**Paper No: PU-SOE-CSE-31**

**A Novel Wolf Based Trust Accumulation Approach for Preventing the Malicious Activities in Mobile Ad-Hoc Network**

**Ramesh.Vatambetia**

a.Department of Computer Science and Engineering, School of Engineering, Presidency University,

Itgalpur, Rajanakunte, Yelahanka, Bangalore, 560064, India

**Abstract**

Mobile Ad hoc Network is self-organized and movable in nature, it is widely used in various applications including military and private sectors. However, security is one of the key concerns in routing because of the moving nodes; thus it is usually affected by Black Hole and Grey Hole attack. These types of malicious activities are more harmful to the network channel, and once the attack is happened it is difficult to predict and mitigate. To end this problem the current research proposed a novel Grey Wolf Trust Accumulation (GWTA) Schema in wireless mesh network architecture, thus the attacks are identified by the finest function of the GWTA model. Moreover, the predicted attacked nodes are replaced to the last position of the network medium to prevent the packet loss. Furthermore, the comparison studies proved the effectiveness of the proposed model by attaining less packet drop and high throughput ratio rate.

**Keywords:**

Mobile ad-hoc network, Black hole attack, Grey hole attack, Wireless mesh network, Secure routing

**Publication Details:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Journal Name** | **Vol.** | **Month & Year** | **Page No.** | **Publisher** | **Scimago Ranking** |
| Wireless Personal Communications | 111(4) | April, 2020 | Online publication | [Springer Netherlands](https://www.scimagojr.com/journalsearch.php?q=Springer%20Netherlands&tip=pub) | Q3 |