International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 2 Issue 10, October - 2013

A Counter Based Broadcasting Using Symmetric Neighbor Verification Protocol

Nafisa M. Mapari [1], Prof. (Dr.) J. W. Bakal[2]
Pillai's Institute of Technology, Panvel

Abstract

The objective is to determine a small set of forward nodes to ensure full coverage. A formal framework is used to model inaccurate local views in MANETs, where full coverage is guaranteed if three sufficient conditions connectivity, link availability, and consistency are met. A MANET consists of a set of mobile hosts that may communicate with one another from time to time. Broadcasting in MANETs is a fundamental data dissemination mechanism, with important applications, e.g., route query process in many routing protocols, address resolution and diffusing information to the whole network. Broadcasting in MANETs has traditionally been based on flooding, which overwhelm the network with large number of rebroadcast packets. The widely accepted existing routing protocols designed to accommodate the needs of such self-organized networks do not address possible threats or attacks aiming at the disruption of the protocol itself. The widely assumed trusted environment is not really the environment that can be realistically expected in reality. While broadcasting hello packets originated from its neighbours, may aim to create fake symmetric links in the sparse and dense network.

1. INTRODUCTION

A Mobile Ad hoc Network (MANET) is an autonomous system of mobile nodes with routing capabilities connected by wireless links, the union of which forms a communication network modelled in the form of an arbitrary graph. The vision of Mobile Ad Hoc Network (MANET) is wireless internet, where users can move anywhere anytime and still remaining connected with the rest of the world. The main challenges in MANET are reliability, bandwidth and battery power [1]. The network has unpredictable characteristics such as its topology, signal strengths fluctuates with environment and time, communication routes breaks and new ones are formed dynamically. In this context, communication algorithms and protocols should have very light in computational and storage needs in order to conserve energy and bandwidth. Broadcasting is the process in which a source node sends a message to all other nodes in MANET. Network wide broadcasting in Mobile Ad Hoc Network provides important control and route establishment functionality for a number of unicast and multicast protocols. Broadcasting in MANET poses more challenges than in wired networks due to node mobility and scarce system resources. Broadcasting a packet to the entire network is a basic operation and has extensive applications in mobile ad hoc networks (MANETs).

Wireless Mobile Ad Hoc Networking has recently gained a lot of attention in research. A Mobile Ad Hoc Network (MANET) represents the ultimate scenario where the network is operated without the support of any fixed infrastructure. Such networks can be deployed very quickly and are inexpensive as they do not invoke basic infrastructure cost [2]. MANET applications cover various areas such as military or post disaster rescue operations, temporary group collaboration at conferences or lectures, sensor networks and many others. Due to the absence of any fixed infrastructure support in MANETs, the participating nodes must provide the basic communication primitives such as routing, address allocation, name resolution or service discovery themselves. The nature of temporary links and the mobility of the nodes together with wireless transmission effect on attenuation, interference and multipath propagation, bring some inherent issues of mobile ad hoc networks. The links of the mobile ad hoc networks are dynamic in a sense that they are likely to break or change with the movement of the nodes. As the topology changes, the route must be updated immediately by sending a control message. Those unique feature to mobile ad hoc network results in lot of control overhead for route discovery and maintenance. These are highly unacceptable in bandwidth constrained ad hoc networks. Usually these devices have limited computing resources and server energy constraint. Routing strategies along with

mobility management and resource allocation become big challenge to network designers and service provider. The network protocols of mobile ad hoc networks must consider the routing efficiency as well as security. While early research effort assumed a friendly and cooperative environment and focused on problems such as wireless channel access and multi-hop routing, security has become a primary concern in order to provide protected communication between nodes in a hostile environment. The characteristics of MANETs such as open network architecture, shared wireless medium, stringent resource constraints and highly dynamic network topology present a new set of non trivial challenges to security design. Due to these characteristics, mobile ad hoc networks are vulnerable to several types of security attacks.

2. RELATED WORK

One of the earliest broadcast mechanisms is flooding, where every node in the network retransmits a message to its neighbors upon receiving it for the first time. Although flooding is very simple and easy to implement, it can be very costly and may lead to a serious problem, often known as the broadcast storm problem [3, 4] that is characterized by high redundant packet retransmissions, network bandwidth contention and collision. Ni et al [3, 4] have studied the flooding protocol analytically and experimentally. Their obtained results have indicated that rebroadcast could provide at most 61% additional coverage and only 41% additional coverage in average over that already covered by the previous. Therefore, rebroadcasts are very costly and should be used with caution. The authors [5] have classified the broadcast protocols into flooding, probability-based, counter-based, distance-based, location-based and neighbor knowledge schemes. Similarly, neighbor knowledge schemes can be divided into selecting forwarding neighbors and clustering-based. In counter-based scheme inhibits the rebroadcast if the packet has already been received for more than a given number of times. In the probabilistic scheme [6, 7], when receiving a broadcast packet for the first time, a node rebroadcasts the packet with a probability p; when p=1, this scheme reduces to blind flooding. In the distance-based scheme a node rebroadcasts the packet only if the distance between the sender and the receiver is larger than a given threshold. In the location-based scheme, a node rebroadcasts a packet only when the additional coverage due to the new emission is larger than a certain bound. In the selecting forwarding neighbours a broadcasting node selects some of its 1-hop neighbors as rebroadcasting nodes. Finally, the cluster structure is a simple backbone infrastructure whereby the network is partitioned into a group of clusters. Each cluster has one cluster head that dominates all other members in the cluster. A node is called a gateway if it lies within the transmission range of two or more cluster heads. Gateway nodes are generally used for routing between clusters. The rebroadcast is performed by cluster heads and gateways. However, the overhead of cluster formation and maintenance cannot be ignored [5, 8].

2.1 COUNTER-BASED BROADCASTING

A. Mohammed and M.L. Jabaka Says:

Counter-based broadcast scheme aims to mitigate the broadcast storm problem associated with *flooding.* The use of the scheme for broadcasting in MANETs enables mobile nodes to make localized rebroadcast decisions.Ni *et al.* (1999) have shown an inverse relationship between the number of times a packet is received at a particular node and the probability of that node being able to reach additional coverage area on a rebroadcast. This result is the foundation of their counter-based broadcast scheme. Specifically, a node upon reception of a previously unseen packet initiates a counter c that will record the number of times a node receives the same packet. Such a counter is maintained by each node for each broadcast packet. After waiting for a random assessment delay (RAD, which is randomly chosen between 0 and Tmax seconds), if c reaches a predefined threshold C, the packet is rebroadcasted. Each node increments its c by one each time it receives the same packet until the RAD expires. The node compares its c with a predefined counter threshold C. If $c < C$, the node rebroadcasts the packet. Otherwise the packet is dropped [9].

Advantage:

- Counter based broadcasts incur significantly lower overhead compared to blind flooding while maintaining a high degree of propagation for the broadcast messages.
- In dense networks, multiple nodes share similar transmission range. Therefore, these thresholds control the frequency of rebroadcasts and thus might save network resources without affecting delivery ratios.

Limitation:

- In sparse networks there is much less shared coverage; thus some nodes will not receive all the broadcast packets unless the threshold parameter is low.

- If the threshold c is set to a far smaller value, reachability will be poor.
- If *c* is set far large, many redundant rebroadcasts will be generated.

2.2 NEW ADAPTIVE COUNTER BASED BROADCAST USING NEIGHBORHOOD NFORMATION IN MANETS

M. Bani Yassein, A. Al-Dubai, M. Ould Khaoua, Omar M. Al-jarrah says:

This algorithm keeps track of counter c for number of times broadcast packet is received. A counter threshold is decided based on neighboring information. That is a sparse network has a different threshold than a medium or dense network, say *c*1 and c2, respectively. Whenever *c* is greater than or equal to the threshold, the rebroadcast is inhibited [10]. An average neighbor number are calculated as the basis for the selection of the value of *c*. Where *A* be the area of an ad hoc network, *N* be the number of mobile hosts in the network, and *R* be the transmutation range. The average number of neighbor *n* can be obtained as shown below [6, 7].

Equation 1:Average Number of neighbors

$$\overline{n} = (N-1)0.8\frac{\pi^2}{A}$$

Advantages:

- Dynamically adjusts the counter based threshold value *c* at each mobile host according to the value of the local number of neighbours.

Limitations:

- Broadcasting is consider but delay occurring between exchanges of hello message is not focused. Delay occurring in exchanging hello messages may be because of malicious node continuously broadcast the hello packet to the node present in network and because of that your node may take time to respond source node.

2.3 SYMMETRIC NEIGHBOR VERIFICATION PROTOCOL

Soufiene Djahel, Farid Nait-Abdesselam says:

Author says that if the difference between message transmission delay from *i* to *j* (D_{ij}) and from *j* to *I* (D_{ji}) is greater than a threshold represents the difference between the message transmission delay from *i* to *j* and the mes- sage transmission delay from *j* to *i* in the worst case (Δ_t), then the link {*ij*} is asymmetric and there is a misbehaving node that relays the Hello message of *i* to *j* or in the opposite direction. Otherwise it cannot say that nodes *i* and *j* are symmetric neighbors. This is due to the fact that Δ_t is determined based on the speed of light which is, in general, larger than the speed of actual wireless signals. Then it computes the probability that *i* and *j* are actually a symmetric neighbors as follows:

$$Psym_{ij} = |D_{ij} - D_{ji}|/\Delta_t$$

If this probability is smaller than the misbehaving level *lm*, where $0 \leq lm \leq 1$, then it accept the node as symmetric neighbor. Otherwise, we reject it [11].

3. Proposed System:

The **Counter-based broadcasting using Symmetric Neighbor Verification protocol** is based on a counter *c* that is used to keep track of the number of times the broadcast packet is received. A counter threshold is decided based on neighbouring information. That is a sparse network has a different threshold than a medium or dense network, we call them c1, c2 respectively. Whenever *c* is greater than or equal to the threshold, the rebroadcast is inhibited. Once c1 or c2 is fixed it then checks for symmetric neighbor verification [11] .

COUNTER_BASED_BROADCASTING_USING_SYMMETRIC_NEIGHBOR_VERIFICATION_PROTOCOL_Algorithm

Protocol receiving ()

1 *On hearing a broadcast packet m at node X*
2 *Get the Broadcast ID from the packet; n average number of neighbor*
3 *Get degree n of node X (number of neighbors of node X);*
4 **If** *n < n1* **then**

4.1 **Sparse network**
4.2 *Node X has a low degree: the low threshold value (threshold = c1);*
5 **Else**
5.1 **Dense network**
5.2 Node X has a high degree: the high threshold value (threshold = c2);
6 **End if**
7 ***counter = 1***
8 **While (not hearing a message) Do**
8.1 Wait for a random number of slots.
8.2 Submit the packet for transmission and Wait until the transmission actually start
9 **End while**
10 *Increment c*
11 **If** *difference between transmission delay of source and destination < the difference between the message transmission delay from i to j(Dij) and the message transmission delay from j to i(Dji) in the worst case(Δt)* **then**
11.1 *go to Step 14.*
12 **Else**
12.1 **If** *distance between node i to node j < distance between node j to node I* **then**
Node j is asymmetric
12.2 **Else**
Node i is asymmetric
12.3 **End if**
12.4 *Drop the Packet and go to step 14.*
12.5 **If** *(|Dij−Dji|/Δt)< malicious level*
Node i and j are Symmetric, Accept the packet
12.6 ***Else***
Node are asymmetric, Drop the Packet
12.7 **End if**
13 **End if**
14 **If (c < threshold)**
Go to step 7
15 **Else**
Go to step 1
16 **End if**

End

COUNTER_BASED_BROADCASTING_USING_SYMMETRIC_NEIGHBOR_VERIFICATION_PROTOCOL_Algorithm

Figure 1: An outline of the COUNTER BASED BROADCASTING USING SYMMETRIC NEIGHBOR VERIFICATION PROTOCOL Algorithm

The algorithm works as follows. On hearing a broadcast packet *m* at node *X*, the node rebroadcasts the packet according to a low counter based threshold value, say c1 , if the packet is received for the first time, and the number of neighbors of node *X* is less than the minimum numbers of neighbors, *n*1 . And call for subroutine symmetric neighbor verification. Alternatively, if the number of neighbors of the node *X* is greater than maximum number of neighbors, *n*2 , then the counter based threshold value is set high, c2 , where c1 < c2 and call for subroutine symmetric neighbor verification .

5. CONCLUSION

In MANETs, due to node mobility, neighborhood relationship changes frequently. In order to cope with mobility and have up-to-date neighborhood information, nodes advertise 'Hello' packets periodically. This approach focus on counter based authorization of neighbor node called counter based symmetric neighbor validation is introduced. The goal of our approach is to accept valid node in communication network in one broadcasted network nodes. Thus, routes with asymmetric links will be maintained in routing tables, which may lead to data packets loss. And Symmetric Neighbor Verification protocol is based on the principle of checking the symmetry of the link advertised by the neighbor before confirming it.

The selection of misbehaving level lm can be analyzed in more optimal manner and we can design analytical model for optimal value of lm which will help for security requirements of system. We can undertake the required experiments under realistic conditions to better tune the solution. We can also investigate some configurations where the nodes are highly mobile.

References

[1] Natesapillai, Karthikeyan and Palanisamy, V. and Duraiswamy, K., Performance Comparison of Broadcasting Methods in Mobile Ad Hoc Network (February 20, 2009). International Journal of Future Generation Communication and Networking, Vol. 2, No. 2, June 2009.
[2] Vincent Lenders, Martin May, Bernhard Plattner, Service discovery in mobile ad hoc networks: A field theoretic approach, Pervasive and Mobile Computing, Volume 1, Issue 3, September 2005, Pages 343-370, ISSN 1574-1192.

[3] S.-Y. Ni, Y.-C. Tseng, Y.-S. Chen, and J.-P. Sheu,The broadcast storm problem in a mobile ad hoc network, *Wireless Networks*, vol. 8, no. 2, pp.153- 167, 2002

[4] Y.-C. Tseng, S.-Y. Ni, E.-Y. Shih, Adaptive approaches to relieving broadcast storm in a wireless multihop mobile ad hoc network, *IEEE Transactions Computers*, vol. 52, no 5, 2003.

[5] B. Williams, T. Camp, Comparison of broadcasting techniques for mobile ad hoc networks. *Proc. ACM Symposium on Mobile Ad Hoc Networking & Computing* (*MOBIHOC 2002*), pp. 194–205, 2002.

[6] M. Bani-Yassein, M. Ould-Khaoua, L. M. Mackenzie, S. Papanastasiou and A. Jamal, Improving route discovery in ondemand routing protocols using local topology information in MANETs, *Proceedings of the Ninth ACM/IEEE International Symposium on Modeling, Analysis and Simulation of Wireless and Mobile Systems (MSWIM 06)*, pages 95-99, October 2006.

[7] M. Bani-Yassein, M. Ould-Khaoua, L. M. Mackenzie and S. Papanastasiou, Performance Analysis of Adjusted Probabilistic Broadcasting in Mobile Ad Hoc Networks , *International Journal of Wireless Information Networks*, Pages 1-14, Springer Netherlands, Mar 2006.

[8] J. Wu and W. Lou. Forward-node-set-based broadcast in clustered mobile ad hoc networks, special issue on Algorithmic, Geometric, Graph, Combinatorial, and Vectors. *Wireless Networks and MobileComputing*, volume 3(2), pages 155-173,2003.

[9] A. Mohammed, M.L. Jabaka, On the Performance of Counter-Based Broadcast Scheme for Mobile Ad Hoc Networks, *Nigerian Journal of Basic and Applied Science (2009), 17(2), 166-176*

[10] M. Bani Yassein, S. Al-Humoud, M. Ould Khaoua and L.M. Mackenzie, *New Adaptive Counter Based Broadcast Scheme using local Neighbourhood Information in MANETs*, 2009.

[11] Djahel, S.; Naït-Abdesselam, F., "Avoiding virtual link attacks in wireless ad hoc networks," *Computer Systems and Applications, 2008. AICCSA 2008. IEEE/ACS International Conference on* , vol., no., pp.355,360, March 31 2008-April 4 2008.