iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 3 **Issue:** VIII **Month of publication:** August 2015

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

An Efficient Anonymity Protection Technique Using Attribute Based Encryption in Mobile AdHoc Networks

N. Karthika[1], S.Ranilakshmi[2]
[1]*MPhil Scholar, Department Of computer science*
Dr.SNS Rajalakshmi college of Arts& science
[2]*Assistant Professor, Department of Information Technology, computer Technology*
Hindustan College of Arts & Science

Abstract – MobileAdhoc Network represents complex distributed and decentralized system which leads to secure issues in the routing, many existing Anonymous routing protocols relying on either hop-by-hop encryption has proposed to secure data sources, destinations, and routes. The computation cost and transmission delay of the anonymous protocol has to led to high constraint problem, to represent a effective transmission in the MANET against the security proposals, we propose an efficient anonymity protection technique named Attribute Based Encryption for data security. Proposed System initially divides network field into zones and randomly chooses nodes in zones as intermediate relay nodes to establish a non distinguishable anonymous route. In addition, it hides the packet header and payload of the data to strengthen source and destination anonymity protection. Hence system offers anonymity protection to sources, destinations, and routes. It also has strategies to effectively counterpart against intersection and timing attacks. Hence, experimental results proves that use anonymous routing protocols that hide node identities and/or routes from outside observers with less computation and transmission ..
Index terms: Location Preserving, , MANET, DDOS Attack, Eavesdropping Attack, packet dropping, Anonymization

I. INTRODUCTION

Rapid Development of the Mobile ad hoc networks (MANETs) are usually formed by a group of mobile nodes, interconnected via wireless links with features of self organizing and independent infrastructure, which agree to cooperate and forward each other's packets. One of the basic assumptions for the design of routing protocols in MANETs is that every node is honest and cooperative. That means, if a node claims it can reach another node by a certain path or distance, the claim is trusted/true; similarly, if a node reports a link break, the link will no longer be used. While this assumption can fundamentally facilitate the design and implementation of routing protocols, it meanwhile introduces a vulnerability to several types of denial of service (DoS) attacks, eaves dropping attack particularly packet dropping attack. To launch such attack, a malicious node can stealthily drop some or all data or routing packets passing through it. Due to the lack of physical protection and reliable medium access mechanism, packet dropping attack represents a serious threat to the routing function in MANETs using ALERT and Alarm security protocols[12][13]. On other hand limited attack resource can easily join the network and compromise a legitimate node then subsequently start dropping packets that are expected to be relayed in order to disrupt the regular communications. Consequently, all the routes passing through this node fail to establish a correct routing path between the source and destination nodes. ALERT is an on secure routing protocol [3], [4]. In ALERT, the network is completely self-organizing and self configuring, without the need for any existing network infrastructure. The protocol is composed of the two mechanisms: route discovery and route anonymization, which allows nodes to discover and maintain source routes to arbitrary destinations in the ad hoc network in secured manner [3]. ALERT maintains a route cache which keeps track of all the routes. When a node needs to send a packet to a destination it first checks its cache if it already knows a route to the destination. If the route to destination is not available in the route cache then route discovery mechanism is initiated. Route Discovery allows any host in the ad hoc network to dynamically discover a route to any other host in the ad hoc network [3]. A route reply is sent back either if the RREQ packet reaches the destination node itself, or if the RREQ reaches an intermediate node which has an active route to the destination in its route cache. The Route Maintenance procedure keeps check on the operation of the routes and informs the sender of any routing errors. Due to very high probability of routes being lost, Proactive protocols are traditionally classified as either distance-vector or link-state protocols[13][14]. The former are based on the

distributed Bellman-Ford (DBP) algorithm [22], which is known for slow convergence because of the "counting-to-infinity" problem. To address the problem, ABE based Data preserving, an Anonymous routing protocol ,the Destination-Sequenced Distance-Vector routing (DSDV)[7] [4] protocol was proposed for ad-hoc networks. On the other hand, link-state protocols, as represented by OSPF [3][8], have become standard in wired IP networks. They converge more rapidly, but require significantly more control traffic. Since ad-hoc networks are bandwidth limited and their topology changes often, an Optimized Link-State Protocol (OLSR) [5] has been proposed. While being suitable for small networks, some scalability problems can be seen on larger networks. The need to improve convergence and reduce traffic has led to algorithms that combine features of distance-vector and link-state schemes. Such a protocol is the wireless routing protocol (WRP) [6], which eliminates the counting-to-infinity problem and avoids temporary loop without increasing the amount of control traffic. [1] [10].To complement those efforts, this work studies the packet dropping attack, which is known as one of the most destructive threats in MANETs, and illustrates in depth the different schemes used by adversaries targeting on both reactive and proactive protocols using Attribute based Encryption to enhance the security in the Network path by employment of Anonymization principles to the specific attribute of the Request packet and routing information Table- routing table.. Furthermore, we conduct an up-to-date survey of the most valuable contributions aiming to avoid the packet droppers. The careful examination and analysis has allowed us to carry out a comparative study of the existing security schemes in terms of specific design rationale and objectives. The ultimate goal is to identify the strengths and weaknesses of each scheme in order to devise a more effective and practical solution which can achieve a better trade-off between security and network performance. The remainder of the paper is structured as follows. In section 2, we discuss related works of the Routing protocols in MANETs. Section 3 describes the proposed attribute based encryption technique for location preserving and efficient routing. Experimental evaluation of the proposed system is presented in the Section 4. Finally, section 5 concludes the work and points out future research directions.

A. DSR Protocol

Dynamic Source Routing is a protocol developed for routing in mobile ad-hoc networks and was proposed for MANET [6][9]. In a nutshell, it works as follows: Nodes send out a ROUTE REQUEST message, all nodes that receive this message put themselves into the source route and forward it to their neighbors, unless they have received the same request before. If a receiving node is the destination, or has a route to the destination, it does not forward the request, but sends a REPLY message containing the full source route. It may send that reply along the source route in reverse order or issue a ROUTE REQUEST [21] including the route to get back to the source, if the former is not possible due to asymmetric links. ROUTE REPLY messages can be triggered by ROUTE REQUEST messages or are gratuitous. After receiving one or several routes, the source selects the best (by default the shortest), stores it and sends mess ages along that path. The better the route metrics (number of hops, delay, bandwidth, or other criteria) and the sooner the REPLY arrives at the source, the higher the preference given to the route and the longer it will stay in the cache. When a ROUTE REPLY arrives very quickly after a ROUTE REQUEST has been sent out this is an indication of a short path, since the nodes are required to wait for a time corresponding to the length of the route they can advertise, before sending it. This is done in order to avoid a storm of replies. In case of a link failure, the node that cannot forward the packet to the next node sends an error message towards the source. Routes that contain a failed link can be `salvaged' by taking an alternate partial route that does not contain the bad link. Since DSR has no security mechanism they are vulnerable to much type of attacks. It assumes all nodes cooperate in the network so in its present status cannot defend itself from attacks.

B. Reactive Routing Protocols

Reactive Routing Protocols are also called on demand routing. It is more efficient than proactive routing. The main idea behind this type of routing is to find a route between a source and destination whenever that route is needed which helps to avoid routing overhead[20], whereas in proactive protocols we were maintaining all routes without knowing its state of use. So in reactive protocols it is not needed to maintain the routes which are not being used currently. This type of routing is on demand. On demand routing protocols [17], [18], [19] avoids the cost of maintaining routes that are not being used.

C. ALERT Protocol

ALERT dynamically partitions the network field into zones and randomly chooses nodes in zones as intermediate relay nodes, which form a nontraceable anonymous route. In addition, it hides the data initiator/receiver among many initiators/receivers to strengthen source and destination anonymity protection. Thus, ALERT offers anonymity protection to sources, destinations, and

routes. It also has strategies to effectively counter intersection and timing attacks.

II. PROPOSED SOLUTION

A. Network Model

We construct and Mobile Ad hoc Networks with several node. Each node in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger Internet. Because of the infrastructure-less architecture of MANET[11], our risk-aware response system is distributed, which means each node in this system makes its own response decisions based on the evidences and its own individual benefits. Therefore, some nodes in MANET may isolate the malicious node, but others may still keep in cooperation with due to high dependency relationships.

B. Attack Models

1) Modelling Packet Dropping Attacks: Before analyzing the packet dropping attack in details, let us first summarize the different motives that incite some nodes to drop a packet rather than sending or relaying it. In general, a packet can be dropped at either MAC or network layers due to the following reasons:

The size of packets' transmission buffer at MAC level is limited; therefore whenever the buffer is full any new packet arriving from higher layers will be dropped (buffer overflow).
IEEE 802.11 protocol's [4] rules: a data packet is dropped if its retransmission attempts or the one of its corresponding RTS (Request To Send) frame has reached the maximum allowed number, owing to node's movement or collision (a lot of contending nodes).
A data packet may be dropped or lost if it is corrupted during transmission due to some phenomenon specific to radio transmissions such as interference, hidden nodes and high bit error rate.
2) Modelling Black Hole Attack: The black hole attack in MANETs can be classified into several categories in terms of the strategy adopted by the malicious node to launch the attack. In particular the malicious node can intentionally drop all the forwarded packets going through it (black hole), or it can selectively drop the packets originated from or destined to certain nodes that it dislikes. In order to launch a black hole attack, the first step for a malicious node is to find a way that allows it to get involved in the routing/forwarding path of data/control packets. To do so, it exploits the vulnerabilities of the underlying routing protocols which are generally designed with strong assumption of trustworthiness of all the nodes participating in the network. Thus in fig.1 any node can easily misbehave and provoke a severe harm to the network by targeting both data and control packets. Dropping data packets leads to suspend the ongoing communication between the source and the destination node. More seriously, an attacker capturing the incoming control packets can prevent the associated nodes from establishing routes between them. To facilitate understanding, we illustrate them using representative routing protocol in MANETs.

3) Modelling DDOS Attack : DDOS attack is an attempt to make a node unavailable for data transfer in the MANET. DDOS control the node transmission by heavy utilizing the bandwidth of the transmission path . Packet is hindered with high redundant data and RREQ .Attacking node exploits the node communication capabilities entirely.

C. Distinguishing The Network

Partitioning is carried out with help of the routing table
Routing table recovery includes local routing table recovery and global routing recovery. Local routing recovery is performed by victim nodes that detect the attack and automatically recover its own routing table. Global routing recovery involves with sending recovered routing messages by victim nodes and updating their routing table based on corrected routing information in real time by other nodes in MANET [16]. Routing table recovery is an indispensable response and should serve as the first response method after successful detection of attacks.

D. Location Preserving Technique (Attribute Based Encryption)

Our adaptive Strategies for packet preserving to insertion attack and timing attack is established as follows, the response level is

additionally divided into multiple bands. Each band is associated with an isolation degree, which presents a different time period of the isolation action. The response action and band boundaries are all determined in accordance with risk tolerance and can be changed when risk tolerance threshold changes. The risk tolerance thresholds could also be dynamically adjusted by another factors[15], such as attack frequency. If the attack frequency is high, more severe response action should be taken to counter this attack. Our risk-aware response module could achieve this objective by reducing the values of risk tolerance threshold and narrowing the range between two risk tolerance thresholds.

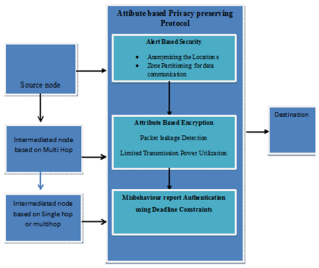


Figure 1: Proposed Architecture of the Anonymization Protocol

1) Algorithm – ABE – Location Preserving Technique

Hierarchical zone Partitioning carried out with vertical and horizontal portioning until source and destination not lies in same node

Z_d= Destination Zone

TD = Temporary Destination is randomly chosen in another zone to the Source in different zone

Destination node is calculated based on the node density and No. of nodes" H"

RF =Random Forwarder is Calculated using ALERT Protocol

Attribute based encryption is carried for Table like Data

2. Sentence level encryption and Paragraph level encryption is carried for the text based data.

Verification of Cipher Text based on the Policy assignment and Domain users

Where p= Domain and L = data

If (p= Key && L= Cipher Text)

Authenticate the Attributes to access the data

Create a write and read access related to signature Assigned

Generate ()

PUD is Used to evaluated based on Cipher text and key (license)

FEK (file Encryption Key can be Disclosed to all Domain user) in terms of Domain and PUD

Break glass Access is Established through hash chain terminating

Revoke ()

III. EXPERIMENTAL RESULTS

In order to evaluate our schemes, we performed simulations using network simulator version 2 (NS-2). NS-2 is a very popular network simulation tool. It uses C language for protocol definition and TCL scripting for building the simulation scenarios.

A. Packet Delivery Ratio

It is the average time taken by a data packet to arrive in the destination. It also includes the delay caused by route discovery process and the queue in data packet transmission. Only the data packets that successfully delivered to destinations that counted.

∑ (arrive time – send time) / ∑ Number of connections. The lower value of end to end delay means the better performance of the protocol.

1) End To End Delay Of The Packet Transmission

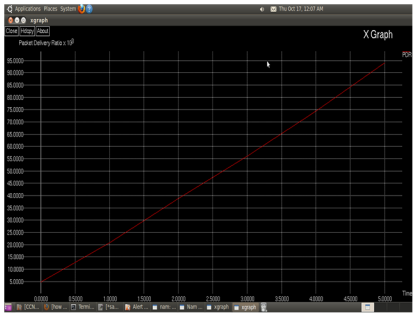


Figure4.1: Packet Delivery ratio of the Packet Transferring

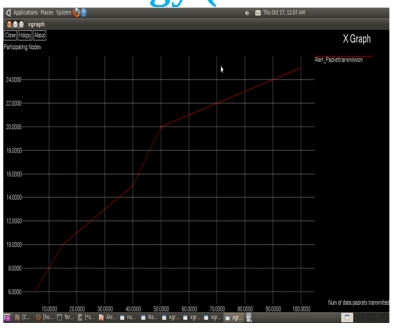
Proposed system has performed against the security attacks and produces the network properties of throughput and latency.

Technique (Algorithm)	File Size in kb	No. of Packets (segments)	Packet loss ratio
ALARM	500	500	2.5
ALERT	500	500	1.58
ABE-Proposed	500	500	1.8

Table 4.1: Performance of the Technique against packet classification attack

Attack Detection rate = 10-(Actual Characteristics of the nodes – Attack models).

Characteristics of the nodes ---→ attack Models + monitoring system w.r.t dynamic changes.



Attack Model----.> set of the desired samples of attacks

Figure 4.2: Throughput of the Packet Transmission

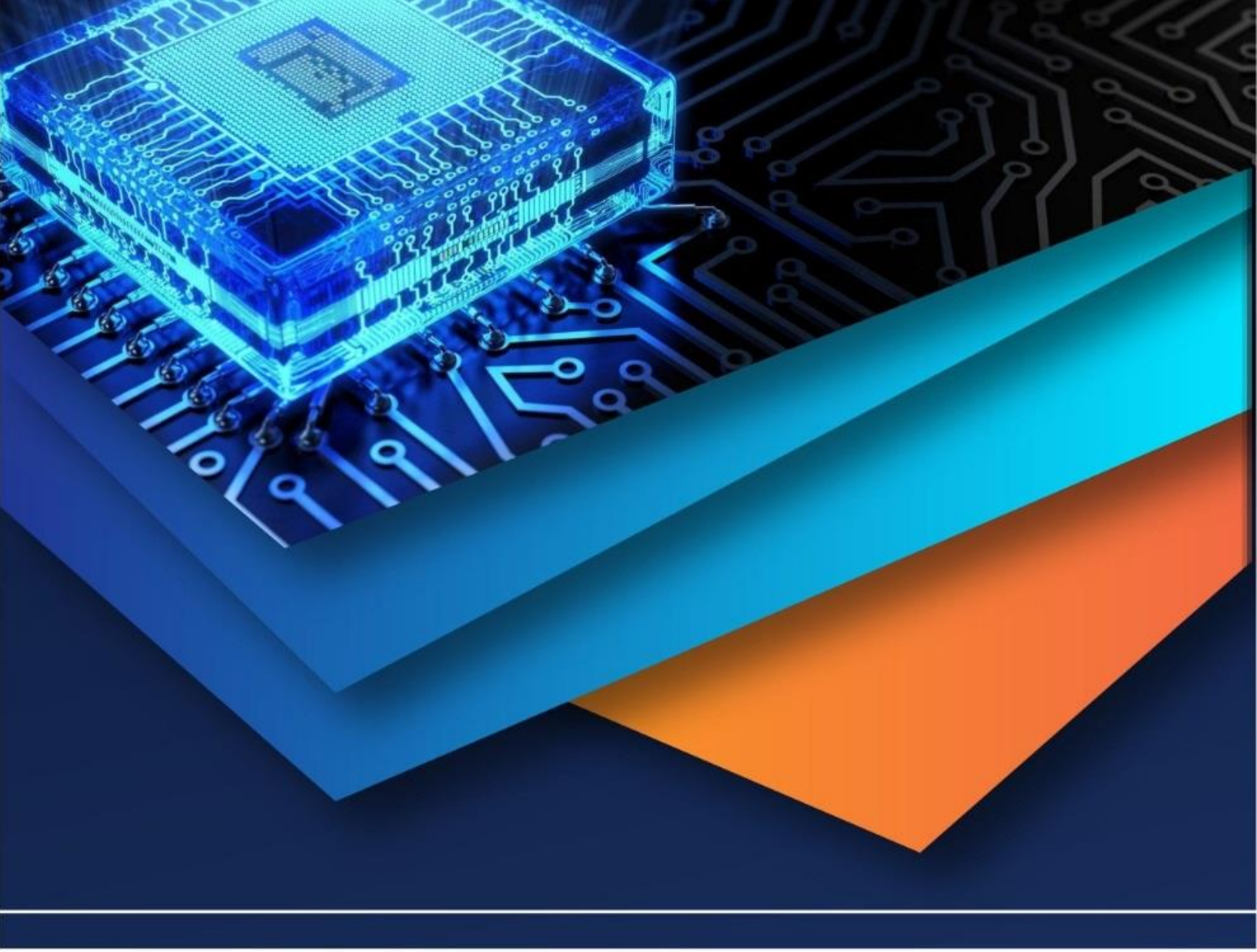
IV. CONCLUSION

We implemented Attribute based Encryption technique for location preserving and data preserving A Preserving confidentiality of physical layer attribute for packet transmission is high importance against the selective jamming attacks. In this work, we analysed the problem of network path security against DDOS to target packets. The System is been secured against the eaves dropping and Black Hole Attacks. Performance evaluation of the system proves that secure configuration of the MANET yields good outcomes in terms of Transmission rate and packet Delivery Ratio ratios. Many Solutions could be suggested for the future work through employment of Hash mapping techniques which results in more security of the defence application.

REFERENCES

[1] A. Pfitzmann, M. Hansen, T. Dresden, and U. Kiel, “Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management a Consolidated Proposal for Terminology, Version 0.31,” technical report, 2005.
[2] Sk.Md.M. Rahman, M. Mambo, A. Inomata, and E. Okamoto, “An Anonymous On-Demand Position-Based Routing in Mobile Ad Hoc Networks,” Proc. Int’l Symp. Applications on Internet (SAINT), 2006.
[3] Z. Zhi and Y.K. Choong, “Anonymizing Geographic Ad Hoc Routing for Preserving Location Privacy,” Proc. Third Int’l Workshop Mobile Distributed Computing (ICDCSW), 2005.
[4] V. Pathak, D. Yao, and L. Iftode, “Securing Location Aware Services over VANET Using Geographical Secure Path Routing,” Proc. IEEE Int’l Conf. Vehicular Electronics and safety (ICVES), 2008.
[5] K.E. Defrawy and G. Tsudik, “ALARM: Anonymous Location- Aided Routing in Suspicious MANETs,” Proc. IEEE Int’l Conf. Network Protocols (ICNP), 2007.
[6] K.E. Defrawy and G. Tsudik, “PRISM: Privacy-Friendly Routing in Suspicious MANETs (and VANETs),” Proc. IEEE Int’l Conf. Network Protocols (ICNP), 2008.
[7] Y.-C. Hu, A. Perrig, and D.B. Johnson, “Ariadne: A Secure On- Demand Routing Protocol for Ad Hoc Networks,” Wireless Networks, vol. 11, pp. 21-38, 2005.
[8] I. Aad, C. Castelluccia, and J. Hubaux, “Packet Coding for Strong Anonymity in Ad Hoc Networks,” Proc. Securecomm and Workshops, 2006.
[9] C.-C. Chou, D.S.L. Wei, C.-C. Jay Kuo, and K. Naik, “An Efficient Anonymous Communication Protocol for Peer-to-Peer Applications over Mobile Ad-Hoc Networks,” IEEE J. Selected Areas in Comm., vol. 25, no. 1, pp. 192-203, Jan. 2007.
[10] X. Wu, “AO2P: Ad Hoc On-Demand Position-Based Private Routing Protocol,” IEEE Trans. Mobile Computing, vol. 4, no. 4, pp. 335-348, July/Aug. 2005.
[11] Tracy Camp, Jeff Boleng, Brad Williams, Lucas Wilcox, William Navidi, “Performance Comparison of Two Location Based Routing Protocols for Ad Hoc Networks” IEEE, vol 3, pp 1678-1687, 2002
[12] Qi Xue , Aura Ganz. “Ad hoc QoS on-demand routing (AQOR) in mobile ad hoc networks”, Journal of Parallel and Distributed Computing, vol. 63. Issue 2, pp. 154 – 165, 2003.
[13] C. Perkins, E. Belding-Royer, and S. Das, “Ad hoc On-demand Distance Vector (AODV) routing,” University of Cincinnati, Internet draft, July 2003
[14] Carlos de Morais Cordeiro and Dharma P. Agrawal, “Mobile Ad hoc Networking,” OBR Research Center for Distributed and Mobile Computing, ECECS, pp. 1-63, 2004.
[15] W. KieS, H. FuSler, and J. Widmer, “Hierarchical location service for mobile ad hoc networks” in Proc. ACM SIGMOBILE, vol. 8, no. 4, pp. 47-58, Oct.2004
[16] Harshavardhan Sabbineni, “Location-Aided Flooding: An Energy- Efficient Data Dissemination Protocol for Wireless Sensor Networks” IEEE TRANSACTIONS ON COMPUTERS, VOL. 54, NO. 1, JANUARY 2005
[17] Nen-Chung Wang , Si-Ming Wang, “An Efficient Location-Aided Routing Protocol for Mobile Ad Hoc Networks,” 11th International Conference, vol. 1, pp. 335-341, 2005.
[18] K. Akkaya, and M. Younis. "A survey on routing protocols for wireless sensor networks. Ad Hoc Networks," 3(3), pp. 325–349, May 2005.

[19] Sidi-Mohammed Senouci and Tinku Mohamed Rasheed, "Modified Location-Aided Routing Protocols for Control Overhead Reduction in Mobile Ad Hoc Networks", FIP — The International Federation for Information Processing, Volume 229, pp 137-146, 2007.
[20] P.T.V.Bhuvaneswari and V.Vaidehi, "Location Aided Energy Efficient Routing Protocol in Wireless Sensor Network," IJSSST, Vol. 11, No. 4, pp. 41-50, 2008.
[21] Tzay-Farn Shih , Hsu-Chun Yen, "Location-aware routing protocol with dynamic adaptation of request zone for mobile ad hoc networks", Journal, vol. 14, Issue 3, pp. 321-333, June 2008
[22] Mohammad A. Mikki, "Energy Efficient Location Aided Routing Protocol for Wireless MANETs," IJCSIS, vol. 4, No. 1 & 2, August 2009.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY