A Protocol Based Routing Technique for Enhancing the Quality of Service in Multi Hop Wireless Networks

P.Arivubrakan, S.Sundari

Abstract: Wireless Networks named as mesh network, ad hoc and sensor networks consists of number of nodes that are communicated with the infrastructure less environment with the no base station or central controller. It is transmitted the packet between the source and destination by multi hop communication. In Adhoc and sensor networks, the communication are depends on the following metrics such as energy efficient, battery constraints, bandwidth, security and the main drawback between the transmissions of packets in Quality of Service because of wireless environment there is possibility of packet loss due the loss of link failures or in between some of other nodes has taken their packet and so on. In ad hoc networks communication takes place more than one hop. In order to attain the maximum throughput, minimum delay, highest bandwidth and jitter (Variation of delay), our proposed protocol named as ODSP (On demand Secured Protocol) will attain above the mentioned metrics by make use of concept of monitoring, scheduling the packets and clustering in wireless networks.

Index Terms: Ad-hoc, Multihop,Networks, Secured communication, Transmission.

I. INTRODUCTION

In wireless Networks, if two nodes are communicating in an environment, without the protocol the packets won’t transmit. The nodes are in static if mesh protocol is used, if it is dynamic, nodes in the ad-hoc networks forms multi hop communication. The real time applications are emergency rescue operation and military operations[1], in order to find difficult in communication between the nodes and coordination among all nodes.

The major issues and challenges in wireless network are
1. Nodes are dynamic in nature.
2. Bandwidth Constraints
3. Error prone broadcast communication.
4. Receiver Node are not within the range of Sender.
5. Energy in terms of power limited.
6. Control overhead
7. Depends on the unicast routing protocol
8. Scalability of resource management

Nodes are dynamic in nature means; there is possibility of lack of node link failures in wireless networks and also another major issue is the hidden fatal difficulty, the nodes of sender1 is not in the transmission range of sender2, there is possibility of packet loss, and also exposed problem occurs if the both sender are in the same range, there is possibility of clashes if both send the information to the receiver, our protocol is used to avoid the major issues in wireless network.

The routing protocol[2] in wireless networks will make use of the Tree based and Mesh based protocol in order to perform multicasting. Tree based routing protocol performs single path communication and the mesh based routing protocol will make use of multiple path for sending and receiving the packets for transmission. The Routing protocol are classified in to 3 major categories, Based on the multicast topology information, initialization of the broadcast session, Based on topology maintenance information., and Based on utilization of specific resources.

The multicast routing protocols can be divided into two major category [3]
1. Application Dependent
2. Application Independent

Tree based routing protocol is further divided into source tree based and shared tree based routing protocol. In source tree based routing protocol, a tree is maintained between the sources while the source tree based routing protocol, only one tree is shared between all the sources. it is more scalable between all the tree based routing protocol[4]. The two operations will be performed in multicasting are the sender initiated and the receiver initiated routing protocol[5].

Fig 1.Multi Hop Wireless Networks

A Protocol Based Routing Technique for Enhancing the Quality of Service in Multi Hop Wireless Networks

Protocol, instead of giving importance to finding the shortest path, the sender has to look for the nearest neighboring node in order to reduce the number of control packets for transmission. Tree establishment and tree maintenance is used to discover the path. To remove the unwanted nodes, the route optimization is used. The disadvantage of the protocol is distance increases, there is possibility of path breaks in leads to delay and the number of packets decreases.

MZRP: Multicast Zone Routing Protocol, is to flooding the packets between nodes, it searches the members of group monitored by zone routing techniques[7]. In Routing zone, on demand approach is used for maintaining the table information of each node in the zone. it is the combination both on reactive and proactive routing protocol. The disadvantages of this protocol are zone size is increases there is possibility of packet loss. Tree establishment an maintenance are accepted over here. If the receiver is far away from the sender node, it takes time for joining in multicast tree[8].

MCEDAR: Multicast Core Extraction Distributed Ad-hoc Routing, the source based tree protocol more efficient and less in security. In order to increases the robustness, the core nodes are nominated to share their neighboring information up to 3 multi hops. It is mainly the concept of mesh infrastructure; the nodes are static in nature. Core nodes also called as minimum nominating nodes in the networks. Core nodes used the concept of piggy backing technique for the communication. The disadvantage of this protocol is more complex proportional to the performance in the network.

DDM: Differential Destination Multicast Routing protocol is used for small nodes in the network. The destination node those who interested for the transmission will send information with unicast[9] routing protocol. It uses minimum memory requirement due to central policy As the number of destination node increases, the size of the network decreases.

WBM: Weight Based Multicast Protocol is mainly focus on the weight of the entry point in the multi cast group. It is based on the join request by the control packet and joins reply by the data packet. The major disadvantage is location prediction may not work in all conditions[10]. Weight factor depends on the network load and the size of the group.

ASTMRP: Adaptive Shared Tree Multicast Routing Protocol[12] A source tree as a rooted node makes it as source and shared tree node having multiple sources. But they are not stable in case of the source. It maintains the list is named as forward list contains the information about the sender ip addresses from which the receiver to get the control packets. It is scalable due to the shared tree but packet delivery ratio is decrease.

ARAN: Authenticated Routing For Adhoc Networks, it is based on cryptographic certificates which eliminate all the attacks present in the network. The route request message is forwarded along with the certificate issued by[13] the source node, the route reply is established between the path which send by the route request. It is followed by the end to end authentication[14-20].

Fig.2 Routing Protocol Classification.

PLBMP: Preferred Link Based Multicast Protocol Selects the set of wireless links to the nearby nodes called as preferred links, and the use of these links for transferring the packets. It is tree based protocol based on single path communication, here each node is maintaining 2 hops of topology information and able to form the multi cast tree. It’s have the two tables that is maintained as NNT (Neighbours-Neighbours Table) and CT(Connect Table). the nodes in the network periodically sends the beacon signal like a alert message. Once the packet checks the eligibility of forwarding a packet in terms of battery power, if not discards that node and retransmit the packet which having the highest power. It is also follow the piggy backing in order to receive acknowledgement, tree establishment removes the inconsistency of the nodes and tree maintenance is there is node failure. [11] it recover in that phase. The disadvantage is significant control overhead even in scarce of bandwidth.

Fig.3 Routing Protocol Process.
Fig. 4 Application of Multi hop Communication

II. PROPOSED METHODOLOGY

A. ODSP

ODSP-On demand secured Protocol.
The protocol mainly based on the improving the packet delivery ratio and effectively make use of the bandwidth and the minimum delay attainment. The nodes are deployed in the environment as wireless. The number of nodes participating in the communication as multi hop. The sender node sends information to the receiver via multi hop based on the parameter metric such as hop distance and bandwidth.
The nodes send a broadcast message to the all the neighboring nodes by make use of the Route Request, in order to avoid the duplicate of the route request is received multiple times, we use RTS, Request to send , message is used via the Route Request for secured. Once the message received by the nodes, it again the send the Route Reply to make sure of the path initiated by the sender. Once the route establishment is finished, The RTS (Request to send) is sending to the final path, after receiving the CTS (Clear to Send). Once the CTS is received from the destination node it sends an information about the stability of the path for transmission.
Once the path is established it will make use of scheduling of packets by time division multiple accesses (TDMA) for the benefits of packet loss.
In order to enhance the robustness of the protocol with high mobility, it is having two types of node, mesh node and another is the core node, each node should maintain the table information about the entry and exit of that corresponding range. The members join din that group want to broadcast the information about the joining based on the distance. It floods the Join Request message to the mesh node as anew node. The core node having the TTL Time to Live parameter to discover the other members, each node form a clustering mechanism as a tree head.
The ODSP is the security aware routing protocol is mainly based on the source node broadcasts a Route Request packet to the all the intermediate node around their range, after route request is received by the intermediate node, it does not have a route to the destination. It route reply packet is reversed by the destination node to the source node. In order to initiate the path, forward security mechanism is used, each packet is maintained the key which is attached to the route request message, if it is equal then the packet will be forwarded at the initial neighboring node. Otherwise the route request message is discarded[21-28].
The key is encrypted as well decrypted at the neighboring node.

![Fig. 5 Established Secured Path.](image)
The execution of the routing protocol is mainly focused on the elimination of distributed denial of service attacks. It does not affect the presence multiple intruders corrupting the key table maintained by the node. It makes use of hash function to avoid the malicious nodes present in the network. The ODSP protocol makes use of sequence number to prevent the formation of loops in between the nodes[30].

B. Advantage

The ODSP in adhoc wireless networks having the benefits such as the detection of any unwanted nodes in the participation of communication between the source node and the destination node. If the route is established, the routing protocol is able to find the path and also ensure about the correctness of the route establishment. The adhoc wireless networks is dynamic, there is possibility of changing the topology, in order to determine of confidentially of network topology based on the key generated by the source node. The security is another major challenge in wireless networks, is to provide the secured communication between the nodes is monitoring by make use of scheduling the packets.

III. RESULTS AND DISCUSSION

NS2 is the network simulator used for the simulation of nodes in wired as well as wireless environment and it is open source software supported in windows operating systems by cygwin and Linux environment. The NS2 the language written in OTCL (Object oriented tool command language) and back end tool is C++.NAM (Network Animator Window) window is to visualize the nodes, how the packets are transformed in that window.
The quality of service is defined as the performance metric by the user in the network. The throughput is
A Protocol Based Routing Technique for Enhancing the Quality of Service in Multi Hop Wireless Networks

defined as quality of the number of bits per second. The implementation is based on the on demand secured routing protocol based on the parameter such as the nodes, packet delivery ratio.
The protocol is mainly find best path in order to identify the unwanted node and in the environment. The dark lines represent the best path.

![Fig.6 Nodes detection at route establishment](image)

![Fig.7 Packets send between source and destination.](image)

**BEST PATH**

**WORST PATH-DETECTION OF UNWANTED NODE**

of the node once its reached to he destination node with the key value, then the transfer the route reply to the node along with the sequence number for guaranteed the path, once the route is established based on above criteria, the data is transferred between the source and destination. Once the data is received by the destination node, acknowledgement is send by the receiver.

![Fig.8 Throughput Attainment-ODSP](image)

**Throughput**

![Fig.9 Delay](image)

**Delay**

**IV. CONCLUSION**
The research paper is implemented the new technique as ODSP routing protocol with the attainment of highest packet delivery ratio when compare with other on demand protocol for secured communication. The major contribution towards the protocol is attainment of quality of service in more than one hop communication of wireless networks for secured way of establishment of route before transfer the packets. In future enhancement, number of nodes will be increased and applied in real time applications.

**REFERENCES**
1. Susan G Varghese,CijiPearl Kurian,VI George “A Study of communication protocols and wireless networking systems
for lighting control applications”IEEE Xplore,Digital Library,2016.


AUTHORS PROFILE

P.Arivubrakan has been working as an assistant professor in the department of computer science and Engineering at Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai and has published the papers in Scopus indexed journals. Specialization in pervasive computing Technologies. The Area of research such as wireless networks, sensor networks and IOT.

S.Sundari has been working as a assistant professor in the department of computer science and Engineering at Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology and has published the papers in Scopus indexed journals. M.E Embedded System Technologies. The Area of research such as wireless networks and network security.