Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 4, April 2014, pg.1221 – 1226

RESEARCH ARTICLE

ENSURING THE NODE AUTOCONFIGURATION AND NODE PREVENTION FROM INTRUDERS USING SFAP

Udaya.R[1]

PG Student, Department of Computer Science and Engineering,
Francis Xavier Engineering College, Tamilnadu, India
Udaya.anur@gmail.com

Jenifer.P[2]

Assistant Professor, Department of Computer Science and Engineering,
Francis Xavier Engineering College, Tamilnadu, India

Abstract— In ad hoc networks the address assignment is a key challenge due to the lack of infrastructure. An ad hoc network creates frequent network partitions caused by mobility of nodes, fading channels and the nodes joining and leaving the network. These network partition associates the various address collisions. The lack of centralized administration make these network attractive to several distributed applications such as sensing and disaster recovering, So it needs an addressing protocol that configures the mobile ad hoc nodes and avoids the unauthorized access to the networks. This paper presents a Secure-Filter addressing protocol (SFAP) autoconfigures the mobile ad hoc nodes based on a distributed database stored in filters. SFAP resolves address collisions of network partitions by exchanging the hash of the filter among neighbors. Secure-Filter addressing protocols with partition detection identify the partition and advertise periodically about the different set of nodes.SFAP implements the security by filtering the unauthorized access using the Dynamic Hole Detection and healing method. The SFAP is to achieve the robust node autoconfiguration that addresses the network partitions to resolve all the address collisions, controls the message losses and ensures the DHEAL security by preventing the transmission routes between the ad hoc nodes.

Keywords— Ad hoc networks, Secure-Filter Addressing Protocols, Partition Detection, Dynamic Hole detection, Healing

I. INTRODUCTION

MOBILE ad hoc networks do not require any previous infrastructure. The lack of a centralized administration in ad hoc makes these networks attractive for several distributed applications, such as remote sensing, Internet access, and disaster recovering. A crucial unaddressed issue of ad hoc networks is the frequent network partitions. The network partitions, caused by node mobility, network fading, and nodes joining and leaving the network, can disrupt the overall distributed network control. Network Initialization is a challenging issue due to lack of servers in the ad hoc network.

As other wireless networks, ad hoc nodes also need a unique network address to enable the multihop routing and full connectivity. Address assignment in ad hoc networks, are more challenging due to the self-organized nature of these environments. Centralized mechanisms, such as Dynamic Host Configuration Protocol (DHCP) or Network Address Translation (NAT), conflict with the distributed nature of ad hoc net-works and do not address network partitioning and merging.

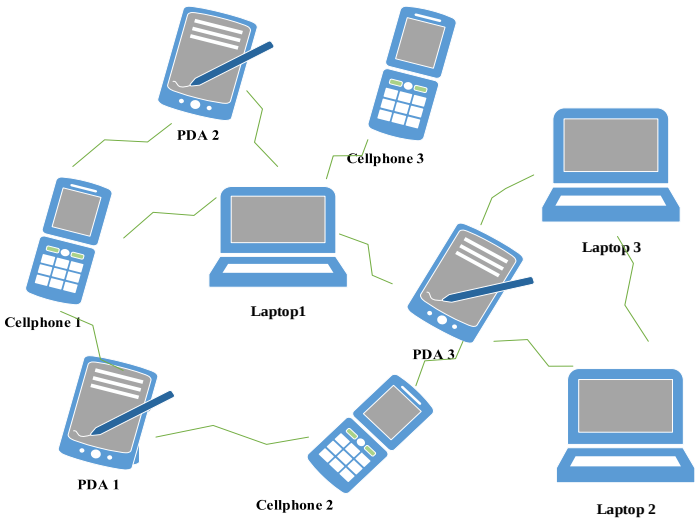

Fig. 1 Structure of Ad hoc Networks

Due to the lack of infrastructure, Addressing protocols require a distributed and self-managed mechanism to avoid address collision with fading channels, frequent network partitions and joining/leaving nodes in a dynamic network. There are no security schemes for preventing the network attackers. Duplicate address detection does not taken the network partitions in ad hoc networks.

The Secure-Filter addressing protocol configures mobile ad hoc nodes based on a distributed database stored in filters that reduces the control load, provides the optimal paths and robust to packet losses and network partitions. Active Duplicate address detection with partition detection (ADAD-PD) detects the address collisions during network partitions. Also the DHEAL(Dynamic Hole Detection and healing) protocol detects and heals the intruder holes in ad hoc networks. The simulation results shows that the SFAP decreases the drop parameter and increases the throughput by evaluation.

II. SFAP

The proposed Secure-Filter Addressing Protocol (SFAP) maintains a distributed database stored in filters containing the currently allocated addresses in a compact fashion. The combination of the Bloom filter and a proposed filter, called Sequence filter, to design a Secure-Filter protocol that assures both the univocal address configuration of the nodes joining the network and the detection of address collisions after merging network partitions. In SFAP every node can easily check whether an address is already assigned or not.

SFAP use the hash of this filter as a partition identifier, providing an easy detection of network partitions. The filters are used to store the allocated addresses without incurring in high storage overhead by exchanging the hash of the filters among neighbors.SFAP proposal is a robust addressing scheme because it guarantees that all the ad hoc nodes share the same allocated list and provides the optimal paths. ADAD with Partition Detection (ADAD-PD) uses partition identifiers, to distinguish the current partition from the others. The protocol with MANET conf is based on the knowledge of the allocated list, includes the allocated addresses, and the allocated Pending list. DHEAL (Dynamic Holes Detection and Healing), ensures the security by detecting and healing the intruder holes in ad hoc networks.

III. SYSTEM ANALYSIS AND DESIGN

In ad hoc networks the address assignment is a key challenge. Autonomous addressing protocols require a distributed and self-managed mechanism to avoid address collisions in a dynamic ad hoc network with fading channels, frequent network partitions, and joining/leaving nodes due to the lack of infrastructure. The node mobility can disrupt the distributed network control. Network initialization is another issue because of the lack of servers in the ad hoc network. Ad hoc nodes also need a unique network address to enable routing in multihop and full connectivity. The distributed nature of ad hoc networks and do not address network security, partitioning and merging. It is hard to avoid duplicated addresses because a random choice of an address by each node would result in a high collision probability in ad hoc networks. Secure-Filter Addressing Protocol (SFAP) assures the univocal address configuration of the nodes joining the network and the detection of address collisions after merging partitions. SFAP resolves all the address collisions and also reduces the control traffic.

In the existing system the Dynamic Host Configuration Protocol (DHCP) or the Network Address Translation (NAT) mechanisms are used in the ad hoc networks. It conflict with the distributed nature of ad hoc networks and do not address network partitioning and merging. The bloom filters are distributed maintained by exchanging the hash of the filters among neighbors. This allows nodes to detect with small control overhead neighbors using different filters, which could cause address collisions. Hashing the MAC address similar to a random address choice and does not guarantee a collision-free address allocation. In Duplicate Address Detection (DAD) every joining node randomly chooses an address and floods the network with an Address Request message (AREQ) and Address Reply message (AREP).In the Dynamic Address assignment, a node

subdivides its available address set with a joining node. The address set reallocation and the detection of given address is not being used anymore can cause a high control load in the ad hoc network.

A. Drawbacks of existing system

- Node mobility with fading channels disrupts the distributed network.
- DHCP and NAT do not address the network partitioning and merging.
- The distributed filter exchange the hash among the neighbors allows the node to detect with small control overhead and cause address collisions.
- The addressing scheme does not guarantee all the nodes that share the same allocated list.
- Hashing the MAC address does not guarantee a collision-free address allocation.
- Duplicate Address Detection does not detect the address duplication during the network partition.
- The reallocation and detection of empty address sets can cause the high control load and storage capacity in the network.
- There is no specialized scheme for detecting the intruder attack in ad hoc networks.

To overcome the drawbacks of existing system SFAP protocol was introduced. The proposed Secure-Filter Addressing Protocol (SFAP) maintains a distributed database stored in filters containing the currently allocated addresses in a compact fashion. The combination of the Bloom filter and a proposed filter, called Sequence filter, to design a Secure-Filter protocol that assures both the univocal address configuration of the nodes joining the network and the detection of address collisions after merging network partitions. In SFAP every node can easily check whether an address is already assigned or not.

SFAP use the hash of this filter as a partition identifier, providing an easy detection of network partitions. The filters are used to store the allocated addresses without incurring in high storage overhead by exchanging the hash of the filters among neighbors. SFAP proposal is a robust addressing scheme because it guarantees that all the ad hoc nodes share the same allocated list and provides the optimal paths. ADAD with Partition Detection (ADAD-PD) uses partition identifiers, to distinguish the current partition from the others. The protocol with MANET conf is based on the knowledge of the allocated list, includes the allocated addresses, and the allocated Pending list. DHEAL (Dynamic Holes Detection and Healing), ensures the security by detecting and healing the intruder holes in ad hoc networks.

B. Advantages

- SFAP easily check whether an address is already assigned or not.
- SFAP achieves low communication overhead, low latency and resolves all address collisions even in network partition merging events.
- It controls the message losses.
- ADAD-PD detects the address duplication during the network partition..
- MANETconf improves the performance of network merging detection and address reallocation.
- DHEAL ensures the security by detecting and healing the intruder holes.

IV. SYSTEM IMPLEMENTATION

The overall system model is explained as follows, Addressing protocols require a distributed and self-managed mechanism to avoid address collision with fading channels, frequent network partitions and joining/leaving nodes in a dynamic network. There are no security schemes for preventing the network attackers. Duplicate address detection does not taken the network partitions in ad hoc networks.

The Secure-Filter addressing protocol configures mobile ad hoc nodes based on a distributed database stored in filters that reduces the control load, provides the optimal paths and robust to packet losses and network partitions. ADAD-PD detects the address collisions during network partitions. Also the DHEAL protocol detects and heals the intruder holes in ad hoc networks. The simulation results shows that the SFAP decreases the drop parameter and increases the throughput by evaluation.

The implementation is described as follows,

A. Creation of Autoconfiguration Nodes

In this module the user have to enter the required source node and destination node by specifying the ad hoc node number without the portfolio selection. The system will create some univocal autoconfiguration ad hoc nodes and the initialization of addressing protocols to configure the nodes with the network initialization.

B. SFAP Configures the Mobile Ad hoc Nodes

The initialized Secure-Filter Addressing protocol (SFAP) configures the mobile ad hoc nodes based on the distributed database stored in filter that reduces the control load, packet losses, duplicate address allocation and address collisions. Now every

node can easily check whether the address is already assigned or not. Partition identifier in the filter can detect the network partitions by sending the topology discover message to its neighbors.

C. Identification of Source and Destination Nodes by Sequence Filter

The Sequence filter stores and compacts addresses based on the sequence of addresses. This Filter is created by adding the first address of the address sequence in the ad hoc network. The filters identify all the nodes by exchanging the hash of the filters among neighbors using the topology discover message. Already configured SFAP discover the topology message between all the nodes even with the fading channel, network partition and joining/leaving nodes, so it guarantees all nodes share the same allocated list. This Filter identifies the source and destination node by the distributed address database stored in filters.

D. Filtering of Efficient Paths Using the ADAD-PD

In this module, filtering of efficient paths between the source and destination node is done using the Secure-filter addressing protocols and ADAD-PD. The SFAP configures the mobile ad hoc nodes by exchanging the topology discover message between the neighbors. The SFAP uses the sequence filter and concatenated bloom filter to maintain the distributed database, using the maintained database it resolves the partition/merging events, fading channels and with the help of ADAD-PD it resolves all the address collisions and duplicate address detection. Then by using the SFAP and DSR finds the two transparent optimal paths. The first optimal path is the selected transmission path. Incase of any path or network failure, the network will automatically choose the second optimal path.

E. Intruder Black Hole Attack between the Ad hoc Nodes

In this module, the intruder is entering in to the ad hoc nodes and creates the intruder black hole attack for the various malicious accesses in the network. The SFAP with ADAD-PD can easily identify the black holes by the hash exchange among the neighbors.

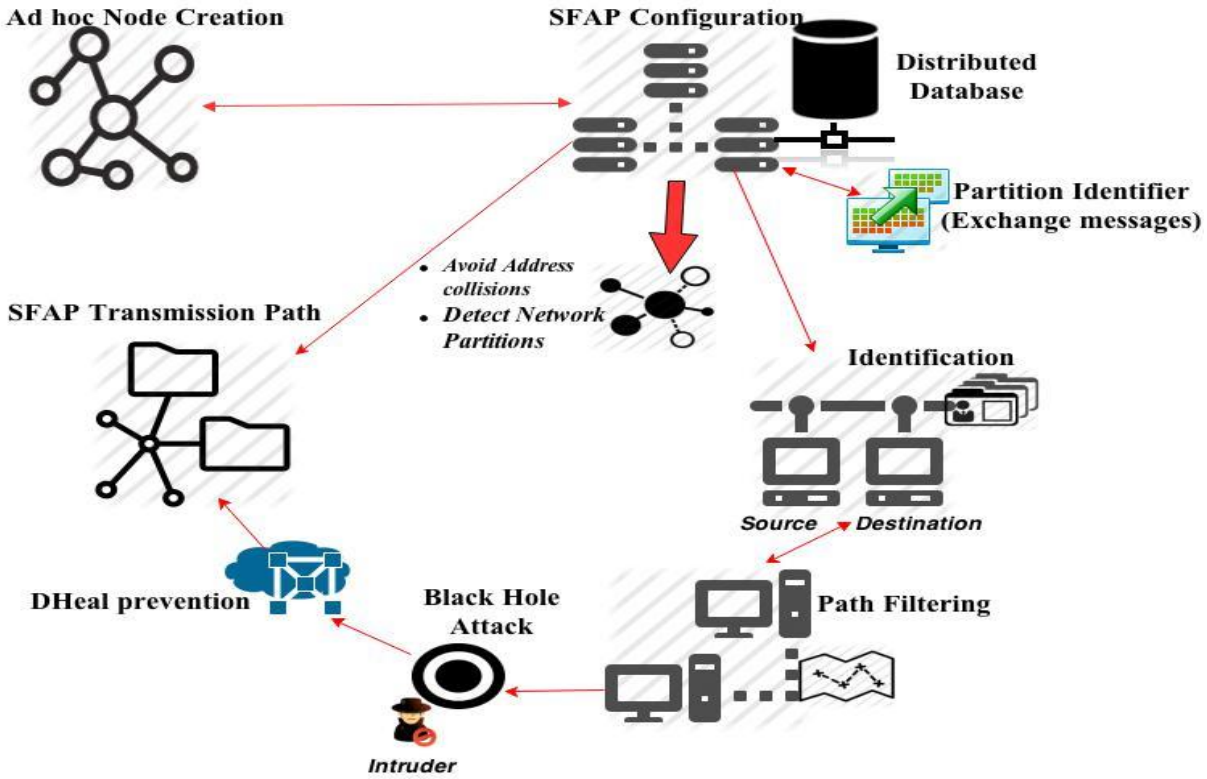

Fig. 2 System Architecture

F. DHEAL Prevention of Optimal Paths from the Intruder Black Hole

This module assures the network security by preventing the optimal paths provided by the Secure-Filter autoconfiguration protocols. The Comprehensive algorithm DHEAL (Dynamic Hole Detection and healing) detects the black hole attack in network and heals the hole. DHEAL with the help of DHD algorithm provide the two transparent optimal path for the effective transmission between the ad hoc nodes.

V. PERFORMANCE EVALUATION

The SFAP analyzed the efficient path in the ad hoc network by the ADAD-PD. Partition Identifier provide an accurate partition detection. In Fig. 3 SFAP reduces the various number of collisions between the ad hoc nodes. This also controls various message losses and reduces the delay in the network. The Graph Comparison show that the SFAP has better performance than DHCP and NAT.

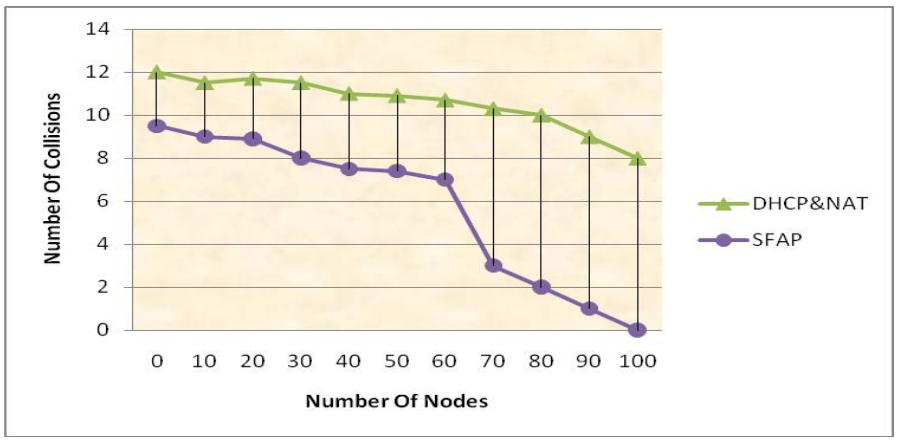

Fig. 3 Comparison of efficient path filtering

The proposed DHEAL fits well for dynamic ad hoc network with the fading channels, frequent network partitions and joining/leaving nodes. SFAP with DHEAL decreases the transmission drops by identifying and healing the intruder holes at the path boundary. In the Fig. 4 the normal Hole detection increases the drop in network transmission after the intruder attack. The DHEAL completely improves the performance by decreasing the transmission drop in the ad hoc network.

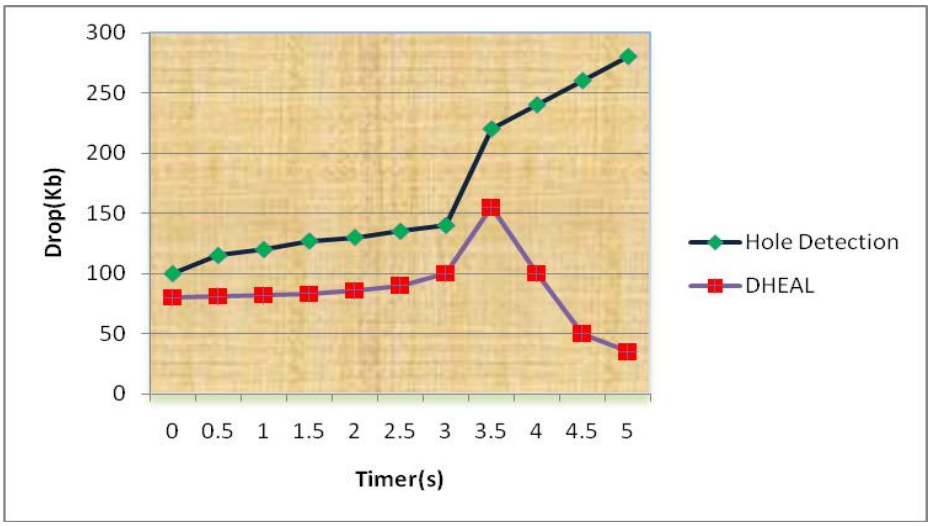

Fig. 4 Comparison of Intruder Prevention

VI. CONCLUSION AND FUTURE ENHANCEMENT

The proposed addressing protocol called Secure-Filter Addressing Protocol fits well for dynamic ad hoc networks with the ad hoc fading channels, frequent network partitions and joining/leaving nodes. The exchange of hash of filters among the neighboring nodes with the partition detection identifies the partition and merging events. This paper reduces the duplicate address, controls the message losses and resolves all the address collision with ADAD-PD. Also the SFAP achieves the optimal transparent path for the transmissions which reduces the control traffic between the ad hoc nodes. Finally the security is assured by preventing the transparent path from the intruder black hole with the presence of DHD and DHEAL. The simulation results show that the SFAP decreases the drop parameter and increases the throughput by evaluation. In the future work SFAP with Ricart-Agrawala algorithm improves the performance in ad hoc networks, Also DHEAL investigate the holes at the network boundary with the help of coverage control.

REFERENCES

1. Natalia Castro Fernandes,Marcelo Duffles Donato Moreira and Otto carlos Muniz Bandeira Duarte (2013), 'An Efficient and Robust Addressing Protocol for Node Autoconfiguration in Ad hoc Networks', IEEE/ACM Transactions on Networking, Vol.21,No.3,pp.845-856.
2. A. Broder and M. Mitzenmacher, "Network applications of Bloom filters:A survey," *Internet Math.*, vol. 1, pp. 485–509, 2002
3. Dongkyun Kim, Hong-Jong Jeong, Toh.C.K, and Sutaek Oh (2009), 'Passive Duplicate Address-Detection Schemes For On-Demand Routing Protocols In Mobile Ad Hoc Networks', IEEE Transactions on Vehicular Technology, Vol. 58, No. 7, pp. 3558-3568.
4. Z. Fan and S. Subramani, "An address autoconfiguration protocol for IPv6 hosts in a mobile ad hoc network," *Comput. Commun.*, vol. 28, no. 4, pp. 339–350, Mar. 2005.
5. M. Fazio, M. Villari, and A. Puliafito, "IP address autoconfiguration in ad hoc networks: Design, implementation and measurements," *Comput. Netw.*, vol. 50, no. 7, pp. 898–920, 2006.
6. N. C. Fernandes,M.D.Moreira, and O. C. M. B. Duarte, "Aself-organized mechanism for thwarting malicious access in ad hoc networks," in *Proc. 29th IEEE INFOCOM Miniconf.*, San Diego, CA, Apr. 2010, pp. 1–5.
7. N. C. Fernandes,M.D.Moreira, and O. C. M. B. Duarte, "An efficient filter-based addressing protocol for autoconfiguration of mobile ad hoc networks," in *Proc. 28th IEEE INFOCOM*, Rio de Janeiro, Brazil, Apr.2009, pp. 2464–2472.
8. Jiming Chen, Junkun Li, and Ten H. Lai (2013), 'Energy-Efficient Intrusion Detection With A Barrier Of Probabilistic Sensors: Global and Local', IEEE Transactions on Wireless Communications, Vol. 12, No. 9, pp. 4742-4755.
9. H. Kim, S. C. Kim, M. Yu, J. K. Song, and P.Mah, "DAP: Dynamic address assignment protocol in mobile ad-hoc networks," in *Proc. IEEE ISCE*, Jun. 2007, pp. 1–6.
10. M. D. D. Moreira, R. P. Laufer, P. B. Velloso, and O. C.M. B. Duarte,"Capacity and robustness tradeoffs in Bloom filters for distributed applications,"*IEEE Trans. Parallel Distrib. Syst.*, vol. 23, no. 12, pp.2219–2230, Dec. 2012.
11. 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.
12. 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.
13. M. R. Senouci, A. Mellouk, and K.Assnoune, "Localized Movement-Assisted Sensor Deployment Algorithm for Hole Detection and Healing," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 5, pp. 1267–1277, 2014.
14. N. H. Vaidya, "Weak duplicate address detection in mobile ad hoc networks,"in *Proc. 3rd ACM MobiHoc*, 2002, pp. 206–216.
15. 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. 1304–1311.

