LTTP: LOAD BALANCED TRANSMISSION AND TRUST BASED PROTOCOL FOR MOBILE AD HOC NETWORKS

K.Mohanaprakash[1] | N.Kartheeban[2] | D.Karthik[2] | A.Lakshmanaprabu[2]

[1](Department of ECE,Assistant Professor,Jay Shriram Group of Institutions, Avinashipalayam, Tirupur-638 660)

[2](Department of ECE,Jay Shriram Group of Institutions, Avinashipalayam,Tirupur-638 660, rainaprabu54@gmail.com)

***Abstract*—*In mobile ad hoc networks (MANETs) a primary requirement for the establishment of in communication among nodes is that nodes should cooperate with each other. In the presence of malevolent nodes, this requirement may lead to serious security concerns for instance, such nodes may disrupt the routing process. This paper attempts to resolve this issue by designing a dynamic source routing (DSR)-based routing mechanism, which is referred to as the cooperative bait detection scheme (CBDS).We present a lightweight dynamic channel allocation mechanism and a cooperative load balancing strategy that are applicable to cluster based MANETs to address this problem. Through extensive simulations we show that both improve the bandwidth efficiency under non-uniform load distributions compared to protocols that do not use these mechanisms as well as compared to the IEEE 802.15.4 protocol with GTS mechanism and the IEEE 802.11 uncoordinated protocol.*

Keywords*— *MANETs, Dynamic Source Routing, Cooperative Bait Detection Scheme.

INTRODUCTION

As the wireless network technology exploded, it has opened a new view to users and expanded the information and application sharing very conveniently and fast. Mobile ad hoc networks (MANETs) use wireless technology without a pre-existing infrastructure (access points). As the name states, MANETs consists of mobile nodes, which can vary from notebooks, PDAs to any electronic device that has the wireless RF transceiver and message handling capability. Mobility and no-infrastructure forms the basis of this network type. Mobility gives maximum freedom to users, as they can be connected to the network, whether they are fixed or moving, unless they are in the range of the network. Also, it is highly dynamic, as the new nodes come, they can be connected to the network very easily. Unlike the fixed networks or traditional wireless networks, MANETs don't need any infrastructure to create and maintain communication between nodes. This property provides the ability to create a network in very unexpected and urgent situations very quickly, also without any extra cost. MANETs are autonomous and decentralized networks. So, they can operate no matter which nodes are connected or not connected to the network. Connectivity of nodes only affects the topology and routing of the network, not the general operations. Since, MANETs don't have any centralization, operations are done distributed, so each node has to have sufficient information about the network and have to operate independently. Two nodes that want to communicate with each other can send and receive messages directly, if they are both in their transmission range. Otherwise, every node is also capable to be a router, and the messages between nodes are relayed by the intermediate nodes, from the originator of the message to the destination. Since the nodes are mobile and the members of the network changes without any notice, the network structure is very dynamic. So, the route the messages are sent by, are dynamic also. Routing is a very vital and performance critic issue for ad hoc networks. So, we are going to handle that procedure in deep.

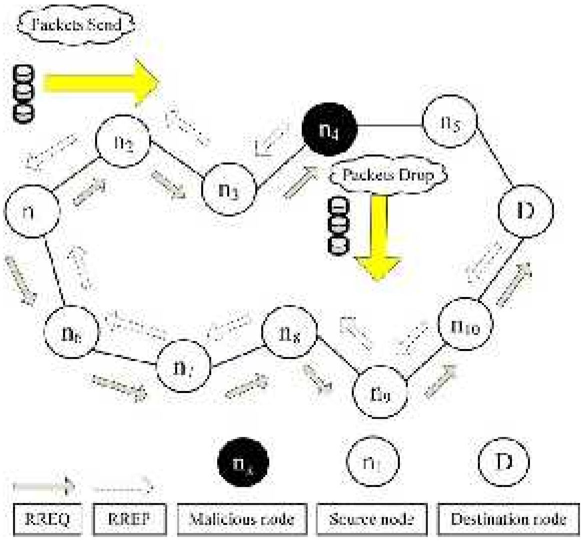


Fig1.Blackhole attack-node n4 drops all the data packets.

RELATED WORK

Avoiding blackhole and cooperative blackhole attacks in wireless ad hoc networks

Many research works have investigated the problem of malicious node detection in MANETs. Most of these solutions deal with the detection of a single malicious node or require enormous resource in terms of time and cost for detecting cooperative blackhole attacks. In addition, some of these methods require specific environment or assumptions in order to operate. In general, detection mechanisms that have been proposed so far can be grouped into two broad categories:

1) Proactive detection schemes, 2) Reactive detection schemes.

Mitigating routing misbehavior in mobile ad hoc networks

This paper describes two techniques that improve throughput in an ad hoc network in the presence of nodes that agree put in an ad hoc network in the presence of nodes that agree to forward packets but fail to do so. To mitigate this problem, we propose categorizing nodes based upon their dynamically measured behavior. We use a watchdog that identifies misbehaving nodes and a patl~rater that helps routing protocols avoid these nodes. Through simulation we evaluate watchdog and pathrater using packet throughput, percentage of overhead (routing) transmissions, and the accuracy of misbehaving node detection. When used together in a network with moderate mobility, the two techniques increase throughput by 17% in the presence of 40% misbehaving nodes, while increasing the percentage of overhead transmissions from the standard routing protocol's 9% to 17%. During extreme mobility, watchdog and pathrater can increase network throughput by 27%, while increasing the overhead transmissions from the standard routing protocol's 12% to 24%. 1. derlying routing algorithm. We introduce two extensions to the Dynamic Source Routing algorithm (DSR) [12] to mitigate the effects of routing misbehavior: the watchdog and the pathratcr. The watchdog identifies misbehaving nodes, while the pathrater avoids routing packets through these nodes. When a node forwards a packet, the node's watchdog verifies that the next node in the path also forwards the packet. The watchdog does this by listening promiscuously to the next node's transmissions. If the next node does not forward the packet, then it is misbehaving. The pathrater uses this knowledge of misbehaving nodes to choose the network path that is most likely to deliver packets. Routing Security in Wireless Ad Hoc Networks

A mobile ad hoc network consists of a collection of wireless mobile nodes that are capable of communicating with each other without the use of a network infrastructure or any centralized administration. MANET is an emerging research area with practical applications. However, wireless MANET is particularly vulnerable due to its fundamental characteristics, such as open medium, dynamic topology, distributed cooperation, and constrained capability. Routing plays an important role in the security of the entire network. In general, routing security in wireless MANETs appears to be a problem that is not trivial to solve. In this article we study the routing security issues of MANETs, and analyze in detail one type of attack the “black hole” problem that can easily be employed against the MANETs. We also propose a solution for the black hole problem for ad hoc on-demand distance vector routing protocol. The MANET is an emerging research area with practical applications. However, a wireless MANET presents a greater security problem than conventional wired and wireless networks due to its fundamental characteristics of open medium, dynamic topology, absence of central authorities, distributed cooperation, and constrained capability. Routing security plays an important role in the security of the entire network. In general, routing security in wireless networks appears to be a nontrivial problem that cannot easily be solved. It is impossible to find a general idea that can work efficiently against all kinds of attacks, since every attack has its own distinct characteristics.

EXISTING SYSTEM

DSR involves two main processes route discovery and route maintenance. To execute the route discovery phase, the source node broadcasts a Route Request (PREQ) packet through the network, If an intermediate node has routing information to the destination in its route cache, it will reply with a PREQ to the source node. When the PREQ is forwarded to a node, the node adds its address information into the route record in the PREQ packet. When destination receives the PREQ, it can know each intermediary node’s address among the route, The destination node relies on the collected routing information among the packets in order to send a reply PREQ message to the source node along with the whole routing information of the established route.

DISADVANTAGES

Increase time delay.

It takes more energy for detecting malicious nodes.

Low energy efficiency.

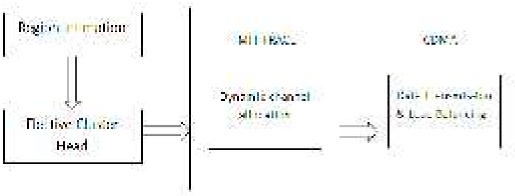
METHODOLOGY:

PROPOSED SYSTEM

In this project we propose two algorithms to cope with the non-uniform load distributions in MANETs: a light weight distributed dynamic channel allocation (DCA) algorithm based on spectrum sensing. We apply these two algorithms for managing non-uniform load distribution in MANETs into an energy efficient real-time coordinated MAC protocol, named MH-TRACE. In MH- TRACE, the channel access is regulated by dynamically selected cluster heads (CHs). MH-TRACE has been shown to have higher throughput and to be more energy efficient compared to CSMA type protocols. Although MH-TRACE incorporates spatial reuse, it does not provide any channel borrowing or load balancing mechanisms and thus does not provide optimal support to non-uniform loads.

ADVANTAGES

Increase the throughput Here we use scalable approach Reduce energy consumption Trust based transmission. Uniform data sharing


Region Formation
Relative Cluster Head
MH-TRACE
Dynamic channel allocation
CDMA
Data Transmission & Load Balancing

ARCHITECTURE DESIGN

MODULES DESCRIPTION LIST OF MODULES

Region Intimation Elective Cluster Head Dynamic Channel Allocation
Data Transmission &Load Balancing
Region Intimation

In the region each node sends ‘hello’ message to other nodes which allows detecting it. Once a node detects ‘hello’ message from another node (neighbor).It maintains a contact record to store information about the neighbor. Nodes do not know their respective region. So we need to intimate the region to the nodes.

Elective Cluster Head

The channel resources are managed and distributed by cluster head (CH). It can be ordinary nodes that are selected to perform the duty, or that can be specialized nodes. The channel needed to the nodes in the network for their transmission is provided by these cluster head. We have to select cluster based on memory, battery and mobility which is having high value and assign them as cluster head.Data Transmission&Load Balancing.In Dynamic channel allocation algorithm the channel controller monitors the power level in all the available channels in the network. If the load on the channel controller increases beyond capacity and measured power level is low, then the channel coordinator send request to other region of channel coordinator, if other region channel coordinator having capacity, then using CSMA protocol it will send acknowledgement. If cluster head receive the acknowledgement it will send that to nodes. Then we can send data from one node to other node within region and also outside the region by splitting a data into packet and send to other region destination nodes. The load on the channel coordinators originate from the demands of the ordinary nodes. Many nodes in a network have access to more than one channel load balancing algorithm is that the active nodes can continuously monitor the load of the channel coordinators and switch from heavily loaded coordinators to the one with available resources. These nodes can detect the depletion of the channels at the coordinator and shift their load to the other coordinators with more available resources. The resources vacated by the nodes that switch can be used for other nodes that do not have access to any other Channel coordinators. Thus time consumed for waiting can be minimized.

Dynamic Channel Allocation

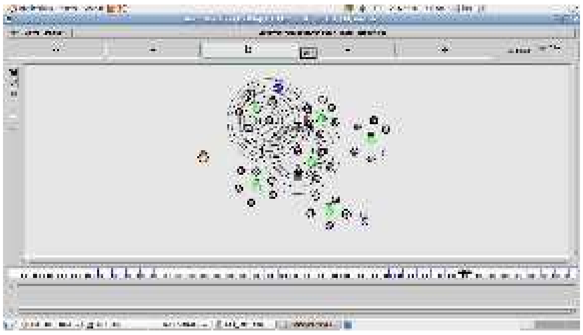
In MH-TRACE certain nodes assumes the roles of channel coordinator, here called cluster head. All cluster head send out periodic beacon packets to announce their presence to the nodes in their neighborhood

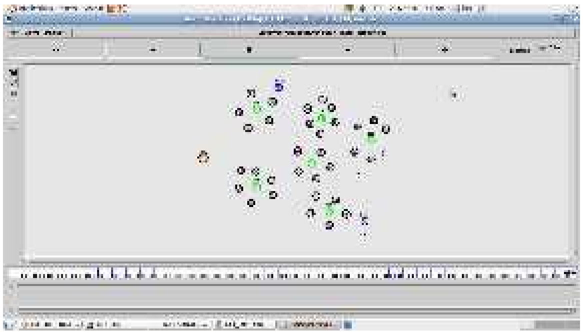
.when a node does not receive a beacon packet from any cluster head for a predefined amount of time, it assumes the role of a channel coordinator. In MH-trace this is divided in to super frame, is repeated in time and further divided into frames. Each cluster head operates one of the frames in super frame. In this frame cluster head maintains the capacity level of all channels. In this algorithm, the channel controllers continuously monitor the power level in all the available channels in the network and assess the availability of the channels by comparing the measured power levels with a threshold. If the load on the channel controller increases beyond capacity, provided that the measured power level is low enough, the channel coordinator starts using an additional channel with the lowest power level measurement

RESULT:

Thus the simulation output of the secure and efficient optimization for cluster based wireless sensor networks is given by,

SIMULATION OUTPUT





REFERENCE

[1] P.-C. Tsou, J.-M. Chang, H.C. Chao, and J.L. Chen, “CBDS:A Cooperative Bait Detection Scheme to prevent malicious node for MANET based on hybrid defense architecture,” in proc. 2nd Intl. Conf. Wireless Commun.,VITAE, Chennai, India, Feb.28-Mar., 03,2011,pp. 1-5.

[2] S. Marti, T.J. Giuli, K. Lai, and M. Baker, “Mitigating routing misbehavior in mobile ad hoc networks,” in proc. 6th Annu. Intl. Conf. Mobicom, 2000, pp. 255-265.

[3] S. Corson and J. Macker, RFC 2501, Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations, Jan. 1999. (Last retrieved March 18, 2013)[Online]. Available:http://www.elook.org/computing/rfc/rfc2501.html.

[4] C. Chang, Y. Wang, and H. Chao, “An efficient Mesh-based core multicast routing protocol on MANETs,” J. Internet Technol., vol. 8, no.2, pp. 229-239, Apr. 2007.

[5] K. Vishnu and A. J Paul, “Detection and removal of cooperative black/gray hole attack in mobile ad hoc networks,” Intl. J. Comput. Appl., vol. 1, no.22, pp. 28-32, 2010.

[6] H. Deng, W. Li, and D. Agarwal, “Routing security in wireless ad hoc network,” IEEE Commun. Mag.,vol. 40, no.10, Oct.2002.

[7] S. Ramaswamy, H. Fu, M. Srekantaradhya, J. Dixon, and K. Nygard,”Prevention of cooperative blackhole attacks in wireless ad hoc networks,” in Proc. Int. Conf. Wireless Netw.,Jun. 2003,pp. 570-575.

[8] H. Weerasinghe and H. Fu, “Preventing cooperative blackhole attacks in mobile ad hoc networks: Simulation implementation and avaluation,” in Proc. IEEE ICC, 2007, pp. 362-367.

[9] I. Rubin, A. Behzad, R. Zhang, H. Luo, and E. Caballero, “TBONE: A mobile- backbone protocol for ad hoc wireless networks,” in proc. IEEE Aerosp. Conf.,2002, vol. 6, pp. 2727-2740.

[10] Y. Xue and K. Nahrstedt, “Providing fault-tolerant ad hoc routing service in adversarial environments,” Wireless Pers. Commun, vol. 29, pp. 367-388, 2004.