IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Vol. 08, Issue 6 (June. 2018), ||V (V) || PP 01-03

Development of Heterogeneous Zone Routing Topology for Mobile Ad Hoc Network

T.R. Muhibur Rahman[1], Dr. Nagaraj B.Patil
[1]*Research Scholar, JJT University, Jhunjhunu, India*
[2]*Dr. Nagaraj B.Patil ,Research Guide, JJT University , Jhunjhunu, India*
Corresponding Author: T.R. Muhibur Rahman

Abstract: An accumulation of wireless mobile hosting companies developing a short-term network without having assistance from any kind of centralized supervision or regular assistance services for situations like conferences, disaster alleviation conditions, IoT sensor systems etc. This paper targets on 'Route discovery' problem and planned model recommends new network topology for MANET communication. The developed topology facilitates hybrid protocols which might be the combination of the proactive as well as reactive strategies. Present research deemed Zone Routing Protocol often known as Hybrid-ZRP as a reference protocol topology model. However, existing ZRP is for homogeneous surroundings so there is a need to develop heterogeneous ZRP for better performance. Hence, we developed check-point ZRP topology.

Keywords: Route discovery, hybrid protocols, zone routing protocol, topology, check-point ZRP, proactive protocols, reactive protocols, QoS

Date of Submission: 07-06-2018 Date of acceptance: 23-06-2018

I. INTRODUCTION

A collection of protocols incorporating the benefits of the two reactive as well as proactive were built to deal with security and also QOS concerns. Out of the hybrid protocols, ZRP has come forth as a extremely capable hybrid routing protocol having confined proactive opportunity because of the development of specific zones. Nevertheless, the existence of overlapping specific zones and some additional hindrances abandon several scope for improvements, necessary to improve the effectiveness of ZRP.

Hybrid routing protocols consist of Zone Routing Protocol (ZRP), Zone dependent hierarchical link state routing (ZHLS) protocol, Hybrid wireless mesh protocol (HWMP). Proactive and reactive routing protocol similar to AODV generate massive amount end to end hold off throughout route discovery and keeping routing table which are defeat in hybrid protocols. However for improved efficiency and productivity ZRP is employed, because of its route maintenance and also route discovery technique. This paper presents the topology enhancement to ZRP which can be more efficient for heterogeneous region applications.

II. BACKGROUND STUDY

The algorithm for synthesizing route aggregation in ZRP begins with development of more specific zones in which the contributing nodes behave as members of the aggregation. Then this zone head is chosen for that newly produced nodes, accompanied by aggregation of all of the routes after which it streaming these to the connection state table [1].

Other author examined protocols amongst diverse variables where there effectiveness is examined. This particular paper offers information on the possible risks which posses in available communication route in real time and also their particular results around the functionality. Several variables are simulated to gauge the performance for protocols. Network layer attacks employed in this work for evaluation narrows the options of applying dysfunctional protocols that additionally proves the need of making use of certain hybrid routing protocol [2].

Author dealt with the blackhole attack together with recommended a modern safety model to deal with this kind of attack. This recommended model facilitates Ad hoc on Demand Distance Vector (AODV) routing protocol and that is the preferred protocol in the MANET. The suggested model not merely offers node authentication but additionally communication authentication using low overhead [3].

In MANETs, risk-free communication is extremely challenging to accomplish due to the fact its nature-like communication channel is open wireless which is often effortlessly utilized by any individual who is available in the radio range of the interacting gadgets, nodes are actually weak, less-efficient communicating devices, the lack of core authority, free of the restriction of topological composition of network, etc [4].

Consequently, it is crucial to build up new topology which may be applied to produce much more security to MANETs.

In other work, the root node serves, alternatively, as a possible attack facts data source. The cluster heads, author recommended, utilizes a MANET particular attack response algorithm [5]. To get rid of topology issue and also to produce foundation protection to new topology, proposed model is discussed in next section-3.

III. PROPOSED RESEARCH MODEL

The proposed research model is designed to provide security for following attacks:*Black Hole Attack:* In these particular attacks attacker nodes directs route response information to route request message that contains minimal sequence number for routing and just before virtually any legitimate reply arises from any genuine node source node considers the attacker node is the appropriate route and begins packet transmission around fake nodes. The packets sent by means of this attacker node are never submitted to any node. This kind of attack occurs whenever attacker node is within the network and attacker consistently requests for packet leading to sleep deprived attack of the node [9]. It could be deemed as refusal of service attack as it obtains all packets and deliver nothing. It is known as black hole as almost all packets sent to it will never be sent to any other nodes that leads to refusal of service. There are two kinds of black hole attack: Solitary black hole attack through which one node reacts as the black hole node in the network. Next one is collaborative black hole attack through which numerous black hole nodes are within one network [6].

Gray Hole attack: Gray hole attack happens in the event the attacker nodes merely keep the packets which might be expected by the attacker and remainder all nodes are dropped. It is usually known as routing misbehavior, as with this the attacker node allows the node to forward but once obtained they are dropped selectively. This kind of attack also brings about denial of service attack [7].

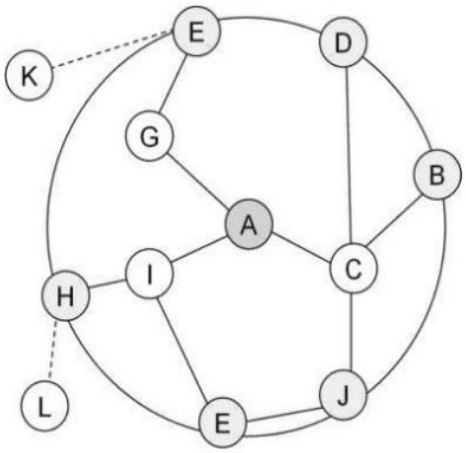

Figure 1: Zone Routing Protocol ZRP Routing [1] (radius=2-Hop; E, D, B, J, E and H are border-nodes)

ZRP does not strictly specify the protocol used but allows for local independent implementations. As multi-protocol support system needs more security, following topology is designed as a new solution of check-point ZRP.

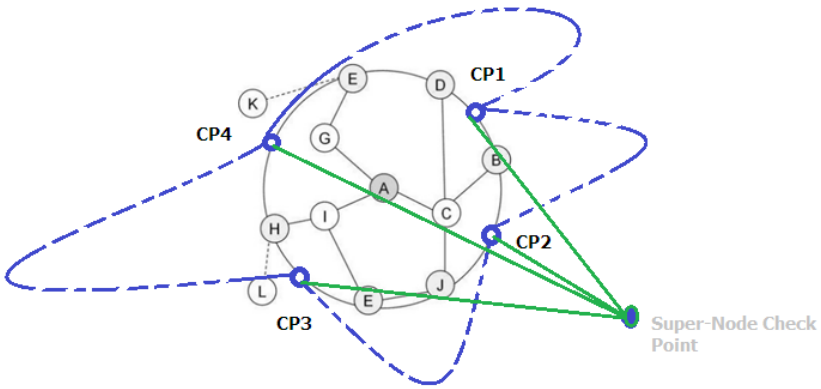

Figure 2: check-point ZRP

As shown in figure 2, the super node check-point will monitor attach possibility in terms of response from check points array [CH1, CH2, CH3, CH4]. These check points are logically executed in random fashion to keep eye on attacker node. If black hole response persists, check points can redirect/close or put routing in sleep mode for predefined delay. Thus, the packet transmission will fail if suspicious action persists. This will be a good solution for MANET security concerns.

IV. CONCLUSION

The new model topology facilitates hybrid protocols which are the combination of the proactive as well as reactive methods. Present research considered Zone Routing Protocol referred to as Hybrid-ZRP as a reference protocol topology model. As, existing ZRP is for homogeneous environment, new topology supports heterogeneous ZRP for better performance.

REFERENCES

[1]. Mehta, Deepa, Indu Kashyap, and Sherin Zafar. "Synthesized hybrid ZRP through aggregated routes." International Journal of Information Technology 10.1 (2018): 83-89.
[2]. Chandra, Apoorva, and Sanjeev Thakur. "Qualitative Analysis of Hybrid Routing Protocols Against Network Layer Attacks in MANET." Apoorva Chandra et al, International Journal of Computer Science and Mobile Computing 4.6 (2015): 538-543.
[3]. Sirajuddin, M. D., Ch Rupa, and A. Prasad. "An Innovative Security Model to Handle Blackhole Attack in MANET." Proceedings of International Conference on Computational Intelligence and Data Engineering. Springer, Singapore, 2018.
[4]. Malhotra, Sachin, and Munesh C. Trivedi. "Symmetric Key Based Authentication Mechanism for Secure Communication in MANETs." Intelligent Communication and Computational Technologies. Springer, Singapore, 2018. 171-180.
[5]. Kaur, Manpreet, Dale Lindskog, and Pavol Zavarsky. "Integrating Intrusion Response Functionality into the MANET Specific Dynamic Intrusion Detection Hierarchy Architecture." Ad Hoc Networks. Springer, Cham, 2018. 69-80.
[6]. Pullagura, Joshua Reginald, and Dhulipalla Venkata Rao. "Simulation-Based Comparison of Vampire Attacks on Traditional Manet Routing Protocols." Information and Communication Technology for Sustainable Development. Springer, Singapore, 2018. 501-509.
[7]. Kalia, Anchal, and Harpreet Bajaj. "EDRI based approach with BERP for Detection & Elimination of Co-operative Black Hole in MANET." International Journal for Science, Management and Technology (IJSMT) 15 (2018).

IOSR Journal of Engineering (IOSRJEN) is UGC approved Journal with Sl. No. 3240, Journal no. 48995.

T.R. Muhibur Rahman "Development of Heterogeneous Zone Routing Topology for Mobile Ad Hoc NetworkIOSR Journal of Engineering (IOSRJEN), vol. 08, no. 6, 2018, pp. 01-03.