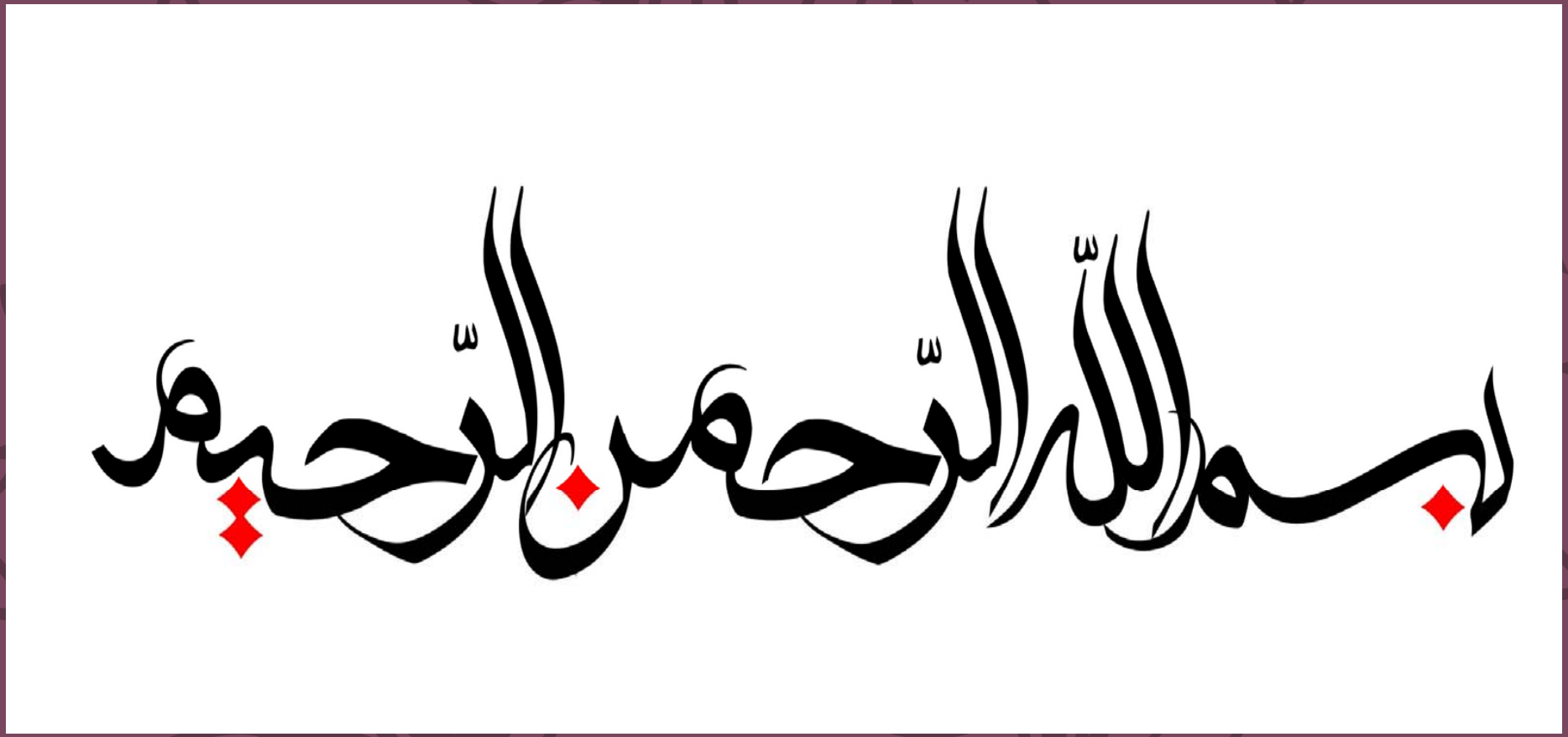


A TRUST BASED APPROACH FOR DETECTION AND ISOLATION OF MALICIOUS NODES IN MANET

Aravindh S[1], Vinoth R S [2] and Vijayan R[3]
[1,2] MS Software Engineering, School of Information Technology and Engineering,
VIT University ,Vellore, Tamil Nadu, India
aravindh.sy@gmail.com
vinoth9592@gmail.com
[3]Assistant Professor(SG),School of Information Technology and Engineering,
VIT University, Vellore, Tamil Nadu, India
rvijayan@vit.ac.in

Abstract— **A Mobile Adhoc Network (MANET) is a self-organized system comprised by multiple mobile wireless nodes. Due to the openness in network topology and the absence of centralized administration in management, MANET is vulnerable to attacks from malicious nodes. Nodes can change position quite frequently, which mean the mobility of the network. Node misbehaviours are serious attacks for routing protocols in MANET. Secure routing is the milestone in mobile Adhoc networks.**

The proposed trust management scheme gives an overview about trust in MANETs and current research in routing on the basis of trust. It uses trust values to favour packet forwarding by maintaining a trust counter for each node. If the trust counter value falls below a trust threshold, the corresponding intermediate node is marked as malicious and isolated from the Network, thus by increasing the performance of the network.

Keywords: **Trust Proctor, Trust Handler, Reputation Accumulator, Reputation Evaluator, DRUT, MANET**

I. Introduction

Wireless networks are defined as computer networks connected through wireless links, such as radio frequencies and infrared rays. Wireless local area networks (WLANs) have arisen with the main purpose of overcoming the limitations imposed by traditional wired networks, thus permitting faster network installations and mobility at lower costs. Ad hoc network consists of mobile nodes which communicate with each other through wireless medium without any fixed infrastructure. Mobile Ad hoc Network (MANET) do not have any fixed infrastructure and consists of wireless nodes that move dynamically without any boundary limitation. MANETs are advantageous because they are quick to install, provide fault tolerance, connectivity and mobility.

A. Security Issues in MANET

Various attacks exist in MANET. Active attack is attack when misbehaving node has to bear some energy costs in order to perform the threat. On the other hand, passive attacks are mainly due to lack of cooperation with the purpose of saving energy selfishly. Nodes that perform active attacks with the aim of damaging other nodes by causing network outage are considered as malicious while nodes that make passive attacks with the aim of saving battery life for their own communications are considered to be selfish.

Gray Hole attack can advertise its route as a valid path with the motivation of intercepting the packets. The packets that pass through the attacked node are dropped with certain probability. Worm Hole Attack follows the tunnelling process. Group of nodes collaborate to encapsulate and exchange messages between them leading to short-circuit of normal flow of packets and consume energy. Black Hole Attack the node advertises as a valid path to the destination and intercepts every packet without forwarding and can generate fake information. Jellyfish Attack can enter into the forwarding group and can delay the packets unnecessarily for a specific time and then forwards the packet resulting in performance degradation. Denial of service attacks aim at the complete disruption of the routing function and the entire operation of the ad-hoc network. In a routing table overflow attack, the malicious node floods the network to consume the resources.

B. Design Challenges in MANET

MANET exhibits unique features like open medium, dynamic topologies, bandwidth constrained, variable capacity links, energy constrained operation, limited physical security MANETs hence attracted by the attackers. The nodes in the MANET are vulnerable to all kinds of attacks launched through compromised node. Constraints in bandwidth, computing power, and battery power in mobile devices can lead to application specific trade-offs between security and resource consumption of the device.

آرم محل
تحصیل

موضوع ارائه :

دانشگاه.....
استاد راهنما : .....

ارائه دهنده : . . . . .

۹۵/۱۰/۱۲

عنوان :.....

فهرست مطالب

استاد راهنما : .....

آرم محل تحصیل

چکیده :

عنوان :.....

استاد راهنما : .....

آرم
محل
تحصیل

مقدمه :

عنوان :.....

استاد راهنما : .....

آرم
محل
تحصیل

معماری سیستم:

عنوان :.....

استاد راهنما : .....

آرم محل تحصیل

عنوان :.....

چکیده :

برای ۱-۶۰ گره

برای ۲-۱۰۰ گره

نتایج برای ۶۰ نود موجود و پیشنهادی

نتایج برای ۱۰۰ نود موجود و پیشنهادی

استاد راهنما : .....

آرم محل تحصیل

محیط شبیه‌سازی NS-2:

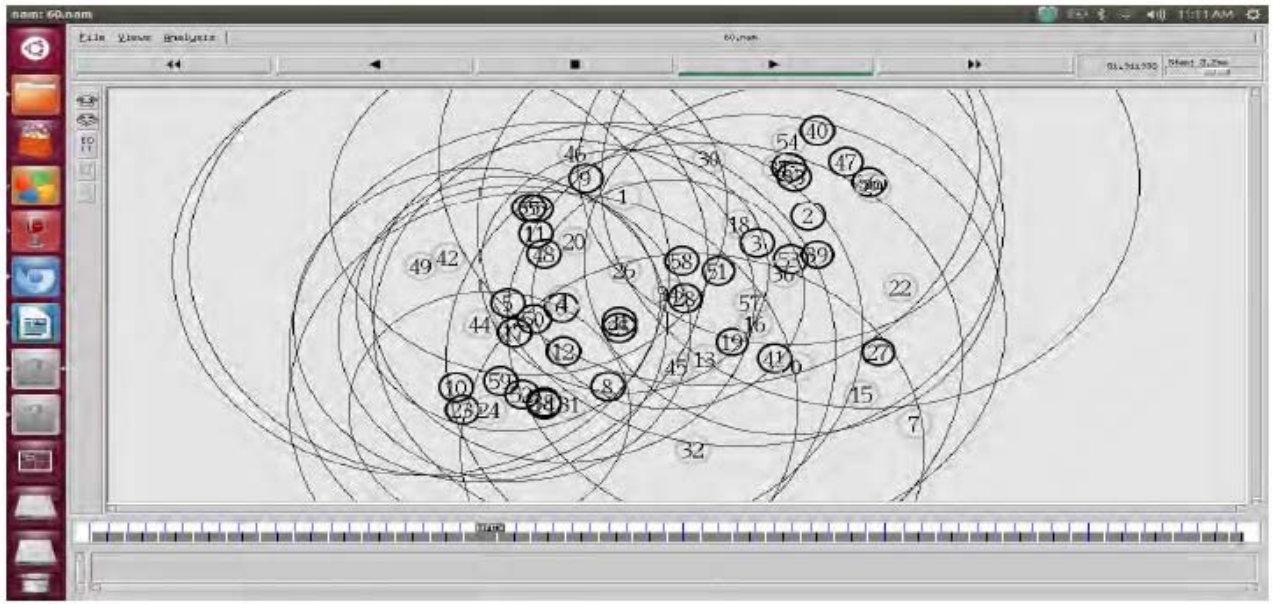
عنوان :.....

استاد راهنما : .....

آرم محل تحصیل

محیط شبیه‌سازی NS-2:
مدل نمونه با .....

عنوان :.....



شکل ..... –.....نمونه .....

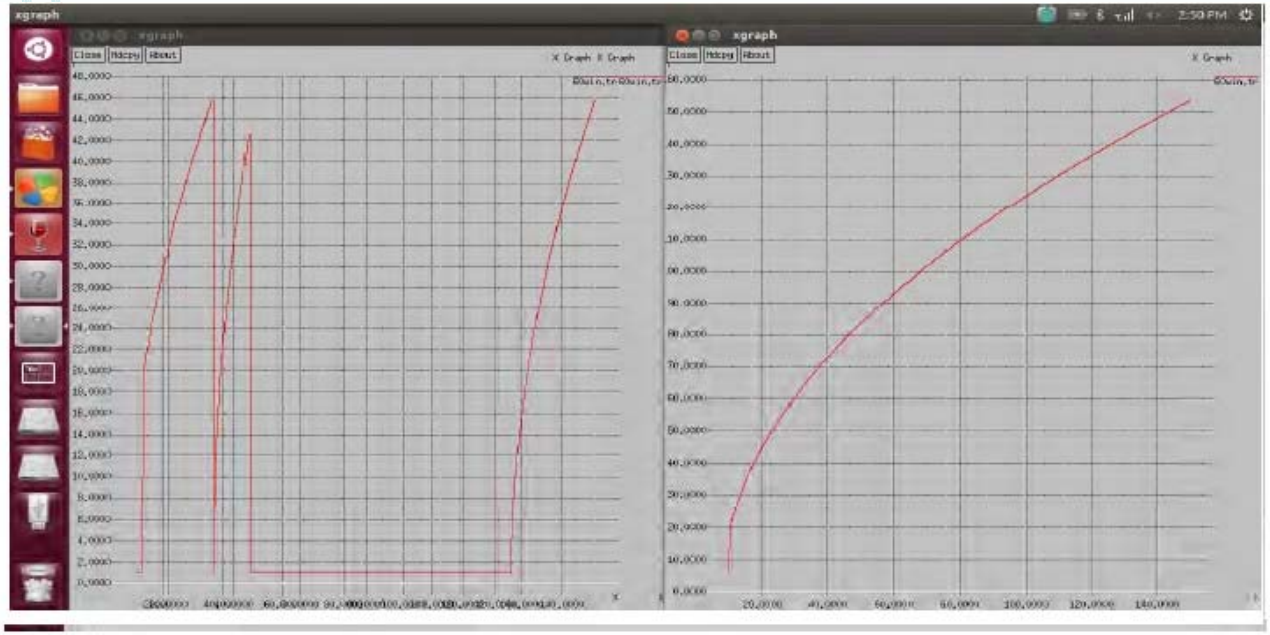
استاد راهنما : .....

آرم
محل
تحصیل

نتایج شبیه سازی:

عنوان :.....

نتایج برای نمونه .....



شکل ۶ – نتایج برای نمونه .....

استاد راهنما : .....

آرم
محل
تحصیل

نتیجه گیری :

عنوان :.....

استاد راهنما : .....

آرم محل تحصیل

عنوان :.....

استاد راهنما : .....

با تشکر از توجه دوستان

پ ا ی ا ن

آرم
محل
تحصیل