International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 07 | July-2016 www.irjet.net p-ISSN: 2395-0072

Efficient and Situation aware Channel Allocation Mobile ad hoc Networks

U. Prem Sagar, V.Bhargavi, Asst.Professor

U.Prem Sagar, PG Scholar, Dept, of CSE, CREC, Tirupati, AP, India
V.Bhargavi, Asst.Professor, Dept. of CSE, CREC, Tirupati, AP, India

Abstract:

A mobile ad hoc network (MANET) is a continuously self-configuring, infrastructure-less network of mobile devices connected without wires. Every device in a MANET is free to move independently in any direction, and can change its links to other devices frequently. In general MAC protocol for wireless networks can be classified as coordinated and uncoordinated MAC protocol. In uncoordinated protocol nodes contend with each other to share the common channel. In this paper lightweight dynamic channel allocation mechanism and a cooperative load balancing strategy are introduced that are applicable to cluster based MANETs to address this problem. We present protocols that utilize these mechanisms to improve performance in terms of throughput, energy consumption and inter-packet delay variation, bandwidth efficiency in MANET. exist in infrastructure based coordinated protocols. In this paper, 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. We present protocols that utilize these mechanisms to improve performance in terms of throughput, energy consumption and inter-packet delay variation It is crucial for the Medium access control of a MANET not only adapt to the dynamic environment but also to efficiently manage bandwidth utilization.

Key Words: Load balancing, dynamic channel allocation, Mobile adhoc network.

1. INTRODUCTION

A Mobile Ad Hoc Network (also called MANET) is a collection of portable devices that establishcommunication without the help of any infrastructure or established communication backbone. Furthermore, Mobile Ad hoc networks- Do not need backbone infrastructure support, Are easy to deploy, Useful when infrastructure is absent, destroyed or impractical also MANET is used manyapplications, such as, Military environments, Soldiers, tanks, planes, taxi cab network, Emergencyoperations, search, rescue, policing etc. Each device in a MANET is free to move independently inany direction, therefore change its links to other devices over and over again. Characteristics ofmobile ad-hoc network are self-organizing, multi-hopping, mobility, scalability, security, energyconversation and autonomous devises which makes MANET suitable for up-coming needs alsoadds complexity to the protocols to be each device to continuously maintain the information required to properly route load.Multicasting is a type of delivering messages from one node to set of nodes simultaneously inefficient manner . In the multicasting process the message is transmitted only once (noretransmission) over the network and is duplicated only at the branch point. It reduces thebandwidth consumption in network, which is possible in videoconferencing and distributedgaming like environment, where the same channel is accessed by many users. The protocols sending multicasting can be categorized in two types 1) Source Based Multicasting Protocols (ADMR,MAODV) and 2) Mesh Based Multicasting Protocols (ODMRP, CAMP). Duringtransmission messages can be stolen and altered or services disruption is also possible in thenetwork; which is called attack. There are many types of attack: 1) Active attack where intentionis to alter the information and make the network overload, 2) Passive attack where intention is tosteal the

message and eavesdrop on the communication, 3) Impression attack which is alsoknown as spoofing where attacker assumes the identity of another node in the network, so thatreceiving messages directed to the node it fakes, 4) Sinkhole attack where a compromised nodetries to attract the data to itself from all neighboring nodes using loopholes in routing algorithmsand 5) Wormholes attacks where a malicious node uses a path outside the network to routemessages to another compromised node at some other location in the network Transmitter .The rest of paper is organized as follows

2. RELATED WORK

In this section we discuss related work in the field of malicious attack in adhoc and wirelessnetwork in concern of security and power utilization. Patroklosg ,Argyroudis and DonaloMahonyentitled "secure routing for mobile ad hoc networks. The assumption of a trusted environment isnot one that can be realistically expected; hence, several efforts have been made toward the design of a secure and robust routing protocol for ad hoc networks. Although the authors mention challenges such as quality of service support and location-aided and power-aware routingapproaches, there is no mention of security considerations. Detection of Routing Misbehavior in manets" 2ACK scheme that serves as an add-on techniquefor routing schemes to detect routing misbehavior and to mitigate their adverse effect is proposed The main idea of the 2ACK scheme is to send two-hop acknowledgment packets in theopposite direction of the routing path. In order to reduce additional routing overhead, only afraction of the received data packets are acknowledged in the 2ACK scheme, called RADAR, to detect anomalous mesh nodes in wireless mesh network is proposed. RADAR scheme provides features for evaluate each node's behavior by abstracting and examining appropriate observations using reputation and captures the node's behavior drifts interms of reputation by exploring their temporal and spatial properties respectively. Scheme to Defend Against Cooperative Black Hole Attacks in Optimized Link State Routing Protocol" a problem of cooperative black hole attack is proposed. Cooperative black holeattack results in dramatic disruption of the network performance. An acknowledgment basedscheme to detect malicious nodes and isolate them from the forwarding process .

A Dynamic Anomaly Detection Scheme for AODV-Based Mobile Ad Hoc Networks" a new anomaly-detection scheme based on a dynamic learning process that allows thetraining data to be updated at particular time intervals is proposed [5]. This dynamic learning process calculates the projection distances based on multidimensional statistics using weightedcoefficients and a forgetting curve.

"AWF-NA: A Complete Solution for Tampered Packet Detection in VANETS" a novel schemecalled Autonomous Watchdog Formation is proposed [6]. Autonomous Watchdog Formation isenabled by 2-hop Neighborhood Awareness (AWF-NA), to ensure nodes automaticallyfunctioning as watchdogs to monitor the behaviors of the relaying nodes.[7] et.at. In packetdropping attack is a node denies to corporate or forwards each other's packet to save its resources or disrupt the communication. [8]Trust is a degree of belief about behavior of a particular entity. various design concepts to develop a MANET trust management system. Suggestions include that trust metric must have unique properties of trust, a trust managementdesign must support cognitive functionality for each node to achieve adaptability to changingnetwork conditions, a trust management system should be situation specific or situation aware, atrust management design must allow optimal settings to be identified under various network and environmental conditions so as to maximize the overall trust of the sys-tem for successful mission
executions.

3.SECUREDROUTINGPROTOCOL

The secured routing protocol play important role in mobile ad hoc network. Secured routing
protocol defended the attack such as worm whole attack, black hole attack and other internal

andexternal attack. In modification of on-demand routing protocol for prevention of attack, variousauthor are proposed a method such as EAODV (Enhanced on demand distance vector routingprotocol) and SBRP (secured backup routing protocol).SBRP is very efficient protocol forsecured communication in ad hoc network. The process of backup routing protocolexecutes in three phase. (1) Secured route discovery across the node (2) backup node setup (3)route maintenance across the node. The secured process takes time for execution of process ofSBRP protocol. The process of SBRP protocol are not energy efficient, but it is secured protocolagainst external and internal attack of ad hoc network. The process of activation of SBRPprotocol divided into three groups for energy saving mode such one is sleep mode, transit mode and active mode of action of node.

For the reduction of power consumption, we modified theactivation process of control message protocol according to sleep mode, transit state and activemode. The modified protocol acquired the process of thresholds priority Oder on the basic ofneighbor's node. The selection of neighbor node deepens on the mode operation in three sections.According to order of state create cluster of priority of group. After creation of group calculate
average threshold value, compare each group value with minimum threshold value, and pass thecontrol message for communication. Through this process mode of activation, state of node isminimized the time of route establishment and maintenance. The selection of proper node inminimum time and other node in sleep mode the consumption of power is reduces. We modifiedSBRP protocol for selection of node during on demand request node according to sleep andactivation mode of communication. Each node locally assigned priority value of node. activation group of node and denoted by GA. Having the same group at all nodes ensures thatsame average thresholds value. The node neighbor`s a and b are unaware that they have selected

4. RESULT ANALYSIS:-

For the effectiveness of some standard parameter for performance analysis.Throughput: It gives the fraction of the channel capacity used for useful transmission (Datapackets correctly delivered to the destination) and is defined as the total number of packetsreceived by the destination. It is in fact a measure of the effectiveness of a routing protocol .Average end-to-end delay: This includes all possible delays caused by buffering during routediscovery latency, queuing at the interface queue, retransmission delays at the MAC, andpropagation and transfer times[7].Packet delivery fraction: The ratio of the data packets delivered to the destinations to thosegenerated by the traffic sources [10]shows that throughput of our network simulation in given scenario for both protocol SBP and modified
SBP protocol. Throughput is calculated on the biases of packet delivery ratio to source to destination shows that the energy variation in both protocol SBP and Modified SBP routing protocol for given network parameter. The analysis of energy model gives a information about lifetime of network in giventime duration. The modified SBP routing protocol increase life time of network.

5. CONCLUSION

In this paper we modified the secured stateless protocol for secured routing and minimized the
utilization of power during path discovering and establishment. For the authentication of groupnode used group signature technique and sleep mode threshold concept for power minimization.The proposed algorithm divide node in two states sleep mode and active mode. The process ofgoing node sleep to active mode calculates priority of all sleep node and compare with arithmetic
mean of threshold. The value of sleep mode greater and equal to threshold thus acts as mastercommunication. Our experimental result shows maximum life time network in comparison torouting protocol. In future we also improved the key authentication mechanismn groupcommunication.

REFERENCES

[1] Patroklosg. Argyroudis AND Donalo'Mahony "secure routing for mobile ad hoc networks" in IEEE
Communication, 2005.

[2] Kejun Liu, Jing Deng, Pramod K. Varshney and KashyapBalakrishnan "An Acknowledgment-Based Approach for the Detection of Routing Misbehavior in MANETs" in IEEE Transaction, 2007.

[3] Zonghua Zhang, FaridNait-Abdesselam, Pin-Han Ho and Xiaodong Lin "RADAR:a ReputAtion based Scheme for Detecting Anomalous Nodes in WiReless Mesh Networks" in IEEE
Communications Society, 2008.

[4] SoufineDjahel, FaridNa¨it-Abdesselam and AshfaqKhokhar "An Acknowledgment-Based Scheme
to Defend Against Cooperative Black Hole Attacks in Optimized Link State Routing Protocol" in
IEEE Communications Society, 2008.

[5] Hidehisa Nakayama, Satoshi Kurosawa, Abbas Jamalipour,YoshiakiNemoto and Nei Kato "A Dynamic Anomaly Detection Scheme for AODV-Based Mobile Ad Hoc Networks" in IEEE
Transactions On Vehicular Technology, 2009.

[6] Zhengming Li, ChunxiaoChigan and Danniel Wong "AWF-NA: A Complete Solution for Tampered Packet Detection in VANETs" in IEEE Communications Society, 2008.

[7] SoufieneDjahel, FaridNait-abdesselam and Zonghua Zhang "Mitigating Packet Dropping Problem in
Mobile Ad Hoc Networks: Proposals and Challenges" in IEEE Communications Surveys, 2011.

[8] Jin-Hee Cho, Ananthram Swami and Ing-Ray Chen "A Survey on Trust Management for Mobile Ad
Hoc Networks" in IEEE Communications Surveys, 2011.

[9] Jian-Ming Chang, Po-Chun Tsou, Han-Chieh Chao and Jiann-Liang Chen "CBDS: A Cooperative
Bait Detection Scheme to Prevent Malicious Node for MANET Based on Hybrid Defense
Architecture" in IEEE Transaction, 2011.

[10] Ian F. Akyildiz, Xudong Wang and Weilin Wang "Wireless mesh networks: a survey" in Science