Energy Aware and Anonymous Location Based Efficient Routing Protocol

N.Nivethitha[1], G.Balaji[2]
[1]PG student,[2] Asst.Professor
Department of Electronics and Communication Engineering
Angel College of Engineering and Technology, Tirupur

***Abstract*- Mobile Ad Hoc Networks (MANETs) uses anonymous routing protocols that hide node identities and routes from outside observers in order to provide anonymity protection. However the existing routing protocols produces high cost. To provide High anonymity protection with low cost in MANET, we proposed Energy Aware ALERT (Anonymous Location Based Efficient Routing Protocol).It consider the energy level of each node in the network, and chooses a node which has highest energy as a intermediate relay node to increase the life time of the network and also provides secured anonymity protection to the source, destination and Routes. In energy-aware ALERT protocol E-GPSR is used to choose a high level energy node as a intermediate relay node. Experimental results exhibit consistency with the theoretical analysis, and show that Energy-aware ALERT achieves better route anonymity protection with lower cost compared to other anonymous routing protocols. Also, Energy-aware ALERT achieves comparable routing efficiency to the E-GPSR geographical routing protocol.**

***Keywords*- MANET, GPSR Algorithm, Anonymity Protection, E-GPSR Algorithm, Routing, ALERT**

I. INTRODUCTION

A mobile ad hoc network (MANET) is a dynamic distributed system of wireless nodes that move independently of each other. Rapid development of MANETs has stimulated numerous wireless applications that can be used in a wide number of areas such as commerce, emergency services, military, education, and entertainment. Anonymous routing protocols are crucial in MANETs to provide secure communications by hiding node identities and preventing traffic analysis attacks from outside observers. Routing protocols in MANETs can be classified into topology based and position based protocols. Topology based protocols are either proactive or reactive in nature. Proactive routing protocols determine and maintain routes between any pair of nodes irrespective of their requirement [1][2].

Existing anonymity routing protocols in MANETs can be mainly classified into two categories: hop-by-hop encryption and redundant traffic. Greedy Perimeter Stateless Routing (GPSR) [3] is a well known and most commonly used position based routing protocol for MANETs. GPSR works as follows: The source periodically uses a location service scheme to learn about the latest location information of the destination and includes it in the header of every data packet. If the destination is not directly reachable, the source node forwards the data packet to the neighbor node that lies closest to the destination. Such a greedy procedure of forwarding the data packets is also repeated at the intermediate nodes. In case, a forwarding node could not find a neighbor that lies closer to the destination than itself, the node switches to perimeter forwarding. With perimeter forwarding, the data packet is forwarded to the first neighbor node that is come across, when the line connecting the forwarding node and the destination of the data packet is rotated in the anti clockwise direction. The location of the forwarding node in which greedy forwarding failed (and perimeter forwarding began to be used) is recorded in the data packet. We switch back to greedy forwarding when the data packet reaches a forwarding node which can find a neighbor node that is away from the destination node by a distance smaller than the distance between the destination node and the node at which perimeter forwarding began.

During both greedy forwarding and perimeter forwarding, the energy available at the chosen neighbor node to forward the data packet is not considered. In networks of moderate and high density, greedy forwarding happens to be used more than 98% of the time and the need for perimeter forwarding is highly unlikely. For optimizing the greedy forwarding phase of GPSR, the energy available at the neighbor nodes of a forwarding node before deciding the next hop node for transmitting the data packet was considered. Accordingly, an energy aware version of GPSR (E-GPSR) was proposed which operates as follows: a forwarding node first determines a candidate set of neighbor nodes – the nodes that lie closer to the destination than itself. The weight of each such candidate neighbor node is then computed to be the sum of the fraction of the initial energy currently available at the neighbor node and the progress (i.e., the fraction of the distance covered between the forwarding node and the destination) obtained with the selection of the neighbor node. The candidate neighbor node that has the largest weight value is the chosen next hop node to receive the data packet. This procedure is repeated at every hop where greedy forwarding is possible. In case, greedy forwarding is not possible, similar to GPSR, E-GPSR switches to perimeter forwarding. The rest of the paper is organized as follows: Section 2 discusses the ALERT protocol used in MANETs. Section 3 discusses the performance evaluation. Section 4 describes the simulation environment and presents the simulation results. Section 5 concludes the paper and lists the future work.

II. ALERT PROTOCOL

ALERT can be applied to different network models with various node movement patterns such as random way point model [4] and group mobility model [5]. ALERT dynamically partitions a network field into zones and randomly chooses nodes in zones as intermediate relay nodes, which form a non traceable anonymous route. Specifically, in each routing step, a data sender or forwarder partitions the network field in order to separate itself and the destination into two zones. It then randomly chooses a node in the other zone as the next relay node and uses the GPSR [6] algorithm to send the data to the relay node. In the last step, the data is broadcasted to k nodes in the destination zone, providing k-anonymity to the destination. In addition, ALERT has a strategy to hide the data initiator among a number of initiators to strengthen the anonymity protection of the source. ALERT is also resilient to intersection attacks [7] and timing attacks [7]. Anonymity and efficiency of ALERT also theoretically analyzed.

A. *ZONE PARTITIONING*

For ease of illustration, we assume the entire network area is generally a rectangle. The information of the bottom-right and upper left boundary of the network area is configured into each node when it joins in the system. ALERT features a dynamic and unpredictable routing path, which consists of a number of dynamically determined intermediate relay nodes. As shown in the upper part of Fig. 1, given an area, we horizontally partition it into two zones A1 and A2. We then vertically partition zone A1 to B1 and B2. After that, we horizontally partition zone B2 into two zones. Such zone partitioning consecutively splits the smallest zone in an alternating horizontal and vertical manner. We call this partition process hierarchical zone partition. ALERT uses the hierarchical zone partition and randomly chooses a node in the partitioned zone in each step as an intermediate relay node (i.e., data forwarder), thus dynamically generating an unpredictable routing path for a message.

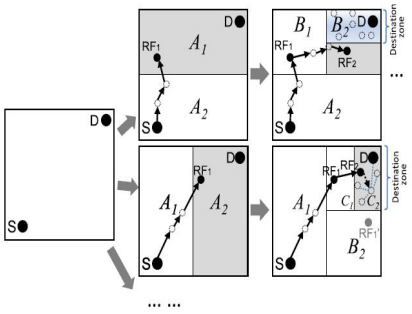

Fig 1. Examples of Different Zone Partitions

Fig. 2 shows an example of routing in ALERT. We call the zone having k nodes where D resides the destination zone, denoted as ZD. k is used to control the degree of anonymity protection for the destination. The shaded zone in Fig. 2 is the destination zone. Specifically, in the ALERT routing, each data source or forwarder executes the hierarchical zone partition. It first checks whether itself and destination are in the same zone. If so, it divides the zone alternatively in the horizontal and vertical directions. The node repeats this process until itself and ZD are not in the same zone. It then randomly chooses a position in the other zone called temporary destination (TD), and uses the GPSR routing algorithm to send the data to the node closest to TD. This node is defined as a random forwarder (RF). ALERT aims at achieving k-anonymity [8] for destination node D, where k is a predefined integer. Thus, in the last step, the data are broadcasted to k nodes in ZD, providing k-anonymity to the destination.

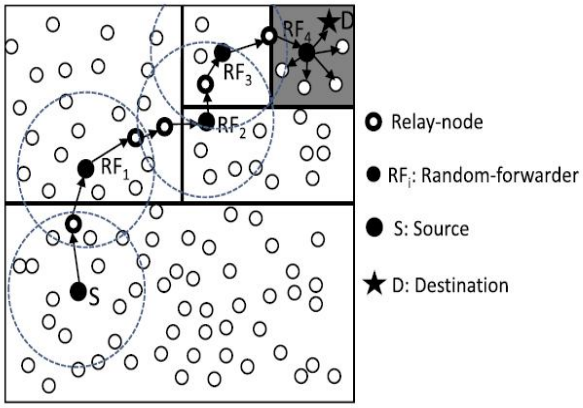

Fig 2. Routing Among Zones in ALERT

B. *GREEDY FORWARDING ALGORITHM USED IN E-GPSR*

Let (XD, YD) and (XF, YF) respectively denote the locations of the destination node D and the forwarding node F that has the data packet addressed to the destination node D.Pseudocode for Greedy forwarding algorithm used in E-GPSR is explained below. We first form a candidate set of neighboring nodes, Candidate-Neighbor-List (F), which is a subset of the Neighbor-List (F). For every neighbor I ξ Neighbor-List (F), I ξ Candidate-Neighbor-List (F), if and only if, the distance between the neighbor node I and the destination node D is less than the distance between the forwarding node F and D. For every neighbor node I ξ Candidate-Neighbor-List (F), we then compute a Weight (I), defined as the sum of the (a) fraction of the initial energy currently available at I, referred to as Residual Energy (I), and the (b) fraction of the distance covered with the potential

selection of I, referred to as Progress (F, I), which would be the difference in the distance between F and D and the distance between I and D divided by the distance between F and D. Among such neighbor nodes, the neighbor node that has the maximum Weight value is chosen by F as the next hop node to forward the data packet. If the forwarding node F could not find a neighbor node that lies closer to the destination than itself, the Candidate-Neighbor-List is empty and the node switches to perimeter forwarding.

Input: Forwarding Node F, Destination D, Neighbor-List (F)
Auxiliary Variables: Progress (F, I) where I ξ Neighbor-List (F)
Candidate-Neighbor-List (F), ResidualEnergy (I), AvailableEnergy (I), InitialEnergy (I), Weight(I), I ξ Candidate-Neighbor-List (F), Maximum-Weight
Output: Next-Hop-Node // if Greedy forwarding is successful
NULL // if Greedy forwarding is not successful and // perimeter forwarding is needed
Initialization: Next-Hop-Node = NULL; Maximum-Weight ← 0.0
Candidate-Neighbor-List (F) ← Φ
Begin E-GPSR Greedy Forwarding Algorithm
Distance F-D = $\sqrt{(XF - X\ D)2\ (YF - Y\ D)2}$
for every neighbor node I ξ Neighbor-List (F) **do**
Distance I-D =$\sqrt{(XF - X\ D)2\ (YF - Y\ D)2}$
if (Distance I-D < Distance F-D) **then**
Candidate-Neighbor-List(F) ←Candidate-Neighbor-List(F)U{I}
end if
end for
for every neighbor node I ξ Candidate-Neighbor-List (F) **do**
ResidualEnergy (I)=$AvailableEnergy(I)/InitialEnergy(I)$
Progress(F ,I)=$Distance$ F − D/$Distance$I − D
Weight (I) ← ResidualEnergy (I) + Progress (F, I)
if (Maximum-Weight < Weight (I)) **then**
Maximum-Weight = Weight (I)
Next-Hop-Node ← I
end if
end for
if (Maximum-Weight > 0.0) **then**
return Next-Hop-Node
else
return NULL
end if
End E-GPSR Greedy Forwarding Algorithm

Fig 3. Greedy forwarding Algorithm used in E-GPSR

III.PERFORMANCE EVALUATION

In this section, we provide experimental evaluation of the ALERT protocol, which exhibit consistency with our analytical results. Both prove the superior performance of ALERT in providing anonymity with low cost of overhead. Recall that anonymous routing protocols can be classified into hop-by-hop encryption and redundant traffic. We compare ALERT with two recently proposed anonymous geographic routing protocols: DSDV and AODV, which are based on hop-by-hop encryption and redundant traffic, respectively.

We use ns-2 (version 2.34) as the simulator for our study. We implemented the GPSR and E-GPSR protocols in ns-2. The network dimension used is a 1000m x 1000m square network. The transmission range of each node is assumed to be 250m. The number of nodes used is 50 and 100 nodes representing networks of moderate (on the average 10 neighbors per node) and high density (on the average 20 neighbors per node) respectively where greedy forwarding is predominantly more common over perimeter forwarding. We chose such network density conditions so that the impact of the energy-aware greedy forwarding technique on GPSR can be exploited to the maximum. The average network connectivity at these density values is more than 99% and greedy forwarding is used for at least 98% of the packets sent from each source node. Initially, nodes are uniform-randomly distributed in the network. We assume the availability of an off-line location service scheme through which the source node can learn the exact location of the destination node at the time of sending a data packet.

IV.SIMULATION RESULTS

The simulation result of average delay of the packet versus speed of Node is shown in Figure 4. This result also illustrates based on speed. The delay of the each packet is reduced in E-GPSR compared with other protocols. The simulation result of control overhead vs node density per Node is shown in Figure 5. This result denotes that the overhead of the each packet is reduced compared to other protocols. The simulation result of delivery rate of the packet vs Speed is shown in Figure 5. This shows that the delivery ratio of packet is improved compared with other protocols. The simulation result of throughput of the node is shown in Figure 6. This illustrates throughput of the each packet is improved compared with other protocols based on speed of the node. The simulation result of throughput of the packet vs speed of the node is shown in Figure 7. This shows that the throughput is increased compared with other protocols based on speed of the each packet. The simulation result of energy

consumption is shown in Figure 8.This illustrates E-ALERT consumes more power compared to other protocol.

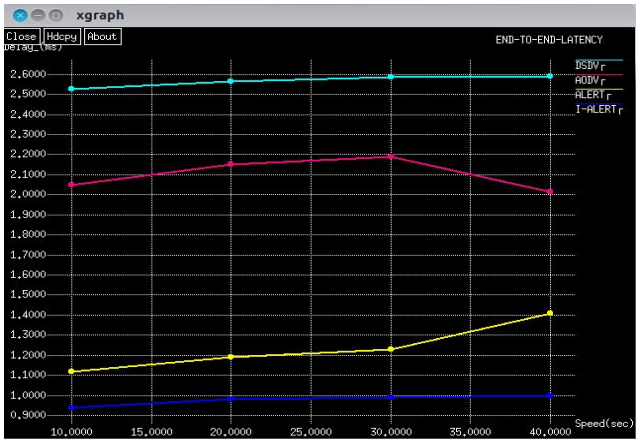

Fig 4.Performance of Average Delay Vs Speed

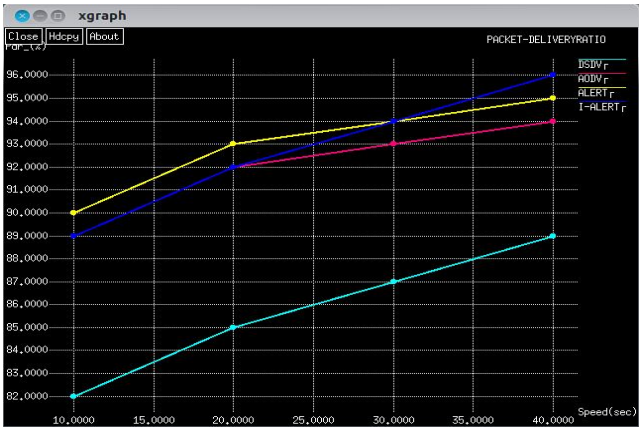

Fig 5.Performance of Packet Delivery rate Vs Speed

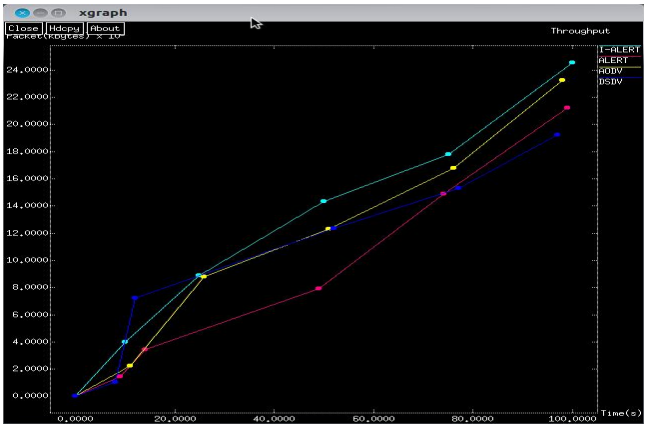

Fig 6.Performance of Throughput

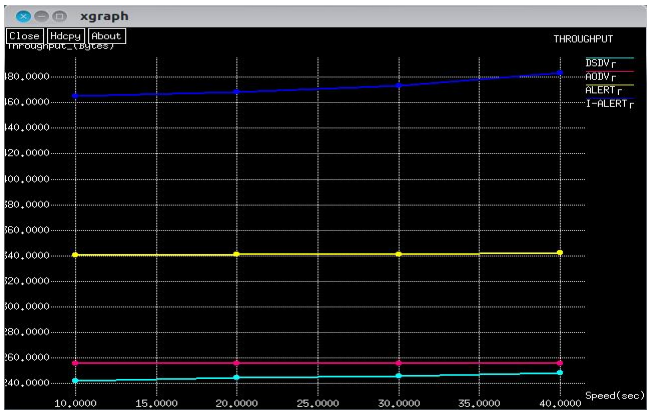

Fig 7.Performance of Throughput versus Speed

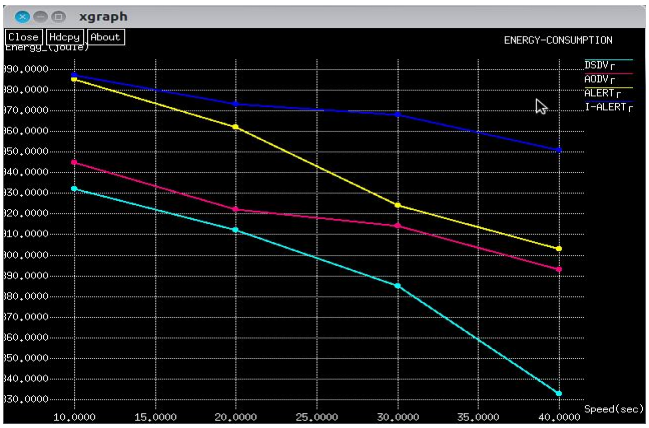

Fig 8. Performance of energy consumption

V.CONCLUSIONS AND FUTURE WORK

Previous anonymous routing protocols, relying on either hop-by-hop encryption or redundant traffic, generate high cost. Also, some protocols are unable to provide complete source, destination, and route anonymity protection. ALERT is distinguished by its low cost and anonymity protection for sources, destinations, and routes. It uses dynamic hierarchical zone partitions and random relay node selections to make it difficult for an intruder to detect the two endpoints and nodes en route. A packet in ALERT includes the source and destination zones rather than their positions to provide anonymity protection to the source and the destination. The time of first node failure for EGPSR could be as large as 55% more (compared to GPSR) for scenarios of low node mobility and high offered data traffic load. As node mobility increases, the relative difference between GPSR and E-GPSR with respect to the time of first node failure decreases. ALERT further strengthens the anonymity protection of source and destination by hiding the

data initiator/receiver among a number of data initiators/ receivers. It has the "notify and go" mechanism for source anonymity, and uses local broadcasting for destination anonymity. In addition, ALERT has an efficient solution to counter intersection attacks. ALERT's ability to fight against timing attacks is also analyzed. Experiment results show that ALERT can offer high anonymity protection at a low cost when compared to other anonymity algorithms. It can also achieve comparable routing efficiency to the base-line E-GPSR algorithm. Like other anonymity routing algorithms, ALERT is not completely bulletproof to all attacks. Future work lies in reinforcing ALERT in an attempt to thwart stronger, active attackers and demonstrating comprehensive theoretical and simulation results.

REFERENCES

[1] J. Broch, D. A. Maltz, D. B. Johnson, Y. C. Hu, J. Jetcheva, "A Performance Comparison of Multi-hop Wireless Ad Hoc Network Routing Protocols," *Proceedings of the 4th ACM Annual International Conference on Mobile Computing and Networking*, pp.85-97, Dallas, TX, USA, October 1998.

[2] P. Johansson, T. Larsson, N. Hedman, B. Mielczarek and M Degermark, "Scenario-based Performance Analysis of Routing Protocols for Mobile Ad hoc Networks," *Proceedings of the 5th ACM Annual International Conference on Mobile Computing and Networking*, pp. 195-206, Seattle, WA, USA, August 1999.

[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] T. Camp, J. Boleng, and V. Davies, "A Survey of Mobility Models for Ad Hoc Network Research," Wireless Communications and Mobile Computing, vol. 2, pp. 483-502, 2002.

[5] X. Hong, M. Gerla, G. Pei, and C.C. Chiang, "A Group Mobility Model for Ad Hoc Wireless Networks," Proc. Second ACM Int'l Workshop Modeling, Analysis and Simulation of Wireless and Mobile Systems (MSWiM), 1999.

[6] S. Ratnasamy, B. Karp, S. Shenker, D. Estrin, R. Govindan, L. Yin, and F. Yu, "Data-Centric Storage in Sensornets with GHT, a Geographic Hash Table," Mobile Network Applications, vol. 8, no. 4, pp. 427-442, 2003.

[7] J. Raymond, "Traffic Analysis: Protocols, Attacks, Design Issues, and Open Problems," Proc. Int'l Workshop Designing Privacy Enhancing Technologies: Design Issues in Anonymity and Unobservability (WDIAU), pp. 10-29, 2001.

[8] L. Sweeney, "k-Anonymity: A Model for Protecting Privacy," Int'l J. Uncertainity Fuzziness Knowledge-Based Systems, vol. 10, no. 5, pp. 557-570, 2002.