IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 1 Issue 2, April 2014.
www.ijiset.com
ISSN 2348 - 7968

DISTRIBUTED AND SELF MANAGED ADDRESSING PROTOCOL FOR DYNAMIC AD HOC NETWORKS

V. Tamizhazhagan Dr. R. Saminathan L.Sathiyaseelan
Department of Computer Science & Engineering, Annamalai University
Annamalainagar – 608 002, Tamil Nadu, India.

ABSTRACT

MANET is used for many distributed network, the lack of a centralized administration makes these networks attractive for several distributed applications, such as sensing, Internet access to deprived communities, and disaster recovering. Mobility feature of the Ad hoc Network produce many problems in the the network, due to this feature ad hoc network does not maintain any infrastructure. It also affects address assignment of the nodes in network ,that is node's address configuration . As other wireless networks, ad hoc nodes also need a unique network address to enable multihop routing and full connectivity. Address assignment in ad hoc networks, is even more challenging issue because of the self-organized nature of these environments Some times it leads to node's address collision in the network. To solve this problem many protocols proposed. It increases the control load of the network. Another important issue is frequency partition in the network due to fading channels. Proposed system gives the solutions to this problem, This 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. The proposed system contributes redundancy avoiding technique by reducing control load.

Keywords – Mobile Ad Hoc Network, Addressing Protocol, FAP, DAD.

1. INTRODUCTION

A Mobile Ad-Hoc Network (MANET) is a self-configuring network of mobile devices connected by wireless links. MANETs are specific network configurations that appear in the context of ubiquitous computing and proliferation of portable computing devices. It is a kind of wireless ad-hoc network, and is a self-configuring[9] network of mobile routers connected by wireless links[3] .The topology of mobile ad-hoc networks is arbitrary. In MANET the routers are free to move randomly and the organize themselves arbitrarily and unpredictably. Many existing works in the address assignment, has the overhead and it does not gives the proper solution to the network partition merge. The best filter for FAP depends on network characteristics such as the estimated number of nodes in the network and the number of available addresses. It also depends on the false-positive and false-negative rates of the filter. Bloom filters do not present a false negative, which means that a membership test of an element that was inserted into the filter is always positive. 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, 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, the proposed system uses the filter signature for partition merge and effective node's address configuration. Actually, when using random numbers to identify the partition instead of hash of the filter, the identifier does not change with the set of assigned addresses. Therefore, filter signatures improves the Collision of node's address is the main problem during the address allocation of the node. While allocating address to the node it should be unique to that node it should not collide with other node's address of the node without collision requires many control operations, that increases control load of the network. Another problem is partition merge, caused by node mobility, fading channel and nodes joining and leaving the network, can disrupt the distributed Network control. Network initialization is another problem, because lack of server in the network addresses. This filter is present at every node to simplify frequent node joining events and reduce the control overhead required to solve address collisions inherent or easily detecting network merging events, in which address conflicts may occur. The Bloom filter which is based on hash functions and the Sequence filter proposed in this paper which compresses data based on the address sequence.

II. RELATED WORKS

A. Cooperation-aware routing scheme for fast varying fading wireless channels

In this paper to analyze cooperation-aware routing [1] for fading networks and show that greedy algorithms are not adequate. Then, we propose a Weighted Cooperation-Aware routing metric (WCA) ,which uses long term channel information to prioritize routes composed by stable links. The key idea is to find the route with the highest probability of presenting good conditions instead of finding the optimal route based on instantaneous link conditions. The analyses are conducted both on entirely cooperative networks and on hybrid networks, The results show that greedy cooperation-aware algorithms do not fully exploit cooperation on typical fading networks. Furthermore, the proposed weighted cooperation-aware metric allows the selection of more stable routes, which present higher end to-end success probabilities. The improvement obtained by the proposed metric is even more significant on hybrid networks, where there are fewer cooperation opportunities. Filter signature defines this Concept is taken from "A Cooperation-Aware Routing Scheme for Fast varying Fading a Wireless Channels" by O. Cunha, Otto Carlos M. B. Duarte, and Guy Pujolle.

B. A Self-organized mechanism for thwarting malicious access in ad hoc networks

In this paper, we propose 'A Controller-node-based Access- Control mechanism [2] for Ad hoc networks (ACACIA). ACACIA is a self-organized public-key management and monitoring system that dismisses any trusted central authority or fixed server. In CACIA, all nodes play an equal role and the proposed mechanisms guarantee high availability even if network membership and topology are highly dynamic. Our mechanism provides both authentication and access control that are suitable for ad hoc networks. ACACIA is based the delegation chain is used to control network access without a centralized administration. As a result, all users are responsible for allowing new users to join the network. Users that allow a malicious user to join are punished in order to keep the network secure. The controller nodes, introduced in this paper, manage certificates and also monitor and punish nodes. Each node in the network is controlled by a dynamic controller set composed of randomly chosen nodes. The random selection provides a distributed

ISSN 2348 - 7968

access control with a different controller set for each node. Indeed, every node belongs to controller sets of other nodes. Therefore, our scheme avoids nodes with special functions because all nodes have the same duties a certificating and monitoring nodes The controller set actions are threshold ruled to an action is taken only if the majority of the set agrees on this a Once ad hoc network membership is highly dynamic, our controller nodes adapt to each network context by changing ACACIA parameters according to the controller set is regenerated whenever a membership change affects this controller a set. Since the controllers are dynamically chosen and based on voting, they provide based autonomy and availability to ACACIA. As the controller sets monitor and punish nodes, ACACIA is safe against attacks and controls node access. The performed evaluations as show that ACACIA availability is up to 90.7% greater than the threshold cryptography-based proposals on network partitions. ACACIA is the concept is drawn from **"**A Self Organized Mechanism for the Warting Malicious Access in Ad Hoc Networks" by Natalia Castro Fernandes, Marcelo Duffles Donato Moreira, and Otto Carlos Muniz Bandeira Duarte.

C. Manetconf: Configuration of hosts in a mobile ad hoc network

A mobile ad hoc network (MANET) is a multi-hop wireless network capable of autonomous operation. The mobility of MANET nodes can lead to frequent and unpredictable topology changes. Most MANET literature assumes that network related information of a node (such as its IP address, net mask, etc.) is configured statically, prior to the node joining the MANET. However, not all nodes have IP addresses permanently assigned to them. In this paper, we first present a survey of possible solutions approaches, and discuss their limitations. Then, we present a distributed dynamic host configuration protocol[7] designed to configure nodes in a MANET. We show that the proposed protocol works correctly and does not have the limitations of earlier approaches. Finally, we evaluate the performance of the solution through simulation experiments, and conclude with a discussion of related security issues. This idea is picked from "Manetconf Configuration of Hosts in a Mobile Ad Hoc Network" by Sanket Nesargi, Ravi Prakash.

D. Distributed Detection of node replication attacks in sensor networks

The low-cost[5], off-the-shelf hardware components in unshielded sensor-network nodes leave them vulnerable to compromise. With little effort, an adversary may capture nodes, analyze and replicate them, and surreptitiously insert these replicas at strategic locations within the network. Such attacks may have severe consequences; they may allow the adversary to corrupt network data or even disconnect significant parts of the network. Previous node replication detection schemes depend primarily on centralized mechanisms with single points of failure, or on neighborhood voting protocols that fail to detect distributed replications. To address these fundamental limitations, we propose two new algorithms based on emergent properties, i.e., properties that arise only through the collective action of multiple nodes. Randomized Multicast distributes node location information to randomly-selected witnesses, exploiting the birthday paradox to detect replicated nodes, while Line-Selected Multicast uses the topology of the network to detect replication. Both algorithms provide globally-aware, distributed node-replica detection[8] and Line-Selected Multicast displays particularly strong performance characteristics. We show that emergent algorithms represent a promising new approach to sensor network security; moreover, our results naturally extend to other classes of networks in which nodes

can be captured, replicated and re-inserted by an adversary. This idea is taken from "Distributed Detection of Node Replication Attacks in Sensor Networks" by Bryan Parno Adrian Perrig and Virgil Gligor.

E. Prophet Address allocation for large scale manets

A mobile device in a manet must be assigned a free ip address before it may participate in unicast communication. This is a fundamental and difficult problem in the practical use of any manet. several solutions have been proposed. A new IP address allocation algorithm, namely prophet allocation, is proposed in the paper. The proposed scheme may be applied to large scale MANET with low complexity low communication overhead even address distribution and low latency, both theoretical analysis and simulation experiments are conducted. The proposed prophet allocation[10] is able to solve the problem of network partition and merger efficiently. This idea is taken from "prophet address allocation for large scale manets" by hongbo zhou and lionel m. ni and matt w. mutka.

F. Capacity and Robustness tradeoffs in bloom filters distributed applications

The Bloom filter is a space-efficient data structure often employed in distributed applications to save bandwidth during data exchange. These savings however come at the cost of errors in the shared data, which are usually assumed low enough to disrupt the application. We argue that this assumption does not hold in a more hostile environment, such as the Internet, where attackers can send a carefully crafted Bloom filter in order to break the application. In this paper, we propose the concatenated Bloom filter (CBF) [4] , an robust Bloom filter that prevents the attacker from interfering on the shared information, protecting the application data while still providing space efficiency. Instead of using a single large filter, the CBF concatenates small sub filters to improve both the filter robustness and capacity. We propose three CBF variants and provide analytical results that show the efficiency of the CBF for different scenarios. We also evaluate the performance of our filter in an IP trace back application and simulation results confirm the effectiveness of the proposed mechanism in the face of attackers. This idea is taken from "Capacity and Robustness Tradeoffs in Bloom Filters for Distributed Applications" by Marcelo Duffles Donato Moreira, Rafael Pinaud Laufer.

G. An Address Auto configuration Protocol For Ipv6 Hosts in a Mobile Ad Hoc Network

A simple solution for address autoconfiguration in ad hoc networks[6] has been proposed by Perkins et al. In Addresses are randomly chosen on net-work 169.254/16 in case of IPv4, or on prefix MANET-PREFIX in case of IPv6. A Manet node performing autoconfiguration chooses two addresses: a temporary address and the actual address to use. The former is used only once in the uniqueness check to minimize the possibility for it to be non-unique. The uniqueness check is based on sending an Address Request AREQ) and expecting an Address Reply (AREP) back in case the address is not unique. If no AREP is received, the uniqueness check is passed. For IPv4, the Address Request/Reply messages are ICMP (Internet Control Message Protocol) packets. For IPv6, the AREQ is a modified Neighbor Solicitation and the AREP is a modified Neighbor Advertisement, as specified in the Neighbor Discovery Protocol The autoconfiguration mechanism is designed to be independent of the routing protocol. Duplicate address detection is performed only once by each node. Therefore this approach does not guarantee address uniqueness in partitioned networks that merge later on. If a network is disconnected, the DAD process has to be performed again when the network

ISSN 2348 - 7968

partition heals. The draft does not specify any method for detecting when the network partition heals, nor any procedure by which such detection would cause new attempts at DAD.

III. NETWORK INITIALIZATION

There is two kinds of initializations in the networks. **Abrupt initialization**: joining of the nodes at the same time is called abrupt Initialization. **Gradual initialization**: joining of the node after some interval and is considered as the gradual initialization. Initially a node waits to join or try to join in the network for that it listens to the medium for a particular period (Tl) .If the node does not receive the hello message with in the listening period it will act as the initiator node .The Initiator node starts the network alone or with other initiator nodes. Otherwise it acts as the joining node with the network already exist. Hello messages used in the initialization for a node to advertise its current association status and partition identifier, which is signature of the filter of each node it contains.AREQ message is used to indicate that previously available address is now allocated. Each AREQ has an identifier number, which is used to differentiate AREQ messages generated by different nodes, but with the same address. An initiator randomly chooses an address, and it also creates an empty filter and starts the network initialization phase .After that the node floods the AREQ messages Nf times in the network. If there is other initator node in the network that also send the AREQ floods messages Nf times to increase the reception of the AREQ messages by all the nodes present in the network. It is for a node randomly choose the address. After particular time of waiting period the node does not waits for the AREQ message .The node leaves the initialization phase ,insert the address in its filter ,the address received by the AREQ messages from each node. And then the node starts to send the Hello messages with filter signature which is the hash value of the address filter. The signature place the important role in the partition events. If the initiator node receives the same address with the different identifier. The node finds there is the address collision. In this situation the node wait for particular time and choose another available address it is to be continued until each node allocates the unique address to it During the wait period it receives the many AREQ messages and check for the address collision Therefore, after, the node knows a more complete list of allocated address, which decreases the probability of choosing a used address. Hence, the period decreases the probability of collisions and, consequently reduces network control load.

END OF NETWORK INITIALIZATION

After the initialization phase of FAP, all initiator nodes have chosen a unique address due to the random address choice and the validation using AREQ messages with identifier numbers. If the initiator node receives any AREQ with the same address that it has chosen, but with a different identifier number, which means that there is an address collision, the node waits for a period and then chooses another available address and sends another AREQ.

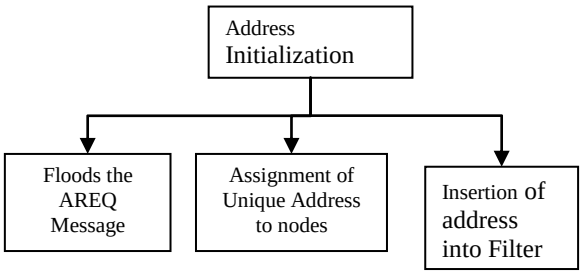

Fig. 1 Network Intialization Process

The Address initialization is divided into three phase (i) Floods the AREQ Messages (ii)Assignment of unique Address to Nodes(iii)Insertion of address into Filters.The initiator nodes have chosen a unique address due to the random address. The node finds there is the

ISSN 2348 - 7968

address collision, in this situation the node wait for particular time and choose another available address it is to be continued until each node allocates the Assignment of unique address to nodes. After, the node knows a complete list of allocated address, then Insertion of address is been inserted into the filter is shown in Fig.1.

IV. JOINING NODE OR NODE INGRESS

During the node joining the host node checks the messages whether for the joining procedure or for partition procedure. After the initialization the node ask for send the Hello message and after the Hello message send by the host node ,the node sends the Address Filter message AF. Now the host node checks for the I bit is set to be 1 or 0, it is indicate whether the messages for joining procedure or the partion procedure. If , the message came from a joining node. Then, the host node answers the request with another AF with bit set to1, indicating that the AF is an answer to a previous filter request. When the joining node receives the AF reply message, it stores the address filter, chooses a random available address, and floods the network with an AREQ to allocate the new address. When the other nodes receive the AREQ, they insert the new address in their filters and update their filter signatures with the hash of the updated filter.

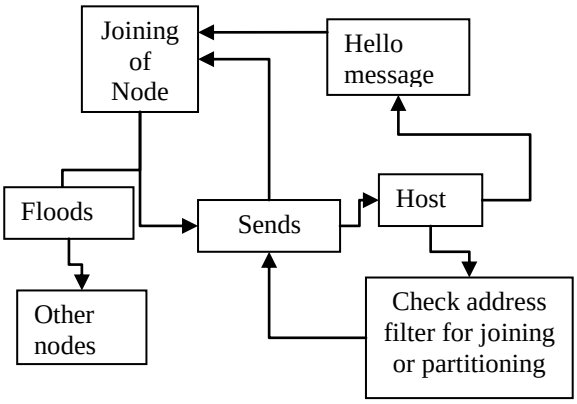

Fig. 2 Node Ingress Process

Fig.2 Shows the node joining Address and the Host Node checks the joining node procedure,it sends message to the Address filter then the Hello message is sends to joining node through the Host node. Then the joining node it checks the address filter, chooses a random available address, and floods the network with an AREQ to allocate the new address.

V.PARTITION DETECTION AND MERGE

Merging events are also detected based on Hello and AF messages nodes in different partitions choose their address based only on the set of addresses of their partition. Hence, nodes in different partitions can select the same address, which may cause collisions after the partitions merged. If Address filter received from the node, in that I bit indicates 0 that is partition to be done. The filter signature of the different partition differ in the signature, from that it is to identified that node contain the different group of address. In this both node distribute filter of its two partitions,

Each node on the lowest-priority partition must check whether its address is on the other partition filter to detect collisions. If there is a collision, the node randomly chooses an available address in both filters and floods the network with an AREQ to allocate the new address. If the node receives an AREQwith the same address that it has chosen, but with a different sequence number, it chooses another address because another node has also chosen the same address. Finally, all the nodes merge the other partition filter with its own filter, insert the addresses received in the AREQs into the new filter, and update the filter signature.

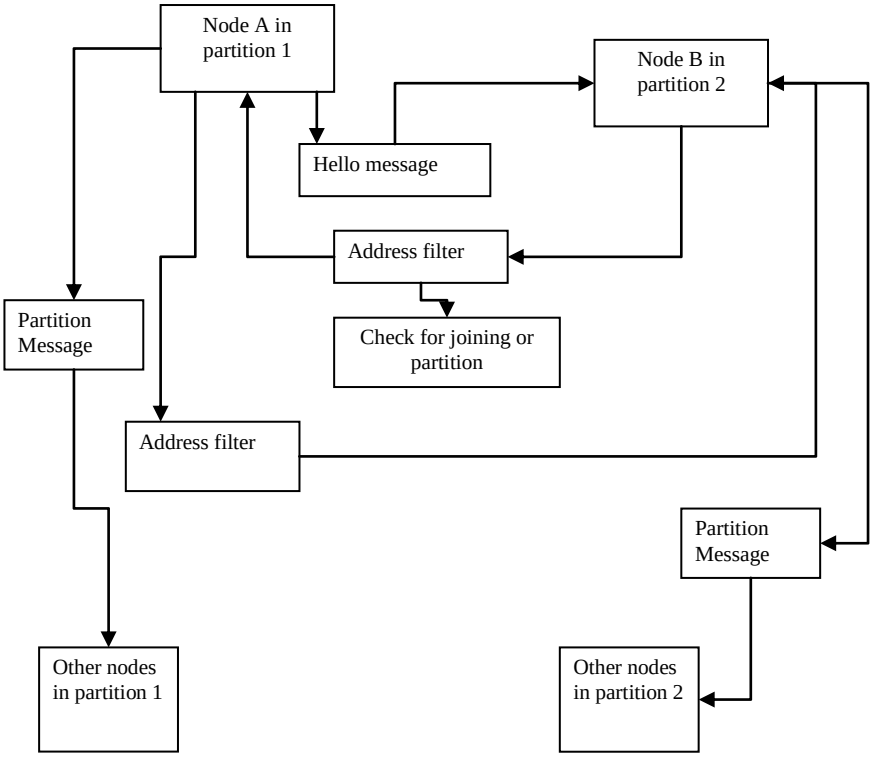

Fig. 3 Partition Merge of Network

Fig.3 represents how the partition Merge of network is shown here. Node A in Partition 1 sends hello message to Node B in Partition 2 then the address filter it checks the message and again sends to Node A in Partition 1. Node A in Partition 1 sends to the address filter then it sends back to Node B in Partition 2 and finally the Node gets Partioned and sends to other Node in Partition 1 and Partition 2.

VI. NODE DEPARTURE

When node leaves the network and the it floods the notification message in the network to remove the address from the address filter to perform the proper shutdown. The departure of the node is indicated by the fraction of the filter. So each time every node verifies that its filter fraction bit to check or to know the departure of node. Therefore, every node verifies this fraction in their address filters every time the filter is updated. If this fraction reaches a threshold that indicates that the filter is full or almost full, all the nodes reset their address filters and returns to the network initialization.

VII. PERFORMANCE EVALUATION

Performance of the protocol is evaluated using Network Simulator [11]proposed protocol is compared with existing protocol.

Control Overhead

- It denotes the number of messages involved in address initialization and comparison and allocation process

Delay

- Time taken by each node for the joining node procedure and on network partition merging events

The impact of the network size, the network density, and the number of transmissions of flooding messages in abrupt network initialization is evaluated. Proposed protocol suffers a greater

influence on the control load than the existing protocol. We first analyze the impact of one node joining the network. A rectangular space with nodes distributed in grid is considered. The control load after the last node joins the network and the required delay to obtain an address is measured. Simulation results reveal that proposed protocol resolves all the address collisions and also reduces the control traffic when compared to existing protocol.

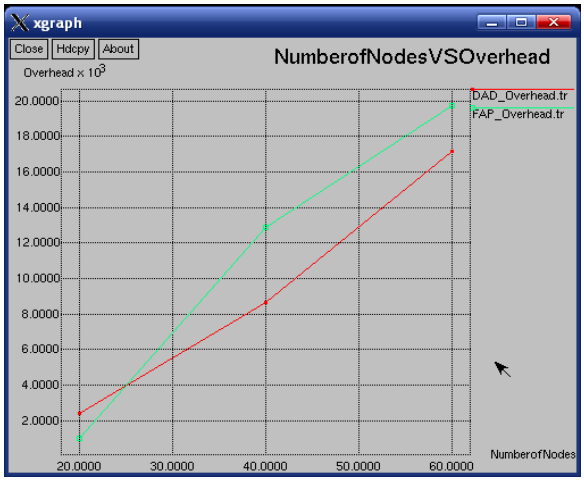

Fig.4 Number of nodes versus Overhead

In Fig.4 This graph shown comparison between the Number of nodes versus overhead of the DAD and the FAP. The number of messages involved in address initialization and comparison and allocation process.FAP contains more messages when compared to DAD.FAP overhead DAD.

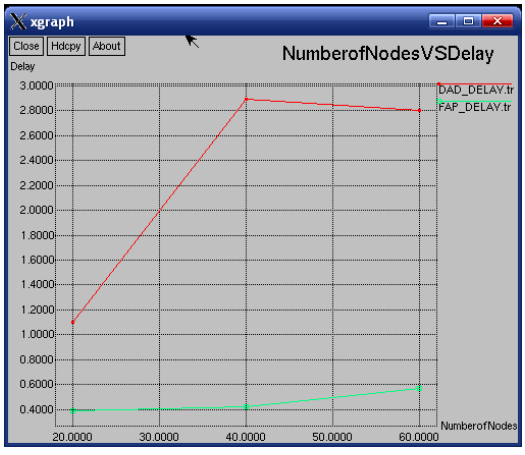

Fig. 5 Number of Nodes versus Delay

In Fig.5 This graph shown comparison between Number of nodes vs Delay between the DAD and the FAP. The Time taken by each node for the joining node procedure and on network partition merging events .While the Mobility Speed of nodes increases in the network the routing process taken place in the network. Number of nodes of DAD increases the rate of Delay when compared to FAP.

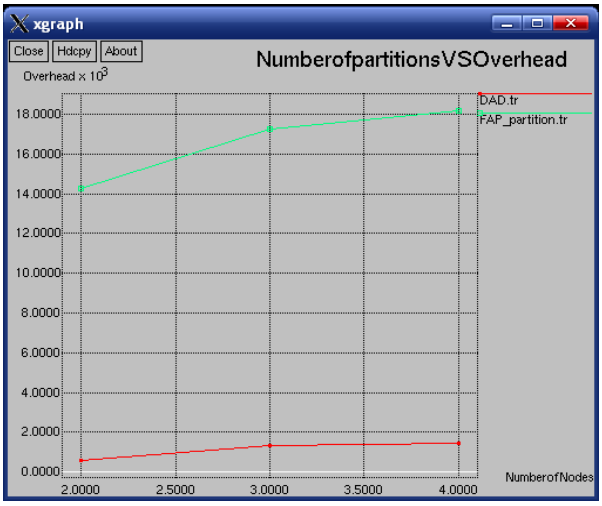

Fig. 6 Number of Partitions versus Overhead

Fig. 6 This graph shown comparison between the Number of partitions versus overhead of DAD and the FAP.FAP increases when compared to DAD, FAP Partitions the number of nodes versus overhead of the DAD .The speed of the communicating nodes increases in the network the delay to reach the destination increases in the network. FAP reaches the overhead.

VIII. CONCLUSION

In this paper the proposed system uses the key idea is to use address filters to avoid collisions, reduce the control load, and decrease the address allocation delay. Proposed FAP avoid the collision of the address in partition merge event. It handles the join and leaves of the nodes properly. The proposed system reduces the control load . FAP provides the smaller delays in the partition merging events and node joining event. Compared to the existing work. This is achieved because FAP is able to detect all merging events and also because FAP is robust to message

losses. FAP initialization Procedure is simple and efficient. The proposed system contributes redundancy avoiding technique by reducing control load.

REFERENCES

[1] D. O.Cunha,O.C.M.B. Duarte,G. Pujolle,"A cooperation aware routing scheme for fast varying fading wireless channels,"IEEE Commun. Lett.,vol.12, no.10, pp.794–796, 2008.

[2] N. C. Fernandes,M.D.Moreira, and O. C. M. B. Duarte, "A self-organized mechanism for thwarting malicious access in ad hoc networks," in Proc. 29th IEEE INFOCOM Miniconf., San Diego, CA, Apr. 2010, pp. 1–5.

[3] Kemal Akkaya , Mohamed Younis. "A survey on routing protocols for wireless sensor networks".

[4] Marcelo Duffles Donato Moreira, Rafael Pinaud Laufer, "Capacity and Robustness Tradeoffs in Bloom Filters for Distributed Applications".

[5] Miguel Elias M. Campista, Igor M. Moraes, Pedro Miguel Esposito, Aurelio Amodei Jr., Daniel de O.Cunha "The Ad Hoc Return Channel:A Low-Cost Solution for Brazilian Interactive Digital TV".

[6] Z. Fan and S. Subramani, "An address autoconfiguration protocol forIPv6 hosts in a mobile ad hoc network," Comput. Commun., vol. 28,no. 4, pp. 339–350, Mar. 2005.

[7] S. Nesargi and R. Prakash, "MANETconf: Configuration of hosts in a mobile ad hoc network," in Proc. 21st Annu. IEEE INFOCOM, Jun. 2002, vol. 2, pp. 1059–1068.

[8] B. Parno, A. Perrig, and V. Gligor, "Distributed detection of node replication attacks in sensor networks," in Proc. IEEE Symp. Security Privacy, May 2005, pp. 49–63.

[9] Srdjan Capkun, Student Member, Levente Buttya´.n "Self-Organized Public-Key Management for Mobile Ad Hoc Networks".

[10] H. Zhou, L. Ni, and M. Mutka, "Prophet address allocation for large scale MANETs," in Proc. 22nd Annu. IEEE INFOCOM, Mar. 2003, vol. 2, pp.1304–11.

[11] Teerawat Issariyakul, Ekram Hossain, "Introduction to Network Simulator NS2", Springer, 2009.