ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

NCPR using Cryptosystem to Reduce Routing Overhead and Secure Data Transmission in MANET

L. B. Isal[1], Prof. A. S. Kapse[2]

M. E. Student, P.R. Patil College of Engineering and Technology, Amravati, Maharashtra, India[1]

Assistant Professor, P.R. Patil College of Engineering and Technology, Amravati, Maharashtra, India[2]

ABSTRACT: Mobile Ad Hoc Network (MANETs) consists of a collection of mobile nodes which can move freely. These nodes can be dynamically self-organized into arbitrary topology networks without a fixed infrastructure. MANETs are highly dynamic network because nodes may join and leave the network at any time. Due to high mobility of nodes in network there is frequent path failure and route discovery in MANET. So the NCPR (Neighbor coverage based probabilistic rebroadcast) is used for reducing routing overhead in Mobile Ad Hoc Networks. A novel rebroadcast delay is used to determine the rebroadcast order, and it obtains the more accurate additional coverage ratio by sensing neighbor coverage knowledge. A connectivity factor is defined to provide the node density adaptation for keeping the network connectivity. By combining the additional coverage ratio and connectivity factor, the rebroadcast probability is calculated. NCPR significantly reduce the routing overhead in the MANET. Once the route is selected from source to destination data is transferred in form of files between nodes. This transmission is unsecured. To make it secure we are going to use a cryptographic technique to avoid possible attacks on sensitive data.

KEYWORDS: MANET, routing overhead, broadcasting rebroadcast probability.

I. INTRODUCTION

Mobile Ad hoc Networks (MANETs)[1] are formed by an autonomous system of mobile nodes that are connected via wireless links without using an existing network infrastructure or centralized administration. The nodes are free to move randomly and act as end points as well as routers to forward packets in a multi-hop environment where all nodes may not be within the transmission range of the source. Broadcasting is a fundamental operation in MANETs as it is extensively used in route discovery, address resolution, and many other network services in a number of routing protocols. For example, Ad hoc On Demand Distance Vector (AODV)[2], Dynamic Source Routing (DSR)[3], use broadcasting or its derivative to establish routes. Existing routing protocols typically assume a simplistic form of broadcasting widely known as flooding, in which each mobile node retransmits a broadcast packet exactly once. Despite its simplicity, it can result in high redundant retransmission, contention and collision, a phenomenon collectively referred to as the broadcast storm problem, which can greatly increase the network communication overhead. To mitigate the deleterious effects of this problem, several broadcast schemes have been suggested. These schemes are commonly divided into two categories; deterministic and probabilistic. Deterministic schemes use network topological information to build a virtual backbone that covers all the nodes in the network. In order to build a virtual backbone, nodes exchange information, typically about their immediate or two hop neighbors. However, they incur a large overhead in terms of time and message complexity for building and maintaining the backbone, especially in the presence of mobility.

II. EXISTING WORK

In the existing system, the conventional on-demand routing protocols use flooding to discover a route. They broadcast a Route REQuest (RREQ) packet to the networks, and the broad-casting induces excessive redundant retransmissions of RREQ packet and causes the broadcast storm problem[4], which leads to a considerable number of packet collisions, especially in dense networks. Therefore, it is indispensable to optimize this broadcasting mechanism.

DOI: 10.15680/IJIRCCE.2016. 0411154

Some methods have been proposed to optimize the broadcast problem in MANETs in the past few years. Williams and Camp [5] categorized broadcasting protocols into four classes: "simple flooding, probability-based methods, area-based methods, and neighbor knowledge methods." For the above four classes of broadcasting protocols, they showed that an increase in the number of nodes in a static network will degrade the performance of the probability based and area-based methods [6]. Kim [7] indicated that the performance of neighbor knowledge methods is better than that of area-based ones, and the performance of area-based methods is better than that of probability-based one.

Xin Ming Zhang [5,8] show that the probabilistic rebroadcast protocol based on neighbor coverage to reduce the routing overhead in MANETs but it cannot provide security during communication. This neighbor coverage knowledge includes additional coverage ratio and connectivity factor. A new scheme is to dynamically calculate the rebroadcast delay, which is used to determine the forwarding order and more effectively exploit the neighbor coverage knowledge. Simulation results show that the proposed protocol generates less rebroadcast traffic than the flooding and some other optimized scheme in literatures. C. Perkins [2] shows that the Ad hoc On-Demand Distance Vector (AODV) routing protocol is intended for use by mobile nodes in an ad hoc network. 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. It uses destination sequence numbers to ensure loop freedom at all times, avoiding problems associated with classical distance vector protocols.

The Ad hoc On-Demand Distance Vector (AODV) algorithm enables dynamic, self-starting, multihop routing between participating mobile nodes wishing to establish and maintain an ad hoc network. AODV allows mobile nodes to obtain routes quickly for new destinations. AODV allows mobile nodes to respond to link breakages and changes in network topology in a timely manner. The destination sequence number is created by the destination to be included along with any route information it sends to requesting nodes.

Disadvantages of exiting system:

1. Routers may overloaded in a dense network leads to frequent link breakages and path failures occurs.
2. Packet delivery does not take place in time, so reduce in packet delivery.
3. Increase in end-to-end delay transmissions.
4. Broadcast storm problem occurs due to number of packet collisions in dense network [9].
5. Security during Communication is not provided.

III. PROPOSED WORK

Neighbor Coverage Based Probabilistic Rebroadcasting protocol (NCPR) works on two key terms. The rebroadcast delay and rebroadcast probability. While calculating rebroadcast delay for each node in the network NCPR have to consider the delay ratio of each node and neighbor set of each node.

A. *UNCOVERED NEIGHBORS SET AND REBROADCAST DELAY:*

The network manager has to identify the uncovered neighbor set for each node. The pre-calculation of this will increase the performance. Whenever a node receives a RREQ packet from another node it will calculate the uncovered neighbor set of that node in terms of source node. So the current node need not broadcast the packet to all neighbors. It can forward it to the uncovered neighbors alone. This will decrease the routing overhead, and increase the packet delivery ratio. For a node ni, the uncovered neighbor set is,

$$UN(n_i)=N(n_i)-[N(n_i)\cap N(s)]-\{s\},\text{...} \qquad (1)$$

Where $N(n_i)$ and $N(s)$ are neighbor set of node n_i and s. Node s sends the request to node n_i.

In order to exploit the neighbor knowledge each node should calculate the delay for rebroadcasting the request for each node. The rebroadcast delay $T_{rd}(n_i)$ for the node ni is,

$$T_{nd}(n_i) = 1 - \frac{|N(s) \cap N(ni)|}{|N(s)|} \text{ ....} \qquad (2)$$

$$T_{rd}(n_i) = MaxDelay * T_{nd}(n_i)$$

DOI: 10.15680/IJIRCCE.2016. 0411154

Where MaxDelay is a fixed value. $T_{nd}(n_i)$ is the node delay ratio of node n_i. The delay value is calculated to exploit the neighbor knowledge; from this network can determine the forwarding order. When a node s sends a RREQ packet, assume node n_j has the highest common neighbor. So forwarding the packet to that node will cover more nodes and other nodes can adjust their uncovered neighbor set according to n_j. The aim of calculating this delay is not to send this packet to more nodes but, to gather neighbor knowledge quickly.

B. *NEIGHBOR KNOWLEDGE AND REBROADCAST PROBABILITY:*

The protocol next calculates the rebroadcast probability. According to delay network manager will calculate set a timer value. When this timer value expires the node will update its final uncovered neighbor set. The nodes in the neighbor set are the nodes which have not yet received the RREQ. Here NCPR define additional coverage ratio $R_{add}(n_i)$ is,

$$R_{add}(n_i) = \frac{|UN(ni)|}{|N(ni)|} \ldots\ldots\ldots\ldots\ldots\ldots \quad (3)$$

The nodes that have to additionally covered have to receive RREQ packets again. The rebroadcast probability should be always high, this will indicate more number of nodes have to receive RREQ and have to process it. Now, network has to define the connectivity factor. The connectivity factor reveals the number of neighbor nodes for a particular node. The connectivity factor $Cf(n_i)$ is ,

$$Cf(n_i) = \frac{Nc}{|N(ni)|} \ldots\ldots\ldots\ldots\ldots\ldots \quad (4)$$

Where N_c is 5.1774 log n [10], and n defines the number of nodes in the network. By calculating both additional coverage ratio and connectivity factor NCPR now define the rebroadcast probability $P_{re}(n_i)$,

$$P_{re}(n_i)= Cf(n_i) * R_{add}(n_i) \ldots\ldots\ldots\ldots \quad (5)$$

If the value of probability exceeds 1 that node set it to 1. This calculation is not depended on local density of the network. The value of Cf is inversely proportional to local node density. This factor makes the NCPR to work efficiently in both dense and sparse area. So whenever a link breakage occurs the protocol has to calculate these parameters and should exploit the neighbor knowledge. So the additional overhead of broadcasting the RREQ is reduced and as the node buffers the packet till the timer expires will increase the packet deliver ratio. The NCPR protocol avoids the use of HELLO packet mechanism. But whenever the timer expires the node have to start from initial stage by broadcasting RREQ and calculating the rebroadcast delay and rebroadcast probability from that node to the destination. Using these parameters NCPR works better compare to other existing protocols. Now the following section will discuss how the NCPR protocol works, the algorithm depicts the working.

C. *ALGORITHM OF NCPR*

Definitions:
RREQi: RREQ packet received from node i.
IDi:id: the unique identifier (id) of RREQi.
N(i): Neighbor set of node i.
UN(i): Uncovered neighbors set of node u for RREQ .
Timer(i): Timer of node i .

1. if node ni receives a new RREQs from source s then do step
2. Compute uncovered neighbors set $UN(n_i)$ for route request RREQs
3. $UN(n_i)=N(n_i)- [N(n_i) \cap N(s)] -\{s\}$
4. Compute the rebroadcast delay $T_{rd}(n_i)$
5. $T_{nd}(n_i) = 1 - \frac{|N(s) \cap N(ni)|}{|N(s)|}$
6. $T_{rd}(n_i)=MaxDelay * T_{nd}(n_i)$
7. Set a Timer(n_i) according to $T_{rd}(n_i)$
8. end if

```
While $n_i$ receives duplicate $RREQ_j$ from $n_j$ before Timer($n_i$) expires do
    Adjust UN($n_i$)
    UN($n_i$) = UN($n_i$) – [UN($n_i$) ∩ N($n_j$)]
    Discard route request $RREQ_j$
end while
if Timer($n_i$) expires then
    Compute the rebroadcast probability $P_{re}(n_i)$
    $R_{add}(n_i) = \frac{|UN(ni)|}{|N(ni)|}$
    $Cf(n_i) = \frac{Nc}{|N(ni)|}$
    $P_{re}(n_i) = Cf(n_i) * R_{add}(n_i)$
    if Random(0,1) ≤ $P_{re}(n_i)$ then
        Broadcast Route request
    Else
        Discard Route request
    end if
end if
```

IV. RSA ALGORITHM

In [11], Algorithm: Generate an RSA key pair.
INPUT: Required modulus bit length, k.
OUTPUT: An RSA key pair ((N,e), d) where N is the modulus, the product of two primes (N=pq) not exceeding k bits in length; e is the public exponent, a number less than and coprime to (p-1)(q-1); and d is the private exponent such that ed ≡ 1 (mod (p-1)(q-1)).

```
Select a value of e from {3, 5, 17, 257, 65537}
Repeat
    p ← genprime(k/2)
until (p mod e) ≠ 1
repeat
    q ← genprime(k - k/2)
until (q mod e) ≠ 1
N ← pq
L ← (p-1)(q-1)
d ← modinv(e, L)
return (N, e, d)
```

Encryption:
Source Node does the following:-

1. Obtains the recipient B's public key (n, e).
2. Represents the plaintext message as a positive integer m, 1 < m < n.
3. Computes the ciphertext c = me mod n.
4. Sends the ciphertext c to B.

Decryption:
Destination Node does the following:-

1. Uses his private key (n, d) to compute m = cd mod n.
2. Extracts the plaintext from the message representative m.

V. SIMULATION RESULTS

To check the performance of proposed NCPR protocol, we evaluate it on NS-2 Simulator. We compare it with the existing AODV protocol. For the simulation, we set the simulation parameters like topology size, number of nodes, transmission range, bandwidth, Queue size, traffic type, number of CBR Connections, packet size, packet rate, minimum speed, maximum speed etc.

Data and control packets share the same physical channel in the IEEE 802.11 protocol, as the number of CBR connections increases, the physical channel will be busier and then the collision of the MAC layer will be more severe. NCPR protocols do not consider load balance, but they can reduce the redundant rebroadcast and alleviate the channel congestion, so as to reduce the packet drops caused by collisions. Here we take different CBR Connections to check the performance of NCPR Protocol.

We evaluate the performance of proposed NCPR protocol on the basis of following network parameters.

1. *Packet delivery ratio*

It is ratio of number of data packets successfully received to destination to number of data packets generated by the source. NCPR protocols increase the packet delivery ratio compared to the conventional AODV protocol. The comparison is shown in graph 1.

2. *Normalized routing overhead*

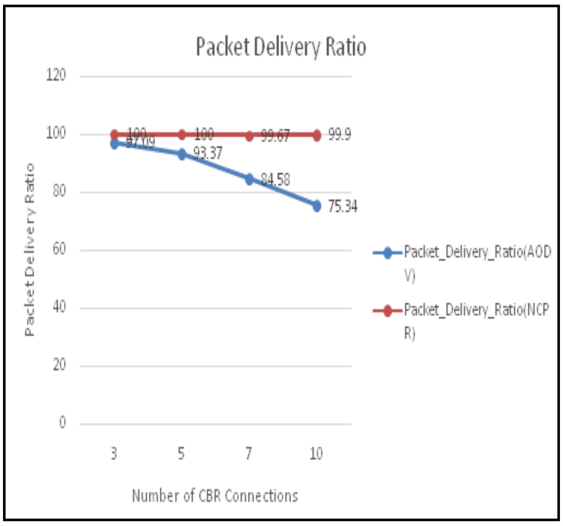
It is the ratio of the total packet size of control packets to the total packet size of data packets delivered to destination. NCPR protocols decrease the normalized routing overhead compared to the conventional AODV protocol. The comparison is shown in graph 2.

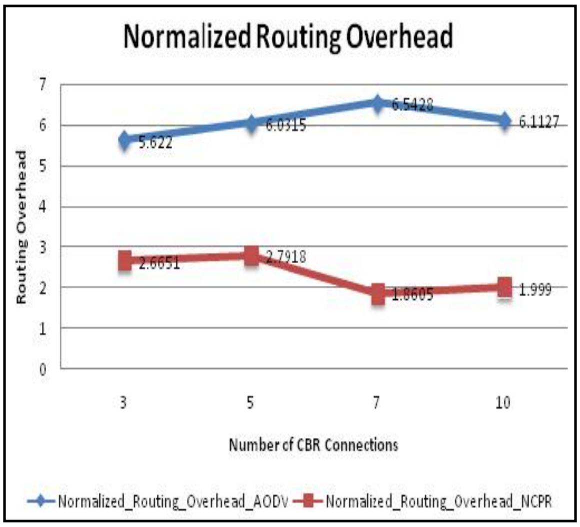
3. *Average End to end delay*

It is the average delay of successfully delivered CBR packets from source to destination. It also includes all the possible delay. NCPR protocols reduce the average end to end delay compared to the conventional AODV protocol. The comparison is shown in graph 3.

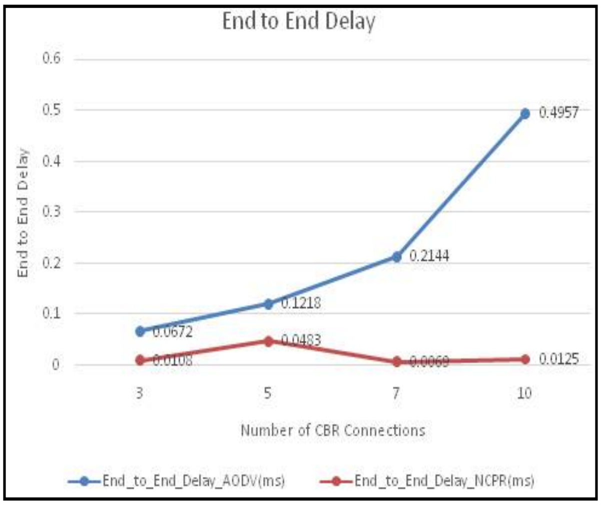
4. *Throughput*

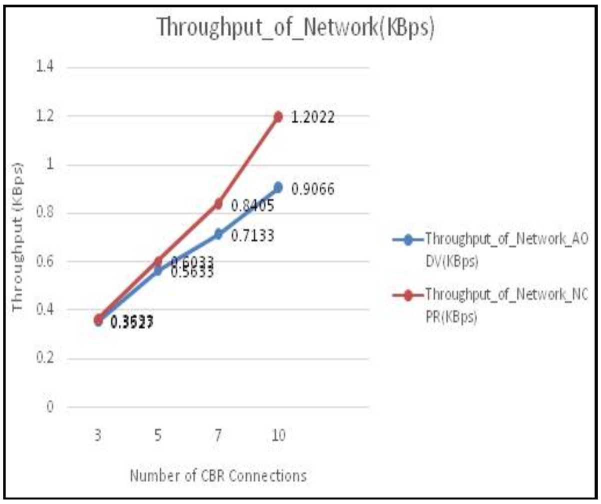
It is the amount of data moved successfully from source to destination in the given time period. It is maximum rate of successful message delivery over communication channel. NCPR protocols increase the throughput of the network compared to the conventional AODV protocol. The comparison is shown in graph 4.





DOI: 10.15680/IJIRCCE.2016. 0411154





VI. Conclusion and Future Work

In this work, the proposed algorithm aims to improve the routing efficiency of MANET .Whenever a route fails it won't suddenly broadcast route request; it will wait till timer expires. At that time the node will buffer the packets. If route is re-established within timer it will send the packets through same link, else it will re-broadcast the route request. The calculation of re-broadcasting probability and rebroadcasting timer helps to improve the performance of the network by reducing the routing overhead. As the buffering of packets and less redundant re-transmission occurs this will lead to high packet delivery ratio.

REFERENCES

1. A Aarti, Dr. S. S. Tyagi, "Study of MANET: Characteristics, Challenges, Application and Security Attacks", International Journal of Advanced Research in Computer Science and Software Engineering, volume 3, Issue 5, pp. 252-257, 2013.
2. C. Perkins, E. Belding-Royer, and S. Das, "Ad Hoc On-Demand Distance Vector (AODV) Routing", IETF RFC 3561, pp 331-343, 2003.
3. D. Johnson, Y. Hu, and D. Maltz, "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR) for IPv4", IETF RFC 4728, vol. 15, pp. 153-181, 2007.
4. Sze-Yao Ni, Yu-Chee Tseng, Yuh-Shyan Chen, and Jang-Ping Sheu, "The Broadcast Storm Problem in a Mobile Ad Hoc Network" ACM/IEEE Mobicom, pp 151-162, 1999.
5. Xin Ming Zhang, En Bo Wang, Jing Jing Xia and Dan Keun Sung, "A Neighbor Coverage-Based Probabilistic Rebroadcast for Reducing Routing Overhead in Mobile Ad Hoc Networks", IEEE Transactions On Mobile Computing, VOL. 12, NO. 3, pp. 424-433, 2013.
6. B. Williams and T. Camp, "Comparison of Broadcasting Techniques for Mobile Ad Hoc Networks," Proc. ACM MobiHoc, pp. 194-205, 2002.
7. J. Kim, Q. Zhang, and D.P. Agrawal, "Probabilistic Broadcasting Based on Coverage Area and Neighbor Confirmation in Mobile Ad Hoc Networks," Proc. IEEE GlobeCom, pp 634-639, 2004.
8. Vijay U. Patil, Prof. A.S. Tamboli, "Review of reducing Routing Overhead in Mobile Ad-hoc Networks by a Neighbor Coverage-Based Algorithm ", IJTEL volume 2, pp 327-330, 2013.
9. A. Mohammed, M. Ould-Khaoua, L.M. Mackenzie, C. Perkins, and J.D. Abdulai, "Probabilistic Counter-Based Route Discovery for Mobile Ad Hoc Networks," Proc. Int'l Conf. Wireless Comm. And Mobile Computing: Connecting the World Wirelessly (IWCMC), pp. 1335-1339, 2009.
10. F. Xue and P.R. Kumar, "The Number of Neighbors Needed for Connectivity of Wireless Networks," Wireless Networks, vol. 10, no. 2, pp. 169-181, 2004.
11. C.P. Pfleeger and S.L.Pfleeger, "Security in Computing", Pearson Education (LPE), 4th edition, Prentice Hall, pp 451-456, oct 2006.