ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 6, June 2016

A Detailed Study on Fundamental Characteristics and Functional Operations of Manet

[1] Narayanasamy Rajendran,[2] Dr. E.R.Naganathan
[1] Research scholar,[1][2] Dept. of Computer Science Engineering
[1] SCSVMV University Kancheepuram, Chennai, India, [2] Hindustan University, Padur, India

***Abstract*— A MANET is a collection of independent mobile nodes that communicates with each other through wireless medium. The MANET architecture is dynamic in nature, the nodes act as transmitter and receiver. The vehicular ad hoc network topology changes frequently due to the dynamic nature of the autonomous mobile nodes. MANET is exposed to multiple kinds of attacks due to its fundamental characteristics like no security mechanism, dynamic topology, no central control devices and open wireless medium. The impact of attacks affects the security, quality of service and the performance of MANET. MANET is the best alternative for developing countries where communications infrastructure doesn't exist. To understand the how MANET is created, configured and controlled we need to understand the following area: MANET Architecture, Clustering Formation, Identification of Host and IP address auto configuration, Handover mechanisms on MANET, Routing on MANET, MANET file sharing, Different types of attacks and Security on MANET.**

I. INTRODUCTION (MANET ARCHITECTURE)

In MANET, mobile nodes can communicate without the need of the fixed communication infrastructure. The autonomous mobile devices in MANET move in any direction dynamically at a variable time in any direction keeps on changing the network topology. Designing a routing protocol is a challenging issue due to the ever changing network topology. The mobile nodes have a restricted transmission range; the nodes within the range can communicate directly. If a node wants to communicate with a node located beyond it transmission range, the other neighbouring nodes will help the source and destination to exchange the message. Due to the dynamic nature of MANET it has several drawbacks: frequent change in network topology without prior notification, difficult to provide real-time service, lack of resources and absence of central control devices.

MANET Advantages:

1. Easy to setup and configure.
2. Cost effective.
3. Flexible design architecture.
4. No need of communication infrastructure.
5. Dynamic network topology.
6. Self-sustainable network.
7. Works without the central control devices.
8. Can be setup at anytime, anywhere and at anyplace easily.
9. Helpful during disaster management.
10. Used in vehicular communications.

MANET Challenges:

1. Unsafe and not completely secured.
2. No Authorization
3. Limited resources.
4. Difficult to identify attacks.
5. Difficult to maintain route.
6. Bandwidth and Energy constraints.
7. High Latency.
8. Transmission Errors.

II. CLUSTERING FORMATION IN MANET

Clustering technique is used to manage the MANET easily, to increase the network stability, to increase routing performance, to reduce routing overhead by decreasing the scope of the routing tables and to save energy. Clustering divide's a single network into multiple interconnected subnets or clusters and increases the

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 6, June 2016

stability of the network. In each cluster, there is one cluster head and multiple clients. These clusters and the clients in the clusters are managed by Cluster Heads (CH), any mobile node or a host can act as a cluster head. To be a cluster head the basic functionalities are processing capacity and transmission power. The cluster head (CH) act as a default gateway to that cluster, it manages the routing information. The mobility and power limitation of the cluster head affects the performance of the cluster. The connections between the clusters are managed by the clustering algorithms.

In [1], two proposed clustering algorithms; the Highest-Degree which takes into consideration the degree of a node, and the Lowest-ID which assigns a unique ID to each node and chooses the node with the minimum ID as a CH. For example in figure 2, the mobile nodes are scattered and not connected.

In figure 3, the mobile nodes are interconnected, formed a cluster and node (E) act as a cluster head which controls and manages the entire cluster.

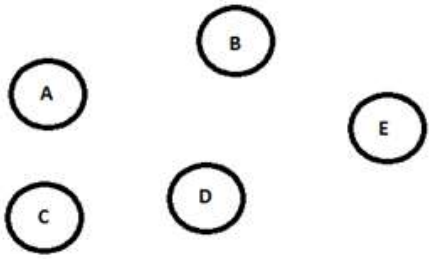


Figure-2 Autonomous Mobile nodes

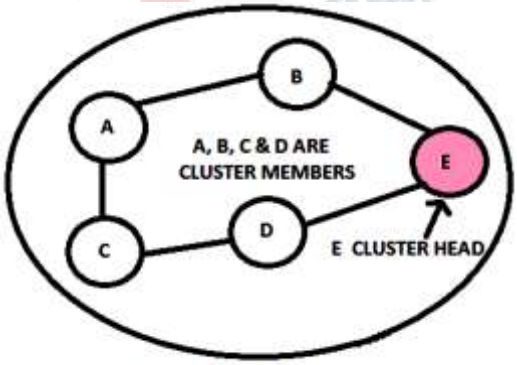


Figure-3 Node A, B, C, D and E formed a cluster

III. IDENTIFICATION OF HOST AND IP ADDRESS AUTO CONFIGURATION

A group of autonomous mobile nodes cooperatively forms an independent mobile ad hoc network without using any fixed architecture. In MANET, the mobile nodes with in the rage can communicate directly and nodes beyond each other's range communicate using multi-hop route through the intermediary nodes. A distributed dynamic host routing protocol designed to configure the nodes in MANET. Host IP address should be unique and no two host in the same network shares the same IP address. A node may join or leave the network at any time, due to that the topology changes variably. The cluster head in the cluster or group, act as a default gateway and router. The cluster head assigns a candidate IP address to the newly arrived nodes. The newly arrived node broadcast a request for IP address; the cluster head receives the request and choose and IP address from the address pool and assign the same to the requester.

The cluster head broadcast the assigned IP address to all the host in the network, once the entire host acknowledges then the IP address is permanently assigned to that host. Before leaving the network a node surrender the IP address to the cluster head by sending a broadcast message. If a node curtly leaves the network or goes down without surrendering its IP address to the cluster head. The cluster head release the IP address of the departed node and it is reused in future. A detailed description of the protocol and correctness proofs can be found in [2].

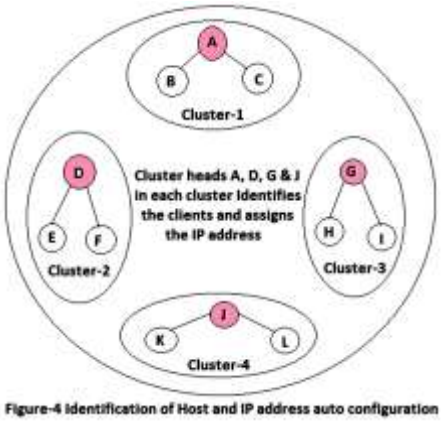


Figure-4 Identification of Host and IP address auto configuration

Hardware based addressing can be used as an alternative

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 6, June 2016

method by using IPv6 stateless auto configuration [3]. The IPv6 version uses a 64 bit Prefix ID and 64 bit Interface ID.

IV. HANDOVER MECHANISMS OF MANET

Handover in the mobile ad hoc network is achieved when the node moves from one cluster to another cluster. When a route breaks in MANET the communication interrupted until the new route is determined also due to this delay increased in the communication. To handle this situation a handover algorithm is used to predict the route failure and it informs the nodes in the cluster well in advance. It discovers the new route before the existing route fails. Link availability algorithm is used to predict the future disconnection of nodes from cluster using global positioning value. In general the handover algorithm achieves the goal by using following steps. Initially it predicts the connectivity period in the route, updates the status of the nodes in the route and sends the handover message when the connectivity period is less than the threshold time. Network Simulator NS-2 [4] is used to simulate AODV and the handover mechanism.

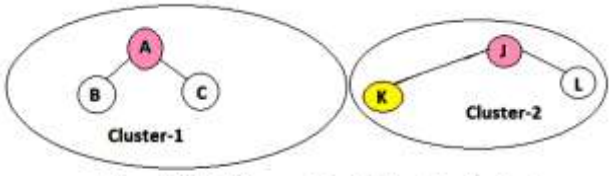


Figure-5 Client (K) moves from Cluster-2 to Cluster-1

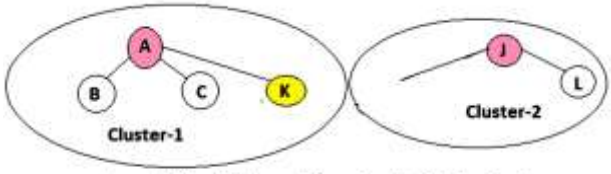


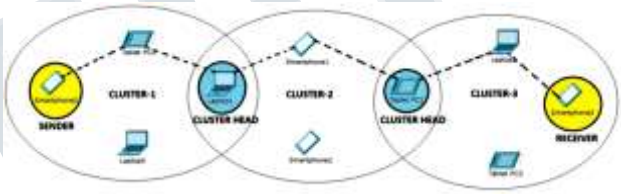
Figure-6 Client (K) moved from cluster-2 to cluster-1

V. A NAME RESOLUTION TECHNIQUE FOR MANET

In MANET, the communications is not as easy as wired network, because identifying and remembering the host address are very difficult. The Name Resolution Technique is used to identify destination by its hostname instead of its IP address. The Name Resolution protocols provide each node a unique hostname and translate the hostname into IP address. The name management module in a node manages name information by exchanging four types of messages, HELLO, CONFLICT, LIST, REQUEST and LIST REPLY [5].

Issues in resolving names in MANET:
1. Absence of cluster head.
2. Dynamic topology
3. Naming conflict issue
4. Naming utility issue

VI. ROUTING ON MANET



The real challenge in MANET is designing a successful routing algorithm due to its dynamic nature and frequent toplogy changes. The charecteristics of ad hoc network are mobility, low bandwidth and low power hence information collection during the initial network setup is a complex process. In wired network traditional routing protocols like distance vector routing [6] or link state routing protocols [7] are used to route the packets. In MNAET, nodes communicate through single channel or multiple channel. In single chanel communication, if the number of mobile host increases the collision and contension rate, also it affects the quality of service. So multiple channel is used an alternative for single channel communication. The channel allocation is a complex task in multiple channel, so the channel assignment protocols are designed and deployed to solve this issue, Also it will assign the channel statically, but it is not convinient for MANET, on-demand allocation is the best suitable method for MANET.

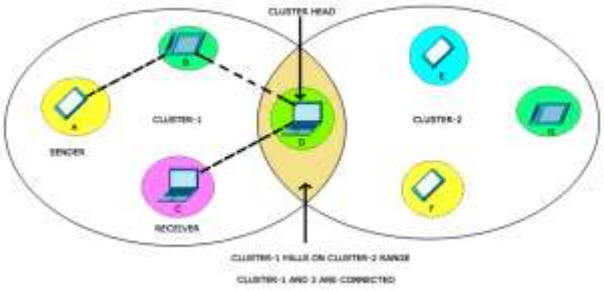
Routing Process

In MANET, the routing algorithm builds a spanning tree

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 6, June 2016

and a generation table for each node. Initially any one of the node in the cluster is selected as a cluster head for the spanning tree, then the spanning tree is extended from the cluster head to client by client. Once all the nodes or clients are connected in the spanning tree, each client will generate a generation table and share with the cluster head. Now the cluster will generate a routing table by collection information from the client's generation table.



In the above diagram, if A wants to send a message to C, node A will search the destination node C address in its generation table, if the address is available then A send the message through the route (Route: A □ B □ D □ C) first node A send the message to its neighbor B, later node B will the send the message to node D, finally node D will deliver the message to C. The receiver node C will do the same process to send the reply.

VII. MANET FILE SHARING

MANET requires the third party applications to share the information and files. Popular MANET applications like Napster and Gnutella are used for sharing files. In [8], In MANET, for the successful exchange of files between nodes, each client requires Gnutella client software. It implements a distributed search system; it broadcast the queries to all the nodes in the cluster. After MANET setup, Gnutella client requests a list of working addresses. Gnutella is a composite network made of cluster head and cluster clients. Cluster head and cluster clients use the query routing protocol to exchange the query routing table. If a search request is broadcasted to the entire cluster client, the node that has the result replies the searcher. In general, searching on the Gnutella network was often unreliable due unstable network and not scalable due to bandwidth cost. Additionally Gnutella adopted a number of other techniques to reduce traffic overhead and make searches more efficient.

VIII. SECURITY ATTACKS ON MANET

In MANET, Security is challenging part of the system. MANETs are more vulnerable to security attacks due to the lack of a trusted centralized authority, easy eavesdropping, dynamic network topology, and limited resources. The most common types of attacks, namely rushing attack, blackhole attack, neighbor attack and jellyfish attack.

Rushing attack:

The On-demand protocols like ADMR, MAODV and ODMRP are vulnerable to rushing attacks; it results in denial of services. Rushing attackers, by skipping some of the routing processes, can quickly forward these packets and be able to gain access to the forwarding group. [10]. When a node send a route request packet (RR packet) to another node in the wireless network, if there an attacker present then he will accept the RR packet and send to his neighbour with high transmission speed as compared to other nodes, which are present in the wireless network. Because of this high transmission speed, packet forwarded by the attacker will first reach to the destination node. Destination node will accept this RR packet and discard other RR [11].

Blackhole attack:

The attacker simply drops all incoming and outgoing data packets and doesn't acknowledge the sender, it results in very low packet delivery ratio [11].

Neighbor attack:

Upon receiving a packet, an intermediate node records its ID in the packet before forwarding the packet to the next node. However, if an attacker simply forwards the packet without recording its ID in the packet, it makes two nodes that are not within the communication range of each other believe that they are neighbors, resulting in a disrupted route [11].

Jellyfish attack:
A jellyfish attacker first needs to intrude into the forwarding group and then it delays data packets unnecessarily for some amount of time before forwarding them; it results in significantly high end-to-end delay and delay jitter, and thus degrades the performance of real-time applications [11].

IX. CONCLUSION

This paper gives an overall idea about the fundamentals characteristics and functional operations of MANET like MANET Architecture, Clustering Formation, Identification of Host and IP address auto configuration, Handover mechanisms on MANET, Routing on MANET, MANET file sharing, Different types of attacks and Security on MANET.

X. REFERENCES

[1] M.S. Al-Kahtani and H.T. Mouftah "A stable clustering formation infrastructure protocol in mobile ad hoc networks" IEEE international conference on Wireless and Mobile computing, Network and Communications, Volume: 3, PP: 406 – 413, 2005

[2] S. Nesargi and R. Prakash, "DADHCP: Distributed Dynamic Configuration of Hosts in a Mobile Ad Hoc Network," Tech. Rep. UTDCS-04-01, University of Texas at Dallas, Department of Computer Science, 2001.

[3] S. Thomson and T. Narten, "IPv6 Stateless Address Autoconfiguration, RFC 2462," Internet Engineering Task Force, Zeroconf Working Group, December 1998.

[4] Kevin Fall and Kannan Varadhan, editors. The ns manual (formerly ns Notes and Documentation). The VINT project, UC Berkeley, LBL, UCS/ISI and XEROX PARC.

[5] M. Aoki; M. Saito; H. Aida; H. Tokuda, "ANARCH: a name resolution scheme for mobile ad hoc networks", 17th International Conference on Advanced Information Networking and Applications, 2003. AINA Pages: 723 - 730, 2003.

[6] J. M. McQuillan, I. Richer, and E. C. Rosen, " The new routing algorithm for ARPANET", IEEE Transactions on Communications, 28(5):711 - 719, 1980.

[7] C. Hedrick, "Routing information protocol", Internet Request for Comments RFC 1058, June 1988

[8] T. Klingberg and R. Manfredi, "Gnutella 0.6, draft," http://groups.yahoo.com/group/the gdf/files/ Development/GnutellaProtocol-v0.6-200206draft.txt, 2002.

[9].."Gnutella Protocol Development". Rfc-gnutella.sourceforge.net. Retrieved 2017-04-13.

[10] Y.C. Hu, A. Perrig, and D.B. Johnson, "Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols", Proceedings of ACM WiSe 2003, San Diego, CA, Sep. 2003.

[11] Satyam Shrivastava, "Rushing Attack and its Prevention Techniques", "international Journal of Application or Innovation in Engineering and Management", Volume 2, Issue 4, April 2013.