Volume 6, Issue 4, April 2016 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Implementing Cryptographic Algorithm in Term of Privacy in AODV Routing Protocol

[1]Reena Chaudhary, [2]Sunil Ahuja

[1] M.Tech (CSE), [2] Assistant Professor, (CSE)

[1, 2] Doon Valley Institute of Engineering and Technology, Karnal, Haryana, India

Abstract: An ad hoc network is a collection of mobile nodes that are dynamically located in such a manner that the interconnections between nodes are capable of changing on a continual basis. The majority of ad hoc routing protocol research has been done using simulation only. One of the most motivating reasons to use simulation is the difficulty of creating a real implementation. We have studied the various problems in Ad-hoc On-demand Distance Vector Routing Protocol in Mobile Ad-hoc Network. Further, it offers quick adaptation to dynamic link conditions, low processing and memory overhead, low network utilization, and determines unicast routes to destinations within the ad hoc network. But there are still many problems in AODV routing protocol like AODV does not specify any special security measures, delay caused by route discovery process etc. Therefore this paper specially shows security in term of privacy with the help of cryptographic algorithm in AODV routing protocol by using NS2 simulator. So that AODV routing protocol will work more efficiently in ad hoc wireless network.

Keywords: MANET, Routing protocol, NS2 simulator

I. INTRODUCTION

An ad hoc network is a collection of mobile nodes forming a temporary network without the aid of any centralized administration or standard support services regularly available on conventional networks[1]. An ad hoc network is a temporary network connection created for a specific purpose such as transferring data from one computer to another. Nodes in ad hoc networks are computing and communication devices, which can be laptop computers, PDA's mobile phones, or even sensors. In this paper, we consider Ad-Hoc On-Demand Distance Vector (AODV) routing protocol due to the reason that it uses the shortest number of wireless hops towards a destination as the primary metric for selecting a route with independence of the traffic congestion. To add security to AODV, Secure AODV was designed to enhance security services to the original AODV. Secure AODV protocol was designed with cryptographic techniques, which can have significant impact on the routing performance of AODV routing protocol [2]. An ad hoc network can be envisioned as a collection of mobile routers, each equipped with a wireless transceiver. The basic assumption in an ad hoc network is that if two nodes willing to communicate are outside the wireless transmission range of each other they may still able to communicate if other node in the network are willing to forward those packet from them. Applications of ad hoc networks include military tactical communication, emergency relief operations, commercial and educational use in remote areas, and in meetings and other situations where the networking is mission oriented or community based [3].

II. ROUTING IN MANET

Routing is the mechanism by which user traffic is directed and transported through the network from the source node to the destination node. Objectives include maximizing network performance from the application point of view-application requirement, while minimizing the cost of the network itself in accordance with its capacity. The application requirements are hop count, delay, throughput, loss rate, stability, cost and the network capacity is a function of available resources that reside at each node and number of nodes in the network as well as its density, frequency of end –to- end connection (i.e. number of communication), frequency of topology changes (mobility rate)[3].

The properties that are desirable in MANET routing protocol are [5]:

1) Distributed operation

The protocol should be distributed. It should not be dependent on a centralized controlling node. This is the case even for stationary networks. The dissimilarity is that the nodes in an ad hoc can enter or leave the network very easily and because of mobility the network can be partitioned.

2) Loop free

To improve the overall performance, routing protocol should assure that the routes supplied are loop free. This avoids any misuse of bandwidth or CPU consumption.

3) Demand Based operation

To minimize the control overhead in the network and thus not misuse the network resource the protocol should be reactive. This means that the protocol should react only when needed and should not periodically broadcast control information. There should not be rebroadcast of messages until the route is requested by the source and thus the protocol should react only if needed.

4) Unidirectional Link support

The radio environment can cause the formation of unidirectional links. Utilization of these links and not only the bi-directional links improves the routing protocol performance.

5) Security

The radio environment is especially vulnerable to impersonation attacks so to ensure the wanted behavior of the routing protocol we need some sort of security measures. Authentication and encryption is the way to go and problem here lies within distributing the keys among the nodes in the ad hoc network.

6) Power conservation

The nodes in the ad hoc network can be laptops and thin clients such as PDA's that are limited in battery power and therefore uses some standby mode to save the power. It is therefore very important that the routing protocol has support for the sleep modes.

7) Multiple Routes

To reduce the number of reactions to topological change and congestion multiple routes can be used. If one route becomes invalid, it is possible that another stored route could still be valid and thus saving the routing protocol from initiating another route discovery procedure.

III. ROUTING PROTOCOL

At network layer, routing protocols are used to find route for transmission of packets. Routing is the most fundamental research issue in ad hoc networking. A Routing protocol is a protocol that specifies how routers communicate with each other, disseminating information that enables them to select routes between any two nodes on a computer network by routing algorithms[6]. Classification of routing protocol in mobile ad hoc network can be done in many ways, but most of these are done depending on routing strategy and network structure. The routing protocols can be categorized as flat routing, hierarchical routing and geographic position assisted routing while depending on the network structure [7]. According to the routing strategy routing protocols for ad hoc networks can be categorized as: Proactive (Table Driven) and reactive (source initiated On-demand) as shown in Fig 1.

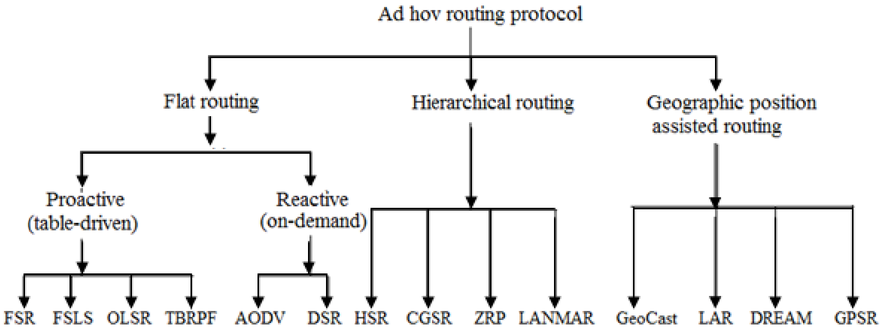


Fig.1: Classification of Routing Protocols

IV. PROTOCOL USED IN SIMULATION

A) Ad Hoc On-Demand Distance Vector (Aodv) Routing Protocol:

Ad hoc On-demand Distance Vector Routing (AODV) is an improvement on the DSDV algorithm. Ad hoc on-demand distance vector (AODV) routing protocol is also well known in terms of better delivery ratio and less link failures while maintaining a reasonable routing control overhead[8].

It typically minimizes the number of broadcasts by creating routes on-demand as opposed to DSDV that maintains the list of all the routes. To find a path to the destination, the source broadcasts a route request packet. The neighbors in turn broadcast the packet to their neighbors till it reaches an intermediate node that has a recent route information about the destination or till it reaches the destination. A node discards a route request packet that it has already seen. The route request packet uses sequence numbers to ensure that the routes are loop free and to make sure that if the intermediate nodes reply to route requests, they reply with the latest information only.

When a node forwards a route request packet to its neighbors, it also records in its tables the node from which the first copy of the request came. This information is used to construct the reverse path for the route reply packet. AODV uses only symmetric links because the route reply packet follows the reverse path of route request packet. As the route reply packet traverses back to the source, the nodes along the path enter the forward route into their tables.

If the source moves then it can reinitiate route discovery to the destination. If one of the intermediate nodes move then the moved nodes neighbor realizes the link failure and sends a link failure notification to its upstream neighbors and so on till it reaches the source upon which the source can reinitiate route discovery if needed.

Ad hoc On-demand Distance Vector Routing protocol is a pure on-demand route acquisition system, since nodes that are not on a selected path do not maintain routing information or participate in routing table exchange [9].

When a source node desires to send a message to some destination node and does not already have a valid route to that destination, it initiates a path discovery process to locate the other node. It broadcasts a route request (RREQ) packet to its neighbors, which then forward the request to their neighbors, and so on, until either the destination or an intermediate node with a "fresh enough" route to the destination is located. Fig.2 illustrates the propagation of the broadcast RREQs across the network.

AODV utilizes destination sequence number to ensure all routes are loop-free and contain the most recent route information. Each node maintains its own sequence number, as well as a broadcast ID. The broadcast ID is incremented for every RREQ the node initiates, and together with the node's IP address, uniquely identifies a RREQ. Along with its own sequence number and the broadcast ID, the source node includes in the RREQ the most recent sequence number it has for the destination. Intermediate nodes can reply to the RREQ only if they have a route to the destination whose corresponding destination sequence number is greater than or equal to that contained in the RREQ.

During the process of forwarding the RREQ, intermediate nodes recode in their route tables the address of the neighbor from which the first copy of the broadcast packet is received, thereby establishing a reverse path. If additional copies of the same RREQ are later received, these packets are discarded.

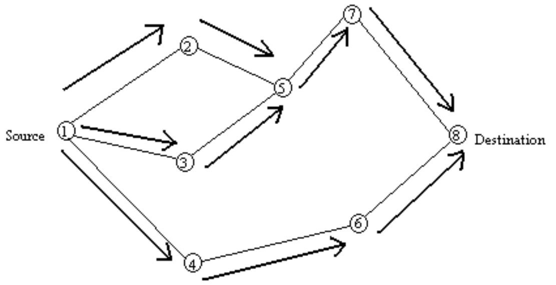


Fig. 2 : Propagation of route request (RREQ) packet[10].

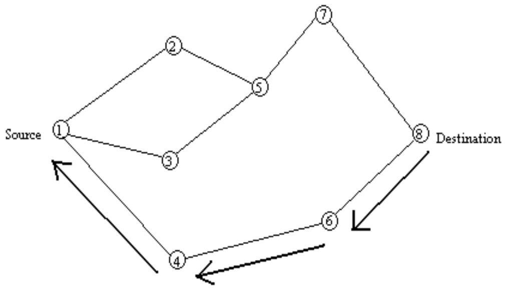


Fig. 3: Path taken by the Route Reply (RREP) packet[10].

Once the RREQ reaches the destination or an intermediate node with a fresh enough route, the destination intermediate node responds by unicasting a route reply (RREP) packet back to the neighbor from which it first received the RREQ as shown in Fig.3. As the RREP is routed back along the reverse path, nodes along this path set up forward route entries in their route table which point to the node from which the RREP came. These forward route entries indicate the active forward route. Associated with each route entry is route timer which will cause the deletion of the entry if it is not used within the specified lifetime. Because the RREP is forward along the path established by the RREQ, AODV only supports the use of symmetric links. Based on the AODV protocol we improve the flooding algorithm to make it more efficient and use efficient one way Hash functions to protect routing information. Before describing the scheme, we first introduce the management of the local node groups, for it is the base of the scheme.

In this mechanism, firstly, the packet is encrypted in the sender side and then transmits the packet over the network. The packet contains information such as routing protocol, destination address etc. which is useful for correct recipient of packet at correct location. When the receiver receives the packet, it is in encrypted form which can be decrypted by only the other key which is present at receiver node previously. After decrypting the packet, the original message can be read from that packet. Thus, this will increase security of network during data transmission [11].

B) Diffie Hellman Algorithm:

Diffie–Hellman key exchange (D–H) is a specific method of exchanging keys. It is one of the practical examples of key exchange implemented within the field of cryptography. The Diffie–Hellman key exchange method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel [12]. This key can then be used to encrypt subsequent communications using a symmetric key cipher. The scheme was first published by Whitfield Diffie and Martin Hellman. Although Diffie–Hellman key agreement itself is an anonymous (non-authenticated) key-agreement protocol, it provides the basis for a variety of authenticated protocols, and is used to provide perfect forward secrecy in Transport Layer Security's ephemeral modes. Diffie–Hellman establishes a shared secret that can be used for secret communications by exchanging data over a public network as shown in Table1.

Table 1: Diffie Hellman Algorithm

X			Y		
Secret	**Public**	**Calculates**	**Sends**	**Calculates**	**Public**
A	p, g		p, g →		
A	p, g, A	g^a mod p=A	A →		p, g
A	p, g, A		← B	g^b mod p=B	p, g, A, B
a, s	p, g, A, B	B^b mod p= s		A^b mod p= s	p, g, A, B

C) Algorithm Used:

```
Algo(S,D)
/*S is the source Node and D is the Destination Node*/
{
    1)  Find the path between S and D called P1,P2,P3….Pn
    2)  For Each Node Generate the KeyGroup for the communication using Deffie-Hellman Algorithm
    a.  Unique Private Key Pvk
    b.  Global Public Key Puk
    c.  Shared Key Shk
    3)  On Node S retrieve the Public Key of D and Perform the encryption
              DATA:  hello
                   Encrypted DATA: hello + 3 = khoor
           // This encrypted data send to other nodes
    4)  Perform the Communication between Source and Destination
    5)  For Each Node in path called Pi verify the shared key
    6)  On Receiver Side Perform the Decoding using PrivateKey(D)
            Decryption algo: khoor - 3
            Decrypted Data = hello
    7)  Discard the Bad Packets coming from unauthorized nodes.
    8)  Perform the Secure Communication over the network.
}
```

D) Network Simulator Ns-2:

In simulation approach we build software. It has emerged as an attractive alternative that is heavily used in result analysis of computer systems.

NS-2 is a discrete event simulator targeted at networking research. It provides substantial support for simulation of TCP, routing and multicast protocol over wired and wireless network. It Consist of two simulation tools. The network simulator (ns) contains all commonly used IP protocols. The network animator (nam) is use to visualize the simulations.

Ns-2 fully simulates a layered network from the physical radio transmission channel to high-level applications. The Ns-2 simulator has several features that make it suitable for our simulations. Ns-2 is an object- oriented simulator written in C++ and OTcl. Ns-2 is highly extensible. It not only support most commonly used IP protocols but also allows the users to extend or implement their own protocols. It also provides powerful trace functionalities. The full source code of Ns-2 can be downloaded and compiled for multiple platforms such as UNIX, Windows and Cygwin.

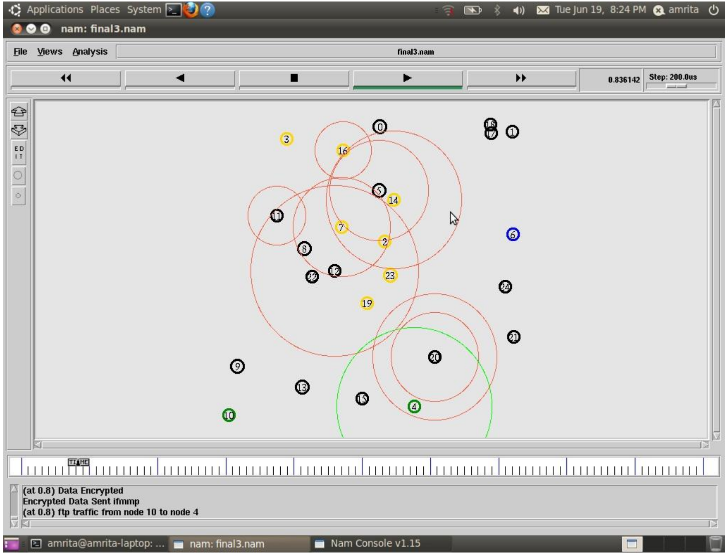
Here the basic parameter of the proposed work is presented respective to the simulation environment. The system is implemented on Cygwin Environment with NS-2 simulator and XGraph is used as the tool for graph analysis. In this we use various parameters and its value shown in Table 2.

Table 2: Simulation Parameters

PARAMETER	**VALUE**
Number of nodes	25
Topography dimension	500m x 500m
Traffic type	CBR
Radio Propagation Model	Two-Ray Ground Model
MAC Type	802.15.4 MAC layer
Protocol	AODV

E) Result Analysis:

The mobile ad hoc network comprising of 25 mobile nodes is constructed in the NS-2 simulator. The position of the mobile nodes is defined in terms of X & Y coordinates values as shown in Fig.4. The given scenario showing the packet transmission from the source node to the destination node in ad hoc on-demand distance vector routing protocol in MANET. Fig.5 shows X graph of packet received, Packet loss, number of bytes transferred, packet delay and Fig.6 shows X Graph of the packet received, Last Packet Time, Bit Rate.



```
(at 0.8) Data Encrypted
Encrypted Data Sent ifmmp
(at 0.8) ftp traffic from node 10 to node 4
```

Fig. 4: Simulation for AODV.

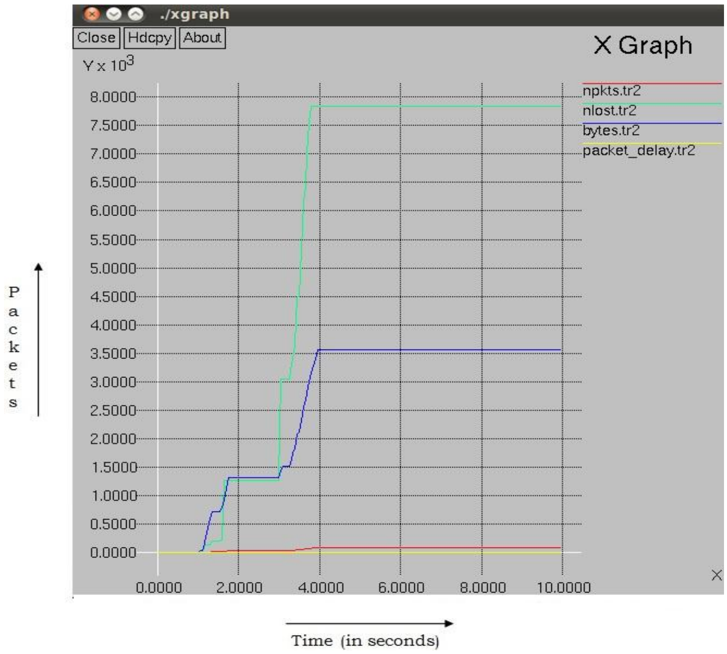


Fig.5: X graph shows packet received, Packet loss, number of bytes transferred, packet delay.

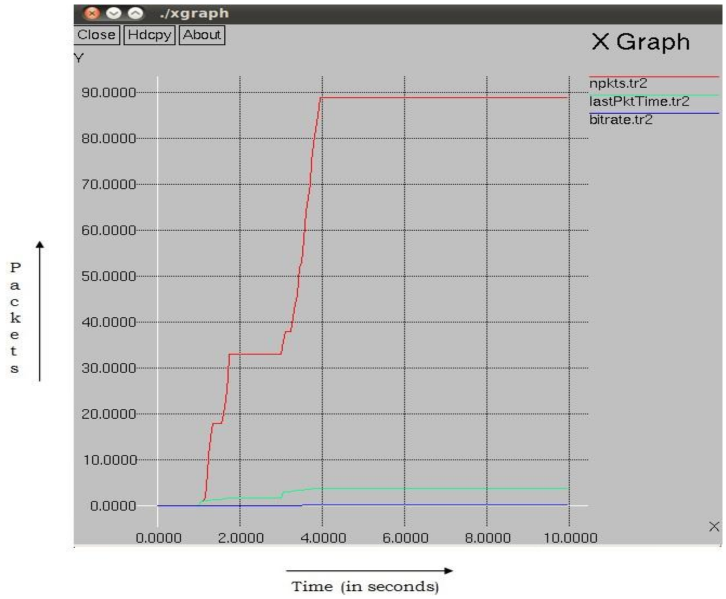


Fig.6: X Graph shows the packet received, Last Packet Time, Bit Rate..

V. CONCLUSION

AODV performs well in static scenarios under low traffic loads, but with even small node movements it fails to maintain good throughput. In contrast, AODV, the only reactive protocol assessed that suffers from scalability problems, because it is a reactive protocol, its overhead is directly proportional to the number of traffic flows.

In this paper, with the help cryptographic algorithm for security measures in Ad-hoc on-demand distance vector routing protocol by using NS-2 simulator so that AODV will work more efficiently & have secure communication in ad-hoc network. By doing this we conclude that data packet is much more securely reached at destination but only sufficient amount of packet is reached rest of the packet are lost in the network.

ACKNOWLEDGMENT

I deem it my proud privilege to express my indebtedness and sincere thanks for vulnerable guidance rendered to my guide. Mr. Sunil Ahuja, Assistant Professor, of department of Computer Science and Engineering at Doon Valley Institute of Engineering and Technology, Karnal. I got new knowledge for this kind and valuable guidance for the completion of my dissertation. His consistent support and intellectual guidance made me energize and give up the new idea. I am thankful to professor, H.O.D of Computer Science & Engineering for this support and providing necessary facility to carry out the work. I am thankful to all my faculty members of Computer Science & Engineering department for their generous help in various ways for the completion of this work. Finally, I am also thankful to my parents, my friends who have helped me a lot in completion of my dissertation.

REFERENCES

[1] https://www.cs.wmich.edu/wsn/doc/adhocrouting/AdhocRouting.pdfby SR Thampuran

[2] Yulei Wu, Félix Gómez Mármol and Ahmed Al-Dubai, “Introduction to advances in trust, security, and privacy for wireless networks”, EURASIP Journal on Wireless Communications and Networking 2013

[3] Krishna Paul, S. Bandyopadhyay, A. Mukherjee, D. Saha ,”A Stability-based On-Demand Multicast Routing in Ad-hoc Wireless Networks“(https://www.iimcal.ac.in/sites/all/files/sirg/11-8-routing-Stability-Based.PDF)

[4] http://shodhganga.inflibnet.ac.in/bitstream/10603/36201/2/c1.pdf

[5] P. Ramya, Gowtham.N, Sri Guruprassad.N, Suresh Kumar.S, Vinoth.K,Vishnu Vinod,” Implementing OSPF Protocol in CISCO 2800 Series Router” IJIET, ISSN: 2319 – 1058, Vol. 1 Issue 4 Dec 2012

[6] Suchita Baxla, Prof. Rajesh Nema,” Performance Analysis of AODV, OLSR, DSR AND GRP Routing Protocol of Mobile Adhoc Network – A Review”, IJCSMC, ISSN 2320–088X, Vol. 2, Issue. 6, June 2013

[7] http://shodhganga.inflibnet.ac.in/bitstream/10603/17900/11/11_chapter%202.pdf

[8] C. Sreedhar, Dr. S. Madhusudhana Verma, Dr. N. Kasiviswanath,” Performance Analysis of Secure Routing Protocols in Mobile Ad-Hoc Networks”, IJCST Vol. 3, Issue 1, Jan. - March 2012

[9] Xinjun Du, Ying Wang Jianhua, Ge Yumin Wang, “A Method for Security Enhancements in AODV Protocol”, IEEE, 2003

[10] http://www.cse.wustl.edu/~jain/cis788-99/ftp/adhoc_routing/

[11] Nidhi Chhajed, Mayank Kumar Sharma,” Secure Transmission in Wireless Sensor Network using AODV Routing Protocol”, IJRITCC, Dec 2015

[12] http://cryptography.wikia.com/wiki/Diffie%E2%80%93Hellman_key_exchange