at the source, the higher the inclination given to the route and the more it will remain in the cache. Exactly when a ROUTE REPLY arrives quickly after a ROUTE REQUEST has been passed on, this implies a short way.



In MANET, there are two systems for affirmation: proactive (e.g., OLSR) and responsive (e.g., AODV). While the Attacks in ad hoc networks can be designated: dynamic or disengaged attacks. On account of latent attack, the attacker hub tunes in to the channel without sending any message amid correspondence. It endeavors to find significant data as opposed to disturbing the operation of a protocol. On account of dynamic attack, the attacker hub will be coordinated to stop the typical operation of every individual hub or debase the execution of the impromptu system all in all. Portable hubs doing correspondence in MANET confront many attacks which incorporate denial of service, packet delay, packet change, packet dropping, and spoofing, and so forth. To battle such attacks, MANET protocols must meet fundamental security objectives.

The objective of the security answers for MANET is to provide security prerequisites. These are Data confidentiality, authentication, availability, non-repudiation and, data integrity [3].Above security prerequisites can be actualized in directing protocols in view of the necessities. These security objectives are quickly characterized as underneath:

(a) Integrity indicates the realness of data sent starting with one hub then onto the next. That is, it guarantees that a message sent from hub A to hub B was not changed by any malicious hub C amid its transmission.

(b) Authentication guarantees that correspondence starting with one hub then onto the next is bona fide.

(c) Non-renouncement is the capacity to guarantee t hat a hub can't preclude the sending from claiming a message that it started.

(d) Data confidentiality guarantees that a specific system content is never revealed to unapproved substances other than its (their) coveted recipient(s). Data confidentiality is by and large accomplished by utilizing cryptographic components, for example, symmetric or hilter kilter data encryption.

(e) Availability guarantees administrations are usable when required, along these lines courses returned by ad hoc routing protocols must be legitimate and should stay utilitarian. Secure Routing In MANET there are different conceivable assaults, to ensure against these assaults a routing convention must satisfy an arrangement of prerequisites [3] to guarantee that the predetermined way from source to goal works accurately within the sight of malicious hubs. Right now, various secure routing protocols [3,4] that orders with malicious hubs that can stop the present working situation of a routing convention by changing routing data, by sending false routing data and by acting like different hubs.

3. ARAN (Authenticated Routing for Ad-hoc Networks) ARAN [5]: Isa independent convention in view of AODV which gives validation, message trustworthiness and non-renouncement in ad-hoc arranges by utilizing cryptographic open key testaments issued by an approved element. It is trailed by a route procedure to guaranteeend-to-end security administrations. Yet, it requires the utilization of confided in certification server. The essential disadvantage of this convention is every hub that trades a route disclosure or a route answer message must be agreed upon. This procedure is especially control devouring and comes about into increment in the span of the routing messages at each jump amid correspondenc

4. **The Secure Routing Protocol (SRP):**Gives end-to-end verification which can be executed in existing ad-hoc routing protocols with numerous security upgrades. A definitive objective of the proposed plot is to fuse a security relationship between the sender hub starting the question and the expected goal. A common mystery has been built up between sender hub and goal hub utilizing this security affiliation. By the utilization of a mutual mystery, the non-alterable fields of the sent routing messages are secured. This plan is solid where various non-colluding hubs are available, and gives rectify routing data time-to-time. In SRP, the halfway hubs those display subjective and malicious practices are not accounted amid correspondence.

5.ARIADNE [6] :

An on-request secure ad hoc routing tradition, depends upon exceedingly profitable symmetric cryptography to give security against vindictive hubs [6,7]. It keeps aggressors or traded off hubs from altering uncompromised routes comprising of uncompromised hubs. ARIADNE and the MAC that guarantees end-to-end confirmation of a routing message. Proficient mix of one way hash work and shared keys influences ARIADNE more to secure. ARIADNE gives a security against assaults that adjust and manufacture routing data. When it is utilized with an advanced adaptation of TESLA [7, 8], it is safe to wormhole attacksts. Notwithstanding, it is as yet helpless against egotistical hub assault or attack. General security strategy are reliable yet key trades are intense, making ARIADNE non attainable in the present ad hoc situations.

2 Proposed Work :

The proposed work is totally based upon the concept of the Blackhole attack [9, 10, 11] that is a dangerous active attack on the Mobile Ad hoc Networks. A black hole attack is performed by either a solitary fixation point. This also can be performed by the mix of focus center interests. In this work, we have

Time for Simulati on in Sec.	Total Pack ets	Pack ets Recei ved in AOD V	Pack ets Drop ped in AOD V	Delivery Ratio (%)	Pack ets Recei ved in L-AOD V
3.85	62	44	18	29.032258095	62
10.54	178	95	83	46.629213484	178
15.70	287	142	145	50.522648084	287
19.78	432	204	228	52.777777778	432
25.35	511	236	275	53.816047 2381	511

proposed a Blackhole evident affirmation and vulnerability plot which beneficially observes and keeps these attacks. The main objectives of this proposed work are to develop a system to identify and provide a safer side to avoid black hole node in MANET and comparison of proposed detection technique with others. The proposed procedure is holding the ability to detect the Blackhole nodes and prevents the packet dropping in the network. The measure of packets got and the Packet Delivery Ratio have been figured to audit the point of confinement of the proposed plot. In this algorithm the following table compares the proposed scheme L-AODV results with the AODV approach. The network nodes have been simulated and following two parameters have been calculated:

2.1 Packets Received (L-AODV vs AODV scheme):

The number of packets received every five seconds has been calculated and compared in both the L-AODV scheme and the AODV scheme.

2.2 PDR (Packet Delivery Ratio %):

This parameter gives the percentage of packets delivered in the L-AODV scheme and the AODV scheme with the passage of time. We have analyzed the network against these two parameters. The number of packets delivered has been noted down e.g. the simulation starts at 5 seconds. Now the observance is that the number of packets delivered in the L-AODV scheme at 5 seconds is 62 while it is 44 in AODV. It the observance is also that there is no packet drop in this scheme and hence, the L-AODV scheme outperforms the AODV scheme. The same process has been repeated for the packets delivered at approximately ten, fifteen, twenty and twenty five seconds which is shown in the below table.

3 Simulation Graphs:

The simulation Graphs opposed to two network parameters which are Packets received and Packet Delivery Ratio. The two are shown below:

3.1 Calculation of Packets Received:

Here we will calculate the packets received per unit time. The graph plotted for packets received every 5 seconds. Blue bars in this graph depicted the packets received in AODV. Red bars are for packets received in the L-AODV.So L-AODV scheme receives more than approx 50% packets as compared to AODV scheme.

Table III: Delivery Ratio of Packets in AODV and L-AODV

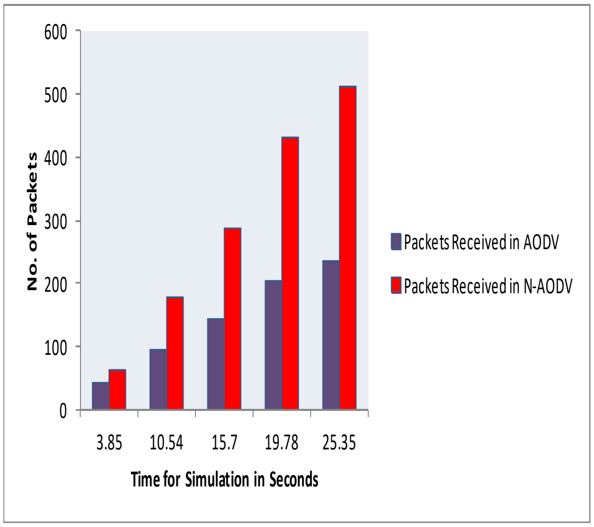


Figure 4 Comparison of packets received in existing AODV and L-AODV Technique

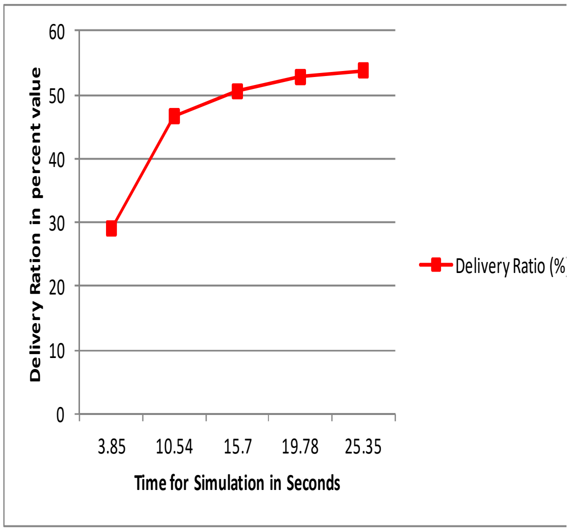


Figure 5: A Graph of Packets Delivery Ratio of existing AODV

3.2 Calculation of PDR (Packet Delivery Ratio %)

This parameter gives the percentage of packets delivered in the L-AODVscheme and the AODV scheme with the passage of time. The plotted graph showing the PDR in old AODV scheme. The PDR ranges from 29% to 53% in old AODV scheme whereas in the L-AODV scheme, the PDR achieved is 100%.

4. CONCLUSIONS AND FUTURE WORK:

In this research, comparison of the L-AODV detection technique with the existing AODV technique is performed. The parameters on which the results have been compared are packets received per second, packets dropped per second and PDR (Packet Delivery Ratio). The outputs dictates that the proposed procedure that is L-AODV of detecting the Blackhole nodes performs better than the existing AODV technique. For future we will expand this L-AODV routing convention for extensive and substantial network.

CONCLUSION:

Because of the uncommon development in the scale and decent variety of mobile computing gadgets, new skylines for remote availability have come into see. In this research, we have demonstrated the significance of an ad hoc routing convention and a portion of the past works. Following that we have proposed our new routing convention in light of Scalability, Battery Power and bandwidth, where the division of hubs will significantly diminish the overhead of the whole network and accelerate the routing procedure. After completely depicting its capacities and instrument, we have recommended different advancements to the convention and used the idea of steadiness file. At long last, we have done constrained trials to demonstrate that our convention is useful and successful; we do see the need in facilitate experimentation with a specific end goal to precisely get to the useful adequacy of our convention in a medium to huge size network.

[1] Royer E. M. and Toh C. K., “A review of current routing protocols for ad hoc mobile wireless networks” IEEE Personal Communications, 6(2):46–55, April 1999.

[2] C. Siva Ram Murthy and B.S. Manoj, “Ad hoc Wireless Networks Architecture and Protocols”, Prentice Hall, 2004.

[3] Huang R., Zhuang Y., Cao Q., “Simulation and Analysis of Protocols in Ad Hoc Network”, 2009 International Conference on Electronic Computer Technology © 2009 IEEE

[4] Perkins C. E., Ad Hoc Networking, ed. Addison-Wesley, 2000

[5] David A. Maltz, “On-Demand Routing in Multi-hop Wireless Mobile Ad Hoc Networks’, May 2010, available at www.monarch.cs.rice.edu

[6] M.S. Corson, S. Batsel and J. Macker, “Architecture consideration for mobile mesh networking”, *Conference Proceeding, IEEE,* Vol.1, 21-24 Oct. 1996, pp. 225-229.

[7] Das S. R., Perkins C. E., Royer E. M. and Marina M. K., “Performance comparison of two on demand routing protocols for ad hoc networks,” IEEE Personal Communications Magazine, special issue on Mobile Ad Hoc Networks, vol. 8, no. 1, pp. 16–29,February 2001

[8] C. E. Perkins and P. Bhagwat, “Highly dynamic destination-sequenced distance vector routing (DSDV) for mobile computers”, Proceedings of ACM SIGCOMM 94, 1994, pp. 34–244.

[9] P. Chenna Reddy, Dr. P. Chandrasekhar Reddy, “Performance Analysis of Adhoc Network Routing Protocols”, Academic Open Internet Journal, SSN 1311-4360, Volume 17, 2006

[10] D. Bertsekas and R. Gallager, “Data Networks” Prentice Hall Publ., New Jersey, 2002.

[11] Tsu-Wei Chen and M. Gerla, "Global State Routing: A New Routing Scheme for Ad-hoc Wireless Networks" Proceedings of International Computing Conference IEEE ICC 1998.

[12] S. Murthy and J. J. Garcia-Luna-Aceves, "An Efficient Routing Protocol for Wireless Networks", ACM Mobile Networks and App. Journal, Special Issue on Routing in Mobile Communication Networks, pp.183-97, 1996.