Asian Journal of Information Technology 14 (1): 23-27, 2015
ISSN: 1682-3915

An Active Addressing Protocol for Auto Configuration of Node in MANETs

P. Seshu Babu, T.V. Subramanyam, I. Leela Priya and M. Venkat Rao
Department of CSE, Vignan's University, Vadlamudi, Guntur, India

Abstract: Assigning the address to mobile ad hoc network is crucial part because it has no infrastructure. A robust protocol has required to enable the network to manage itself avoid collisions. Because of fading channels, frequent partitioning; joining/leaving the nodes to and from the network, collisions may occur. In this study, we analyze light weight protocol which assigns the address to the nodes in the network based on distributed address database stored in filters. This filter reduces the packet losses in the network partitions. The performance of the protocol is evaluated by considering the joining nodes, partition merge events and initialization of network. The final simulation results shows that this protocol overcomes the address collision problem and also controlling the traffic in the network in better way than the other protocols.

Key words: Ad hoc networks, FAP, network partition, trafic, protocol

INTRODUCTION

MANETs is a continuously self-configuring and doesn't have any previous infrastructure and rely on dynamic multi-hop topologies for traffic forwarding. A crucial and usually unaddressed issue of ad hoc networks is the frequent network partitions of the network. Network partitions, caused by node mobility fading channels and node joining and leaving the network can disturb the distributed network control. Due to self organized nature of the MANETs addressing of nodes is more critical part. Centralized mechanisms such as the Dynamic Host Configuration Protocol (DHCP) (Fernandes *et al*., 2013; Zhou *et al*., 2003) having conflicts with the distributed nature of the ad hoc networks due to Network Addresses Translation (NAT), so don't address the network partitioning and merging. A filter based protocol that assures both the univocal address configuration of the nodes joining the network and the detection of address collisions after merging partitions can be designed by considering both the Bloom filter and proposed filter which is called sequence filter (Broder and Mitzenmacher, 2004). The filter is distributed maintained by exchanging the hash of the filter among the neighbors. It is hard to avoid duplicated addresses in simple distributed addressing schemes (Fernandes *et al*., 2013) because a random choice of an address by each node would result in a high collision probability. The IETF Zircons working group proposes hardware based addressing schemes as demonstrated by the birthday paradox which assigns an Ipv6 network address to a node based on the address (Thomson and Narten, 1998; Fan *et al*., 2000).

PROPOSED SYSTEM

Filter based addressing protocol: The main idea behind the proposed protocol is dynamically auto configure network address, resolving collisions with a low control load, even in the case of node joining or node merging events. Two filters depending on the scenario are proposed as follows: the bloom filter which is based on hash functions and the proposed sequence filter which compresses database on the addresses sequences. The system proposes the FAP; it achieves low communication overhead and low latency, resolving all address collisions even in network partition merging events. When compared to other system it reduces the overhead (Fernandes *et al*., 2013, 2009). The proposed system contributes redundancy avoiding technique by reducing control load. This proposed system proposes the FAP to node's address configuration. Address assignment is a key challenge in ad hoc networks due to the lack of infrastructure. Autonomous addressing protocols require a distributed and self-managed mechanism to avoid address collisions in a dynamic network with fading channels, frequent partitions and joining/leaving nodes (Thomson and Narten, 1998; Fan *et al*., 2000).

Bloom filter: The bloom filter is a space-efficient probabilistic data structure that is used to test whether an element is a member of a set. The bloom filter is used in distributed applications because of its compact data structure nature (Zhou *et al*., 2003; Moreira *et al*., 2012). The bloom filter is compressed of an m bit vector that represents a set A = $\{a_1, a_2, a_3, ..., a_m\}$ composed of n

Corresponding Author: P. Seshu Babu, Department of CSE, Vignan's University, Vadlamudi, Guntur, India

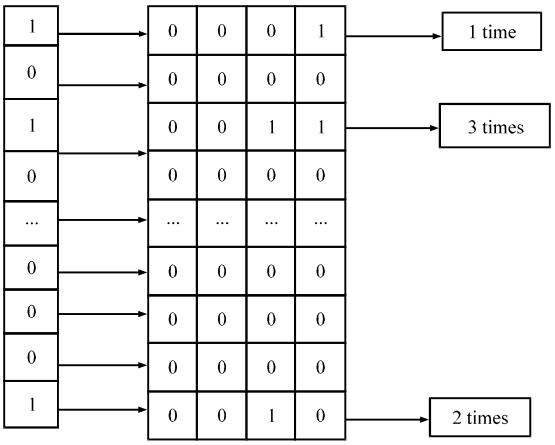

Fig. 1: Blooms filters with counters

elements (Fig. 1). The elements are inserted in the filter through a set of independent hash functions like (h_1, h_2, ..., h_k) where outputs are uniformly distributed over m bits (Cunha *et al*., 2008; Vaidya, 2002). Bloom filters do not present false negatives which mean that a membership test of an element that was inserted into the filter is always positive (Fernandes *et al*., 2009). If m is the number of bits in the array, the probability that a certain bit is not set to 1 by a certain hash function during the insertion of an element is given by 1-1/m. If k is the number of hash functions, the probability that the bit is not set to 1 by any of the hash functions is given by $p_{0 = (1-1/m)}^{kn}$. Which show that the false-positive probability decreases when the number of elements n of set A is decreases or the size of the filter, m is increased. Each bit of the filter is replaced by a counter when there is a need of removal of element from the filter (Thomson and Narten, 1998; Kim *et al*., 2007). Which is given by P_{fp}. $P_{fp = (1-P}0)^k$.

Sequence filter: This filter is created by the concatenation of the first address of the address sequence which we call initial element (a_0) with an r bit vector where r is the address rang size. In this filter, each address suffix is represented by one bit. The sequence filter, proposed in this proposed system which compresses data based on the address sequence. If a bit is in 1, then the address with the given suffix is considered as inserted into the filter; otherwise, the bit in 0 indicates that the address does not belong to the filter. Therefore, there are neither false positive nor false negative in the sequence filter because each available address is deterministically represented by its respective bit. The sequence filter and the procedure to insert an elements into the filter are shown in Fig. 2.

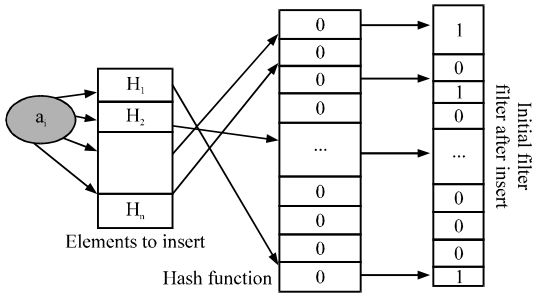

Fig. 2: Sequence filter

PROCEDURES OF FILTER BASED ADDRESSING PROTOCOL

Network initialization: In the network initialization procedure deals with the auto configuration of the initial set of nodes. In this initialization phase, there are two kinds of initialization in the networks. Which are called one is abrupt initialization and another one is gradual initialization. The joining nodes arrive one after the other with a long interval in between partitions. This is called gradual initialization; abrupt initialization is occurred when all the nodes arrive at the same time. The hello message is used by node to advertise its current association status and partition identifiers (Vaidya, 2002). The AREQ message is used to advertise that a previously available address is now allocated. Each AREQ has an identifiers numbers. All initiator nodes have chosen a unique address after the initialization phase of FAP, due to the random address choice and the validate using AREQ messages with identifier numbers. Additionally, every node knows all currently allocated addresses with a high probability. Consequently, each node also creates an address filter containing all the allocated addresses (Fazio *et al*., 2006).

In FAP, a node trying to join the network listens to the medium for a period TL. It starts the network, acting as the initiator node if the node does not receive a hello message within the particular period of time. An initiator node may start the network single or with other initiator nodes in the network. Otherwise, if the node received hello message, then it cause address collisions in the network. Already exists and the nodes act as a joining node. This triggers much partition merging procedure simultaneously (Fig. 3).

Node ingress and network merging events: After the initialization each node starts broadcasting periodic hello messages containing its address filter signature. Up on the reception of a hello, neighbours evaluate whether the signature in the message is the same as its own signature to detect the merging events. If the nodes listen to a hello,

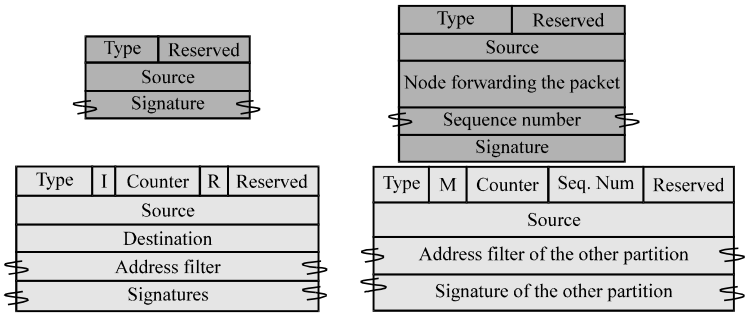

Fig. 3: Messages of FAP for initialization, joining node and partition merging procedure

there is an at least one node with an address filter and the network already exist hence the node knows that it is a joining node instead of an initiator node. The joining node then asked for the source of the first listened of hello message to send the address filter of the later using the Address Filter (AF) message (Broder and Mitzenmacher, 2004). All the address filter signatures acceptable by the node sending a message are placed in the field called signatures in AF message.

Partition and merging of events: Merging events are also detected based on hello and address filter messages nodes in different of partitions chose their address based only on the set of addresses of their partitions. The update of the filter signature after a node ingress or partition merging follows rules and requires the filed signature in the Address Filter (AF). If the signature on the hello different of their current filter signature but equal to some stored signature, the nodes will not consider that the neighbour is on another partition.

Node departure: The address of the departure node should become available for the other nodes when it leaves. The departing node floods the network with a notification to remove its address from the address filter, then that node should be shut down immediately (Fazio *et al*., 2006; Kim *et al*., 2007). The address remains allocated in the filters which can make the available addresses when the departing node does not notify the network. This can be identified in the address filter by the fraction of bits set to 1 in the Bloom and in the sequence filter and by the fraction of counters greater than one in the counter bloom filter. In the first case, the joining nodes do not identify that their addresses are the same because the messages of the other node seems to the first node like a retransmission of its own messages (Zhou *et al*., 2003; Broder and Mitzenmacher, 2004). In the second case, the partitioning and merging procedure is not started because the signatures of the hellos are the same for both partitions and consequently the merged network would have a collision for each of its addresses.

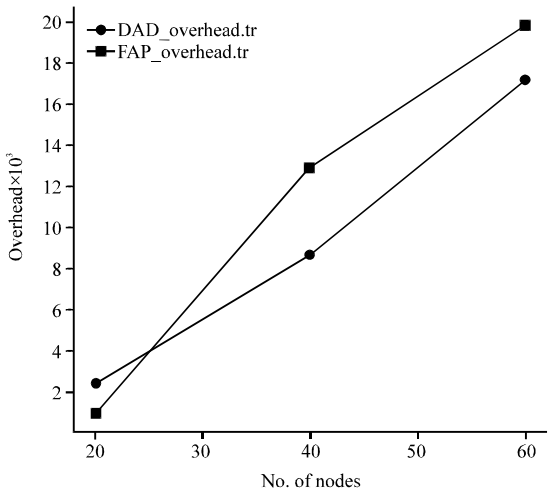

Fig. 4: Number of nodes vs. overhead

SIMULATION RESULTS

We implemented FAP in the network simulator-2 and evaluated it considering the shadowing model for radio propagation and the NS-2 IEEE 802.11 Model for the medium access control. We first analyse the impact of one node joining the network. We consider a rectangular space with node distributed in the simulation area. We measure the control load after the last node joins the network and required delay to obtain an addresses, in these results, we observed that our proposal. In abrupt network initialization, we evaluated the impact of the size of network, the density of the network and the number of transmissions of flooding messages, assuming that nodes are distributed in simulation area.

Figure 4 shows comparison between numbers of nodes increases the overhead of the DAD and the FAP. Figure 5 shows comparison between numbers of nodes increases the delay of the DAD and the FAP. Figure 6 shows comparison between number of partitions and the overhead DAD and the FAP.

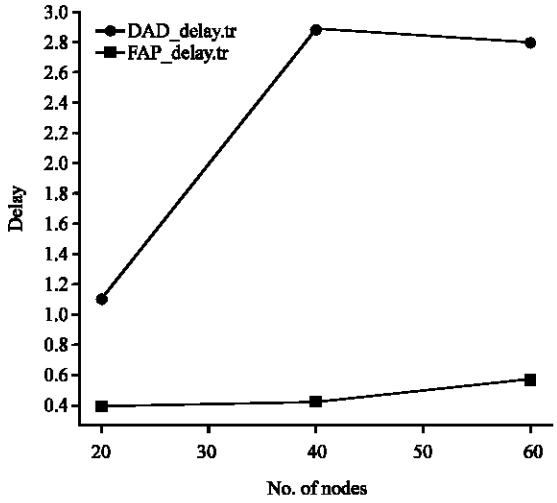

Fig. 5: Number of nodes vs. delay

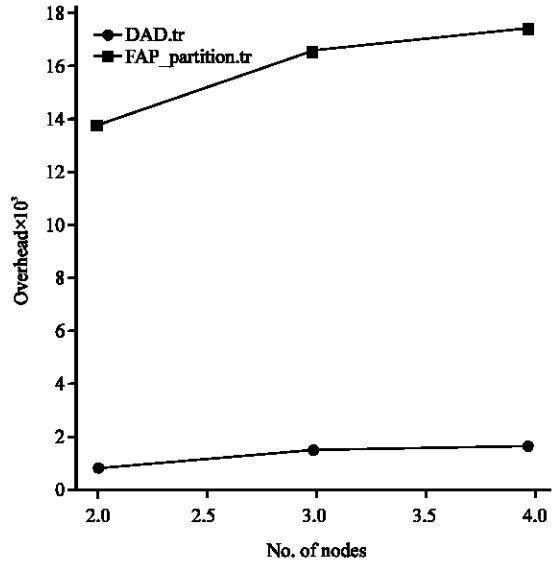

Fig. 6: Number of partitions vs. overhead

CONCLUSION

The proposed system address collisions are avoided, control load is decreased and decrease the address allocation delay by using address filters. The FAP and sequence filter methods avoids the address collision in partition merge event. The joining and leaving of the nodes can be handled by FAP. The proposed system reduces the control load on the network. It provides smaller delays in the partition merging events and node joining event compared to the existing work. This is achieved because FAP and sequence filter is able to detect all merging events and also FAP is robust to message losses. The initialization procedure of FAP is simple and efficient. The proposed system contributes redundancy avoiding technique by reducing control load.

RECOMMENDATIONS

The FAP process may be improved in future by adding other techniques and other parameter to be considered to enhance the proposed approach to provide better results in delay and reduction of the control load.

REFERENCES

Broder, A. and M. Mitzenmacher, 2004. Network applications of bloom filters: A survey. Internet Mathemat., 1: 485-509.

Cunha, D.O., O.C.M.B. Duarte and G. Pujolle, 2008. A cooperation aware routing scheme for fast varying fading wireless channels. IEEE Commun. Lett., 12: 794-796.

Fan, L., P. Cao, J. Almeida and A.Z. Broder, 2000. Summary cache: A scalable Wide-area web cache sharing protocol. IEEE/ACM Trans. Network., 8: 281-293.

Fazio, M., M. Villari and A. Puliafito, 2006. IP address autoconfiguration in ad hoc networks: Design, implementation and measurements. Comput. Networks, 50: 898-920.

Fernandes, N.C., M.D.D. Moreira and O.C.M.B. Duarte, 2009. An efficient filter-based addressing protocol for autoconfiguration of mobile ad hoc networks. Proceedings of the IEEE INFOCOM, April 19-25, 2009, Rio de Janeiro, pp: 2464-2472.

Fernandes, N.C., M.D.D. Moreira and O.C.M.B. Duarte, 2013. An efficient and robust addressing protocol for node autoconfiguration in Ad hoc networks. IEEE/ACM Trans. Network., 21: 845-856.

Kim, H., S.C. Kim, M. Yu, J.K. Song and P. Mah, 2007. DAP: Dynamic address assignment protocol in mobile Ad-hoc networks. Proceedings of the IEEE International Symposium on Consumer Electronics, June 20-23, 2007, Irving, TX., pp: 1-6.

Moreira, M.D.D., R.P. Laufer, P.B. Velloso and O.C.M.B. Duarte, 2012. Capacity and robustness tradeoffs in bloom filters for distributed applications. IEEE Trans. Parallel Distrib. Syst., 23: 2219-2230.

Thomson, S. and T. Narten, 1998. IPv6 stateless address auto configuration. RFC 2462, 1998. https://www.ietf.org/rfc/rfc2462.txt.

Vaidya, N.H., 2002. Weak duplicate address detection in mobile Ad hoc networks. Proceedings of the 3rd ACM International Symposium on Mobile Ad hoc Networking and Computing, Lausanne, Switzerland, June 9-11, 2002, ACM, New York, USA., pp: 206-216.

Zhou, H., L.M. Ni and M.W. Mutka, 2003. Prophet address allocation for large scale MANETs. Proceedings of the Annual Joint Conference of the IEEE Computer and Communications, IEEE Societies Volume 2, March 30-April 3, 2003, San Francisco, CA., pp: 1304-1311.