



**RESEARCH ARTICLE**

# Mitigating Location Attacks through Trust Based Model in MANETS

**SAI MIDHILA<sup>1</sup>, G ARULKUMARAN<sup>2</sup>, K PRABHAKAR<sup>3</sup>**

Student, Information Technology, Vivekanandha College of Engineering for Women, TamilNadu, India<sup>1</sup>

Assistant Professor Department of Information Technology Vivekanandha College of Engineering for Women  
Tiruchengode, Erode<sup>2</sup>

Assistant Professor Department of Information Technology Vivekanandha College of Engineering for Women  
Tiruchengode, Erode<sup>3</sup>

saimidhus@gmail.com<sup>1</sup>

erarkumaran@gmail.com<sup>2</sup>

k.prabhakar86@gmail.com<sup>3</sup>

## ABSTRACT

Mobile Ad Hoc Networks (MANETs) use anonymous routing protocols that hide node identities and routes from outside observers in order to provide anonymity protection. However, existing anonymous routing protocols which rely on either hop-by-hop encryption or redundant traffic generate high cost or cannot provide full anonymity protection to data sources, destinations, and routes. The high cost exacerbates the inherent resource constraint problem in MANETs especially in multimedia wireless applications. ALERT mechanism offers anonymity protection to sources, destinations, and also routes. It has strategies which effectively help to counter intersection and timing attacks. To offer high security protection at a low cost, we propose a Trust Based Model through Recommendation and local information of neighboring node for Efficient Routing based on this ALERT. Trust model dynamically partitions the nodes into benign and suspicious based on the data transmission of neighboring node and also it mitigates the network attack through formation of intermediate relay nodes, which form a non-traceable anonymous route. It hides the data initiator/receiver among many initiators/receivers to strengthen the source and destination anonymity protection.

## Keywords

Mobile ad hoc networks; anonymity; routing protocol; trust based model

Full Text: <http://www.ijcsmc.com/docs/papers/December2013/V2I12201367.pdf>