Energy Efficient Cluster Based Optimizing Broadcast Mechanism for Adhoc Networks

M.Preethi [1], S.Vibu[2]
1 Assistant Professor, AVS Engineering College, Salem
2 M.E. Computer Science and Engineering, AVS Engineering College, Salem

Abstract

A mobile ad hoc network (MANET) is a collection of mobile nodes dynamically forming a temporary network without the use of any existing network infrastructure or centralized administration. Blind flooding is extensively use in ad hoc routing protocols for on-demand route discovery, where a mobile node blindly rebroadcasts received Route Request (RREQ) packets until a route to a particular destination is established. This can potentially lead to high channel contention, causing redundant retransmissions and thus excessive packet collisions in the network. These create the overhead in the routing protocol during the route discovery. Here Rebroadcast Probability algorithm is used for reducing the routing overhead in route discovery. After finding the path the data packet is send to the destination. Another technique proposed here to provide the data security in MANET using node authentication and digital signature. This security mechanism called SMDNA (Securing MANET Data using Node Authentication) improves the performance of the routing protocol AODV.

Keywords: *collision, contention, digital signature, routing overhead, authentication.*

1. Introduction

MANETs is formed dynamically by an autonomous system of mobile nodes that are linked via wireless network link without using a prevailing fixed network infrastructure and without centralized administration. The nodes are free to move randomly and organize themselves arbitrarily; thus, the network's wireless topology may change promptly and arbitrarily. Nodes in MANETs act as end points and sometimes router to forward packets in a wireless multi-hop environment. One of the fundamental challenges in the design of dynamic routing protocol can efficiently establish routes to deliver the data packet between mobile nodes with minimum communication overhead compared to other network communication while ensuring high throughput and low end-to-end delay.

1.1 Broadcast Storm in MANET

Many routing protocols, such as Ad-hoc On-demand Distance Vector Routing (AODV) and Dynamic Source Routing (DSR), have been proposed for MANETs. The above two protocols are on-demand routing protocols, and they could improve the scalability of MANETs by controlling the routing overhead when a new route is requested .The conventional on-demand routing protocols have used Flooding to realize a route. They broadcast a Route Request (RREQ) packet to the networks, and the broadcasting encourages extreme level of redundant retransmissions of RREQ packet and causes the broadcast storm problem, which leads to a considerable number of packet collisions, particularly in dense networks. Therefore, it is requisite elevate the broadcasting mechanism .Some of the methods have been optimized the broadcast problem in MANETs for past few years. Broadcasting protocols categorized into four classes: simple flooding, probability based methods, area-based methods, and neighbor knowledge methods .These four protocols are only suitable for static network, when the nodes are increased, it degrades the performance of the probability-based and area-based methods. The performance of neighbor knowledge methods is better than that of area-based and probability-based ones.

In this paper, Rebroadcast Probability Using Neighbor-Coverage Knowledge is proposing to limit the number of rebroadcasts and effectually achieve the route discovery without any conflict in the network communication and the node authentication provided by the cryptographic algorithm.

1.2 Security Goals

In providing a secure networking environment some or all of the following service may be required.

1. **Authentication:** This service verifies the identity of node or a user, and to be able to prevent impersonation. There is no central authority in MANET, and it is much more difficult to authenticate an entity. Authentication can be providing using encryption along with cryptographic hash function, digital signature and certificates.

2. Confidentially: Keep the information sent unreadable to unauthorized users or nodes. MANET uses an open medium, so usually all nodes within the direct transmission range can obtain the data. One way to keep information confidential is to encrypt the data.

3. Integrity: Ensure that the data has been not altered during transmission. The integrity service can be provided using cryptography hash function along with some form of encryption.

4. Availability: Ensure that the intended network security services listed above are available to the intended parties when required. The availability is typically endure by redundancy, physical protection and other non-cryptographic means, e.g. use of robust protocol.

5. Non-repudiation: Ensure that parties can prove the transmission or reception of information by another party, i.e. a party cannot falsely deny having received or sent certain data. By producing a signature for the message, the entity cannot later deny the message

6. Access Control: To prevent unauthorized use of network services and system resources. Obviously, access control is tied to authentication attributes.

2. Related Work

Broadcasting is an effective mechanism for route discovery, but the routing overhead associated with the broadcasting can be quite large, especially in high dynamic networks [9].The broadcasting protocol analytically and experimentally are showed that the rebroadcast is very costly and consumes too much network resource. The broadcasting incurs large routing overhead and causes many problems such as redundant retransmissions, contentions, and collisions. Thus, optimizing the broad- casting in route discovery is an effective solution to improve the routing performance. Haas et al. [7] proposed a gossip- based approach, where each node forwards a packet with a probability. They showed that gossip-based approach can save up to 35 percent overhead compared to the flooding. However, when the network density is high or the traffic load is heavy, the improvement of the gossip-based approach is limited.

Kim et al. [5] Proposed a probabilistic broadcasting scheme based on coverage area and neighbor confirmation. This scheme uses the coverage area to set the rebroadcast probability, and uses the neighbor confirmation to guarantee reachability. [8] Proposed a neighbor knowledge scheme named Scalable Broadcast Algorithm (SBA). This scheme determines the rebroadcast of a packet according to the fact whether this rebroadcast would reach additional nodes. Proposed a Dynamic Probabilistic Route Discovery (DPR) scheme based on neighbor coverage. In this approach, each node determines the forwarding probability according to the number of its neighbors and the set of neighbors which are covered by the previous broadcast. This scheme only considers the coverage ratio by the previous node, and it does not consider the neighbors receiving the duplicate RREQ packet. Thus, there is a room of further optimization and extension to the DPR protocol. approach can save up to 35 percent overhead compared to the flooding. However, when the network density is high or the traffic load is heavy, the improvement of the gossip-based approach is limited.

Kim et al. [5] Proposed a probabilistic broadcasting scheme based on coverage area and neighbor confirmation. This scheme uses the coverage area to set the rebroadcast probability, and uses the neighbor confirmation to guarantee reachability. [8] Proposed a neighbor knowledge scheme named Scalable Broadcast Algorithm (SBA). This scheme determines the rebroadcast of a packet according to the fact whether this rebroadcast would reach additional nodes. Proposed a Dynamic Probabilistic Route Discovery (DPR) scheme based on neighbor coverage. In this approach, each node determines the forwarding probability according to the number of its neighbors and the set of neighbors which are covered by the previous broadcast. This scheme only considers the coverage ratio by the previous node, and it does not consider the neighbors receiving the duplicate RREQ packet. Thus, there is a room of further optimization and extension to the DPR protocol. S.Thadvai et al. [11] proposed a method based on message recovery which includes message and the signature hence the communication cost is lower for the message recovery method. In this method they used the Authentication Encryption Scheme (AES) for message recovery.

3. Rebroadcast Probability Using Neighbor-Coverage Knowledge

3.1. Discovery of Neighbor-Coverage Knowledge

The node receives a RREQ packet from its previous node S, we use the neighbor list in the RREQ packet to estimate how many its neighbors have not been covered by the RREQ packet from Source(s). If the node has more neighbors uncovered by the RREQ packet from us, which means that if node a rebroadcasts the RREQ packet, the RREQ packet can reach more additional neighbor nodes. To quantify of the Uncovered Nimbus' (UCN) set up (a) of node a as follows

$$U(u_i) = N(u_i) - [N(u_i) \cap N(s)] - \{s\} \text{----> } (1)$$

where N(s) and $N(u_i)$ are the neighbors sets of node s and u_i, respectively. s is the node which sends an RREQ packet to node u_i.

According to Eq. (1),

We obtain the initial UCN set. Due to broadcast characteristics of a RREQ packet, the node we can receive the duplicate RREQ packets from its neighbors. Node u_i could further adjust the $U(u_i)$ with the neighbor knowledge.

In order to sufficiently exploit the neighborhood knowledge and avoid channel collisions, each node should set a rebroadcast delay. The choice of a proper delay is the key to success for the proposed protocol because the scheme used to determine the delay time affects the dissemination of neighbor coverage knowledge. When a neighbor receives a RREQ packet, it could calculate the rebroadcast delay according to the neighbor list in the RREQ packet and its own neighbor list. The rebroadcast delay $T_d(u_i)$ of node ui is defined as follows:

$$T_p(u_i) = 1-|N(s)\cap N(u_i)||N(s)|$$

$$T_d(u_i) = MaxDelay \times T_p(u_i) \text{ ,-------->(2)}$$

where $T_p(u_i)$ is the delay ratio of node ui, and MaxDelay is a small constant delay. $|\cdot|$ Is the number of elements in a set.

The above rebroadcast delay is defined with the following reasons: Firstly, the delay time is used to determine the node transmission order. To sufficiently exploit the neighbor coverage knowledge, it should be disseminated as quickly as possible. When node s sends a RREQ packet, all its neighbors a, I = 1, 2, · · · , |N (s) | receive and process the RREQ packet. We assume that node u_k has the largest number of common neighbors with node s, according to Eq. (2), node u_k has the lowest delay. Once node u_k rebroadcasts the RREQ packet, there are more nodes to receive it, because node u_k has the largest number of common neighbors. Then there are more nodes which can exploit the neighbor knowledge to adjust their UCN sets. Of course, whether node u_k rebroadcasts the RREQ packet depends on its rebroadcast probability calculated in the next subsection. The objective of this rebroadcast delay is not to rebroadcast the RREQ packet to more nodes, but to disseminate the neighbor coverage knowledge more quickly. After determining the rebroadcast delay, the node can set its own timer.

3.2. Adjustment of uncovered neighbor set

The node which has a more rebroadcast delay might listen to RREQ packets from the nodes, which have lesser one. For example, if node u_i receives a duplicate RREQ packet from its neighbour v_j , it knows that how many its neighbours have been covered by the RREQ packet from v_j . Thus, node ui could further adjust its UCN set according to the neighbor list in the RREQ packet from v_j . Then the $U(u_i)$ can be adjusted as follows:

$$U(u_i) = U(u_i) - [U(u_i) \cap N(v_j)]\text{------->(3)}$$

After adjusting the $U(u_i)$, the RREQ packet received from v_j is discarded. Do not need to adjust the rebroadcast delay because the rebroadcast delay is used to determine the order of disseminating neighbor coverage knowledge to the nodes which receive the same RREQ packet from the upstream node. Thus, it is determined by the neighbors of upstream nodes and its own.

3.3. Rebroadcast Probability

When the timer of the rebroadcast delay of node u_i expires, the node obtains the final UCN set. The nodes belonging to the final UCN set are the nodes that need to receive and process the RREQ packet. Note that, if a node does not sense any duplicate RREQ packets from its neighborhood, its UCN set is not changed, which is the initial UCN set. The additional coverage ratio $R_a(u_i)$.

$$R_a(u_i) = \frac{|U(u_i)|}{N(u_i)} \text{ ----------> (4)}$$

This metric indicates the ratio of the number of nodes that are additionally covered by this rebroadcast to the total number of neighbors of node ui. [10] Derived that if each node connects to more than 5:1774 $\log_n$ of its nearest neighbors, then the probability of the network being connected is approaching 1 as n increases, where n is the number of nodes in the network. Then, we can use 5:1774 $\log_n$ as the connectivity metric of the network.

$$F_c(u_i) = \frac{N_c}{|N(u_i)|} \text{ ----------->(5)}$$

Nc = 5.1774 $\log_n$, the n is the number of nodes inthe network. The Eq. (5), observe that when $|N(u_i)| > N_c$, $Fc(ui) < 1$. The means node ui is in the dense area of the network, then only part of neighbours of

node u_i forwarded the RREQ packet could keep the network connectivity. And $|N(u_i)| < N_c$, $F_c(u_i) > 1$.

The means of node ui is in the sparse area of the network, then node ui should forward the RREQ packet in order to approach network connectivity. Combining the additional coverage ratio and connectivity factor, to obtain the rebroadcast probability Pre (ui) of node ui

$$Pre(ui)=Ra(ui).Fc(ui) \text{ ----------> } (6)$$

Where, if the Pre (ui) is > 1, to set the Pre (ui) to 1.

3.4. Algorithm Description

The formal description of the Dynamic Rebroadcast Probability Using Neighbor-Coverage Knowledge For Reducing Storm Problem in route discovery is shown in Algorithm 1.

Algorithm 1

Definitions:

$RREQ_v$: RREQ packet received from node v.
R_v.id: the unique identifier (id) of $RREQ_v$.
N(u): Neighbor set of node u.
U(u, x): Uncovered neighbors set of node u for RREQ whose id is x.
Timer(u, x): Timer of node u for RREQ packet whose id is x.
{Note that, in the actual implementation of NCPR protocol, every different RREQ needs a UCN set and a Timer.}

1. if u_i receives a new RREQs from s then
2. {Compute initial uncovered neighbors set $U(u_i,R_s.id)$ for $RREQ_s$:}
3. $U(u_i,R_s.id) = N(u_i) - [N(u_i) \cap N(s)] - \{s\}$
4. {Compute the rebroadcast delay $T_d(u_i)$:}
5. $T_p(u_i) = 1 - |N(s) \cap N(u_i)| \; |N(s)|$
6. $T_d(ui) = MaxDelay \times T_p(ui)$
7. Set a Timer(u_i,R_s.id) according to Td(ui)
8. end if
9. while u_i receives a duplicate $RREQ_j$ from v_j before
10. Timer(u_i,R_s.id) expires do
11. {Adjust $U(u_i,R_s.id)$:}
12. $U(u_i,R_s.id) = U(u_i,R_s.id) - [U(u_i,R_s.id) \cap N(v_j)]$
13. discard($RREQ_j$)
14. end while
15. if Timer(u_i,R_s.id) expires then
16. {Compute the rebroadcast probability $P_{re}(u_i)$:}
17. $R_a(u_i) = |U(u_i,R_s.id)| \; |N(u_i)|$
18. $F_c(u_i) = N_c/|N(u_i)$
19. $P_{re}(u_i) = F_c(u_i) \cdot R(u_i)$
20. if Random(0,1) $\leq$ $Pre(u_i)$ then
21. broadcast(RREQs)
22. else
23. discard(RREQs)
24. end if
25. end if

4. MANET Security

4.1. Security Criteria for MANET

In MANET the security to data was not provided while in communication. Also the node authentication of trusted nodes was not provided sufficiently. Whenever a new node wants to join the network there was no provision present to authenticate it and join it in network.

To achieve secure communication in MANET some requirements must be satisfied:

(a) A security association must exist between network members, these security associations ensure authentication and non-repudiation for trusted nodes.

(b) Sensitive information must be exchanged confidentially between the nodes in the network.

(c) Integrity of the information exchanged within the network has to be maintained so that corrupted messages are detected and blocked.

As symmetric cipher algorithm allows us to store the data in a compressed encryption form which results in a small size database. Also it

performs faster encryption/decryption. Due to these advantages we are using symmetric cipher algorithm to perform data encryption and decryption. This will also serve confidentiality. Moreover we combine the MD-5 and RSA public key algorithm to generate the digital signature.

The main advantage of using digital signature is it provides user authentication and data integrity and non-repudiation. As digital signature is akin to signing the document physically, it is the acknowledgement of the message so sender cannot deny the message.

4.2 Securing MANET Data using Node Authentication

Step1. Initially establish the route to receiving node by the control message of AODV i.e. RREQ

Step 2.Receiver then sends back RREP message to the sender along with its hash value of IP address.

Step3.This hash value of IP address is compared with the hash value at sender side, if same then that node is trusted node.

Step4. Issue trusted node a digital signature using MD-5 and RSA

Step5. Using Symmetric key encryption algorithm AES encrypt the data and send it to receiver. Along with digital signature

Step6. Intermediate node checks for digital signature and if valid then forwards data.

Step7. If digital signature is invalid that means malicious node, find another route.

Step8. At receiver side decrypts data using AES

Conclusion

The work proposed here is to reduce the routing overhead and provide the data security in MANET. The Rebroadcast Probability algorithm combines the advantages of the neighbor coverage knowledge and the probable mechanism, which can significantly decrease the number of retransmissions so as to reduce the routing overhead, and can also improve the routing performance. Securing data in mobile ad hoc network using the digital signature scheme applied on AODV routing protocol. Also symmetric key cryptography for the fast encryption/ decryption process. The authentication of node done through the IP address of destination this ensures the reliability of node.

References

[1] C. Perkins, E. Belding-Royer, and S. Das, Ad Hoc On-Demand Distance Vector (AODV) Routing, IETF RFC 3561, 2003.

[2] 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

[3] H. AlAamri, M. Abolhasan, and T. Wysocki, "On Optimizing Route Discovery in Absence of Previous Route Information in MANETs," Proc. IEEE Vehicular Technology Conf. (VTC), pp. 1-5, 2009.

[4] S.Y. Ni, Y.C. Tseng, Y.S. Chen, and J.P. Sheu, "The Broadcast Storm Problem in a Mobile Ad Hoc Network," Proc. ACM/IEEE MobiCom, pp. 151-162, 1999.

[5] 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, 2004.

[6] J.D. Abdulai, M. Ould-Khaoua, and L.M. Mackenzie, "Improving Probabilistic Route Discovery in Mobile Ad Hoc Networks," Proc. IEEE Conf. Local Computer Networks, pp. 739-746, 2007.

[7] Z. Haas, J.Y. Halpern, and L. Li, "Gossip-Based Ad Hoc Routing," Proc. IEEE INFOCOM, vol. 21, pp. 1707-1716, 2002.

[8] W. Peng and X. Lu, "On the Reduction of Broadcast Redundancy in Mobile Ad Hoc Networks," Proc. ACM MobiHoc, pp. 129-130, 2000.

[9] J.D. Abdulai, M. Ould-Khaoua, L.M. Mackenzie, and A. Mo- hammed, "Neighbour Coverage: A Dynamic Probabilistic Route Discovery for Mobile Ad Hoc Networks," Proc. Int'l Symp. Performance Evaluation of Computer and Telecomm. Systems (SPECTS '08), pp. 165-172, 2008.

[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