EVICTION OF MISBEHAVING NODE IN WIRELESS METROPOLITAN MESH NETWORKS

P.X.Britto, S.Monisha, D.Elamathy

Abstract- Adhoc network and Wireless local area network (WLAN) combined together as wireless mesh network. In existing systems, two schemes are proposed to provide security and privacy in wireless mesh networks. Devastation caused by inside nodes i.e. misbehaving nodes is not considered. In this paper we propose a solution in order to evict (detach) the misbehaving node from the network. The technique of inter domain packet filter is used for the prevention of network from misbehaving nodes.

Index terms- **Wireless networks, misbehaving node, BGP**.

I.INRODUCTION

Wireless mesh network comprises of mesh routers and mesh clients. Wireless mesh networks (WMNs) consist of mesh routers and mesh clients, where mesh routers have minimal mobility and form the backbone of WMNs. They provide network access for both mesh and conventional clients. The integration of WMNs with other networks such as the Internet, cellular, IEEE 802.11, IEEE 802.15, IEEE 802.16, sensor networks, etc., can be accomplished through the gateway and bridging functions in the mesh routers. Mesh clients can be either stationary or mobile, and can form a client mesh network among themselves and with mesh routers.

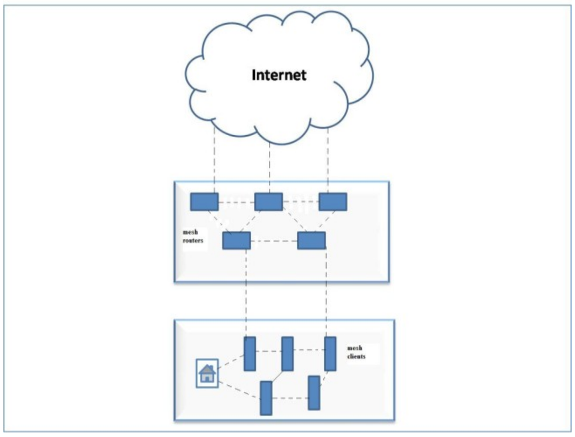

Fig 1. Mesh topology

The routing process depends upon the behaviour of node taking part in the communication. Basically all the routing process assumes that the node is in the proper state, such that the nodes can forward the data packets successfully to the intended user. However, in a network, misbehaving node occurs which leads to the degradation of performance, heavy packet loss and denial of quality of service in the network.

Misbehaving node is a node that which degrades the performance of a network. Misbehaving nodes are broadly classified into following categories.

- Inactive node
- Selfish node
- Malicious node

Inactive node: These nodes, knowingly or unknowingly do not intensely partake in the communication.

Selfish node: These nodes do not forward the packets to the destined node, rather keep it for itself.

Malicious node: these nodes discard the packets as they transfer or will add on irrelevant data on to the packets.

In this paper, we investigate the devastation caused by inactive nodes. We propose a solution in order to evict the misbehaving node. The technique of inter domain packet filter (IDPF) is used to solve this issue.

II SYSTEMIZATION

PSEUDONYM BASED REGISTRATION

The network user does not furnishes its real identity to its service mesh router. Instead it registers itself with a pseudonym which is denoted as NYM-SD rather than disclosing its real identity as S. This pseudonym persists only for one session. In other words, these pseudonyms are updated for each session.

ONOIN ROUTING BASED MESSAGE DELIVERY

Anonymity is maintained and still the routing process is performed. And this is with the help of the pseudonym. Onion routing is claimed to be a ring like structure, in which the intermediate routers are termed as intermediate onion routers. Each onion router is aware only of its source and destination. It cannot navigate through the route discovery. The source contrives the path to the destined node (i.e. destination node) using the path finding algorithm. It determines the layers of encryption it has to perform before forwarding the packet. The source node organises the path as follows (for example).
Rs→Ra→Rb→Rc→Rd.

Each onion router receives the packet from previous onion router, does a layer of decryption and forwards the packet to the intended node. The destination node does the last layer of decryption. It recognises the message and freezes any further packet forwarding.

EVICTION OF MISBEHAVING NODE

The routing process relies on the node behaviour. The performance of the network degrades drastically if the node misbehaves. Inactive nodes constitute a part of misbehaving nodes and they are dealt in this paper.

The onion ring structure with the help of the Inter domain packet filter technique (IDPF) is able to diagnose the misbehaving node and detach them from any further communication in the network.

Inter domain packet filter is constructed using Border gateway protocol (BGP). Implicit informations are drawn from the BGP in order to perform the eviction process. BGP is used for directing the routing decisions. Border gateway protocol guards the table of IP networks. The inter domain packet filter draws information from the BGP and keeps updating all the parcipants of the communication in the network.

If it detects any misbehaving node, it immediately intimates all other parcipants of the process about that particular node. As it identifies the node, it evicts the node from the network for any further communication or packet forwarding. As the node is being evicted, some packets would still be forwarded to it. This packet forwarding would be terminated once it is completely detached from the network. The inter domain packet filter would discover another route for the packets to be delivered to the destined node. Those packets that were delivered to the misbehaving node during the process of eviction would be retransmitted via the newly discovered route. Hence making the communication successful.

CONCLUSION

In this paper, we have scrutinized the problem of misbehaving node (Inactive node) and proposed a solution to evict them from the network in order to avoid packet loss, enhance the performance of the routing process and quality of service. The technique of inter domain packet filter is used to detach the misbehaving node which frequently updates all the participants of the network about the routes. IDPF is constructed using Border gateway protocol. A detailed evaluation shows that the proposed technique prevents the network from misbehaving node.

REFERENCES

[1] Zhenhai Duan, Xin Yuan, Jaideep Chandrashekar "Controlling Ip Spoofing Through Inter Domain Packet Filter".

[2] Matthias Hollick, Jens Schmitt, Christian Seipl, and Ralf Steinmetz "On the Effect of Node Misbehaviour in Ad Hoc Networks".

[3] Zhiguo Wan, Kui Ren, Bo Zhu, Bart Preneel And Ming Gu "Anonymous User Communication For Privacy Protection In Wireless Metropolitan Mesh Networks".

[4] David B. Johnson, David A. Maltz "Dynamic Source Routing in Ad Hoc Wireless Networks".

[5] Ian F. Akyildiz a, Xudong Wang b,*, Weilin Wang b " Wireless mesh networks: a survey".

[6] X. Wu and N. Li, "Achieving Privacy In Mesh Networks," in proc. 4th ACM workshop security ad hoc sens. Networks.