Advanced Location Based Efficient Routing in MANETs

[1]Nair SwatichandraChandrasekharan,[2]Manjusha Deshmukh
[1]M.E. Student, [2]Assistant Professor
[1]Information Technology Department,Pillai College of Engineering, New Panvel, Mumbai, Maharashtra, India
[2]Computer Engineering Department, Pillai College of Engineering, New Panvel, Mumbai, Maharashtra, India

***Abstract*—Mobile Ad Hoc Networks (MANETs) are a self–configuring and autonomous ad-hoc network which uses routing protocols which provides anonymity to the route through which the traffic flows, the data initiator and data receiver are hidden inorder to provide conservation from the adversaries which tries to track down the route or the crucial information's present in the network. There are plenty of routing protocols that provide anonymity but they depend on hop-by-hop encryptions or redundant traffic which ultimately leads to high price and they are not completely satisfying in contributing complete anonymity. In order to provide complete anonymity in a low price, an Advanced Location-based Efficient Routing in MANET (ALER) is proposed. It aims mainly in providing anonymity to the route, data sender and the data receiver. The network fieldis divided into several zones with the help of hierarchical partitioning and it is partition in a dynamical manner. Then nodes are selected randomly from the zones created from the hierarchical partition and as the nodes are arbitrarily choose to generate a non-traceable anonymous route.The proposed protocol also helps in hiding the sender and the destination also very efficiently. It also has strategies to effectively counter intersection, timing attacks. In this routing technique it has tried to overcome the Sybil attack issues which were not solved by the previous routing protocols.**

***IndexTerms*—Advanced Location-based Efficient Routing in MANET (ALER),AODV,Sybil attack,NS2,Hierarchical partition.**

I. INTRODUCTION

Now a day's Mobile Ad Hoc Networks (MANETs) has gained lots of attention and popularity due to its use in numerous areas like education, military, emergency hospital needs,entertainment and commerce which has stimulated numerous wireless applications. MANET poses some major features life organizing itself and independent infrastructure for using in communication and sharing of information. Because of the decentralization feature of MANETs, the nodes can be a member or can detach itself from the network as the network is infrastructure less. Nodes in MANETs are vulnerable to malicious entities; there major aim is to tamper the original information provided and analyzing the confidential data by eavesdropping or by attacking the routing protocol.

Anonymity is very much important and critical in military applications (e.g., soldier communication) although it's not required in civil oriented applications. Let us consider in a battle-field communication is done by establishing a MANET. Enemies can easily intercept the transmission of packets through traffic analysis by doing this they can easily track the positions of the soldiers (i.e. nodes), they can attack commander nodes and can easily block the data transmitted by comprising the relay nodes (RN). For establishing a secure communication providing anonymity in routing protocols is a better solution. The proposed routing protocol efficiently provides anonymity to the route, the data sender and the data receiver. Advanced location efficient routing protocol partitions the network field into multiple zones and then arbitrarily chooses a node in any of the zone and forms a route in order to deliver the packets from the sender to the destination. As the path is created using dynamic partitions adversaries finds it difficult to track the network traffic. Hence the end points are hidden and cannot be recognized as the path used is anonymous. Unlink ability is major strength of privacy protection i.e. source and destination cannot be associated with the packets in their communication by adversaries.There are mainly two anonymity routing techniques existing in MANETs the first one is hop-by-hop and the other one is redundant traffic. But both these method failed to provide complete anonymity protection. In order to which a new protocol came into existence and that is called as ALER, it is consider to give the maximum protection given to the sender and the destination nodes. A route is established anonymously by arbitrarily choosing nodes that acts as intermediate relay nodes and then AODV algorithm is used to forward the data packets.In the final step the data is transferred to 'k' number of nodes in the destination zone. Due to which it helps in providing anonymity in the destination zone.

II. LITERATURE SURVEY

Lot of researchers has done many effective works on MANET routing protocols. In this section we cite the relevant past literature that use the various protocols for routing in MANET and related work.

The paper [10], author Karim El Defrawy and Gene Tsudik proposed some captivating issues arising in such MANETs by designing an anonymous routing framework (ALARM).With the help of node location a map is established and based on this the node decides where the data should be forwarded further. Certain cryptographic methods are used to provide the constrained data integrity, data authenticity, anonymity and intractability.

Xiaoxin Wu and Bharat Bhargava proposed [14] an on-demand ad-hoc position-based private routing algorithm, named as AO2P, for providing anonymous communication. To determine the next best hop a receiver contention was designed.The destination node's location information is exposed. The secure position service system is used to match the actual global positions nodes with its real node identities.

PriyankaGoyal, VintiParmar, Rahul Rishi has accomplished a complete survey on MANET's Vulnerabilities, challenges, Attacks, Application [9]. The author has recommended all the possible vulnerabilities prevailing in the MANET networks. To improve the communication between the nodes certain routing algorithms are recommended. Some security objectives are also stated. It discusses about MANET characteristics.

Zhi Zhou and Kin Choong Yow has proposed a new approach for the anonymous geographic routing algorithm [15], it repress the exposure of identity of nodes and its location information with the help of three components. It assures the the entire network protection. The routing path, location of the nodes is hidden.

In this paper authorL. Sweeneyhave proposed a model named as named k-anonymity [18].It accompanies together a set of policies for providing node conservation.The release of k-1 individuals are not distinguished among the provided anonymity of k nodes, it also provides the details related to the information provided for every person. By using this model it helps in implementing the real world system.The entire information is maintained in the release.It also examines many attacks named as re-identification.The protection is provided privately to the entire information.

An Anonymous Location-based Efficient Routing protocol (ALERT) [6] was proposed by L. Zhao and H. Shen. The network field is divided into several zones with the help of hierarchical partitioning and it is partition in a dynamical manner. Then nodes are selected randomly from the zones created from the hierarchical partition and as the nodes are arbitrarily choose to generate a non-traceable anonymous route. Thus, ALERT provides anonymity conservation to d, data initiator, data receiver and route. The attacks on timing and the intersection attacks are countered effectively. The efficiency of anonymity is analyzed theoretically. ALERT provides a better protection in the anonymity and cost is less compared to the existing routing techniques. Also, ALERT proves to be a better comparable routing algorithm than the GPSR geographical routing protocol.

This paper [8] proposed by Eugene Y. Vassermaand Nicholas Hopper Kansas explores the attacks of depletion in the resource at the routing protocol layer. The entire network gets disabled due to node drainage and hence the power of the battery is becoming less. These attacks rely on popular protocol classes of routing; they are not dependent on specific protocols. All protocols are vulnerable to the Vampire attack which is unable to detect and are devastating to the entire network. These attacks are very simple to inject the malicious node into the network. These malicious node gains all the battery power and it empty up the entire power and bandwidth. This paper provides the recovery or the mitigate methods to overcome these deadly types of attacks. The forwarding nodes are checked again if these nodes are used or not, in-order to avoid the duplication of nodes.

This paper [4] proposed by Nivodhaya.J, Ramyadorai.D has studied the result about the energy level depletion in an geographic anonymous routing protocol ALERT due to Sybil attack. The Mobile Ad Hoc Networks (MANETs) for hostile environment requires secure and stable setup. Anonymous routing strategy which hides the routing information from the outsiders can provide highly secure communication among mobile nodes but cannot guarantee the stability of the network. Highly Secure network along with longer lifetime is the need of the hour for critical environments. Increasing the residual energy of the network indirectly increases its lifetime. Energy conservation in the network can also be achieved by mitigating the effects of the attacks that are aimed at the depletion of the nodal energy directly and network energy indirectly. Sybil attack is one of the well-known effects for such energy drain. The proposed work is aimed at studying the effect of Sybil attack with network energy in ALERT (Anonymous Location based Efficient Routing). Extensive simulations are done by inducing Sybil entities in ALERT routing and the results prove that the conservative network energy level decreases considerably with Sybil nodes.

III. METHODOLOGY

The given system uses advanced location based efficient routing technique in AODV routing protocols. Due to which it provides anonymity with the use of ALER technique. It also provides prevention from Sybil attack in order to avoid duplicate identities, energy consumption of nodes and reduction of network lifetime. In this strategy, MANET's takes the most important protocol AODV and apply it in the ALER routing technique for providing anonymity the route of packet forwarding cannot be determined and also location of the source and destination cannot be determined by the attacker. Thus using this strategy we can make AODV more secure. Here,AODV is used so as its nature is to broadcast the path request message to all the nodes in the network and from which node it receives the response it establishes the path with them and transfers the packet to them. But in the system it applies the ALER technique in AODV for anonymity protection, for this as in ALER it partitions the network into zones. In very first step it divides the network into different zones. It uses a formula for calculating the number of partitions required. In the second step it finds thelocation of the neighbor nodes in order to discover the route. After the selection of random nodes, a condition checks whether the nodes are already used or not, if the nodes are already used once again the ALER routing technique partitions the network and the procedure is repeated till the unused nodes are found. By doing this it is assured that there is no formation of loops. If a loop is detected then the packet send is drooped and the ALER routing technique partitions the zone again and whole procedure is followed again until the loop formation gets avoided. Then the source node multicast the

packets to all neighbors of the destination and which neighbors have minimum distance value create the final path form source to destination.

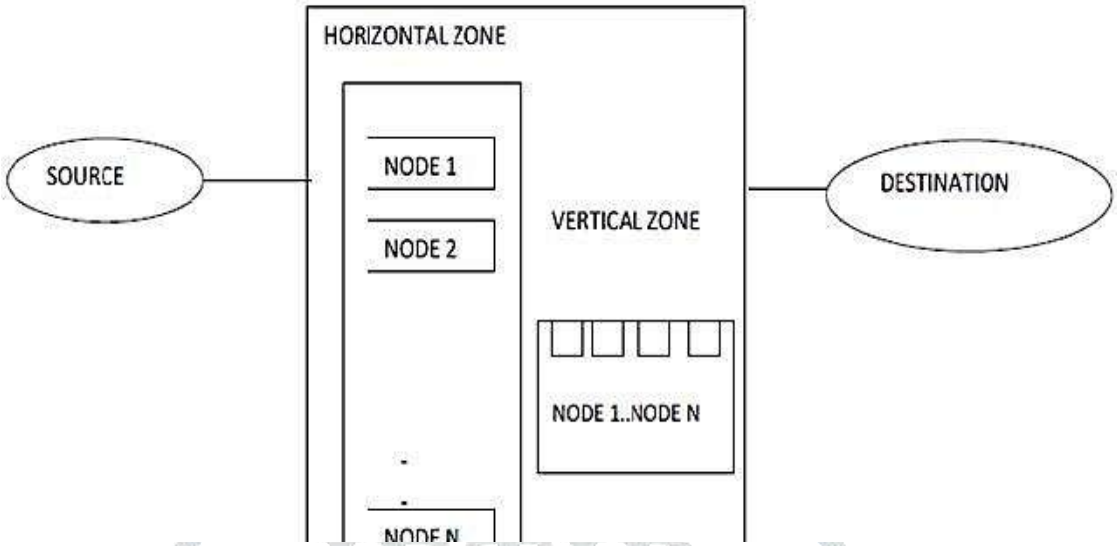

Figure 1 System Architecture

Algorithm Steps for ALER

1. Initially the network in rectangular shape is considerd and then it is divided into multiple zones.
2. When the source node has some data to forward to destination, it will choose random node which will be referred to as random forward. The relay node will be used to check the proper flow of the data between the nodes within the zone. The data will be sent out of the zone using xhash function so that message obtains privacy.
3. From its one hop neighbour nodes, the source node will choose a random node and will inform it by sending the hello message of its election as relay node. The relay node must forward the data to the any random node in the next zone which is nearest to the temporary destination.
4. So before the data transmission starts, the destination zone is identifies using a formula.Itially the number of zones to be partitioned is calculate then zone destination size is calculated.
5. The source node will send few packets to the relay node.
6. If this relay node is packet dropping node then it will not forward the data properly to the next zone. It can drop few of the packets, it can drop all the packets also.
7. From this it identifies that the particular node wich drops the data is malicious node and identifies it as Sybil node.
8. Then that Sybil node is discarded from the route. Then it searches for the other random forwarder node to send the data packet successfully to the destination.
9. If the relay node has properly forwarded the data, then the source node will keep on sending the remaining data to the same relay node.
10.While the data reaches the destination node the unique hashing id is usd for authentication and the data is retrived.
11. Same procedure will be followed by the node in the other zones until data reaches the destination node.

Providing Privacy for ALER

In addition to that high privacy is provided inside the network. Two concepts are used and the first one is xoring method. This is used to reduce the overhead of the data packet transfers so hence it's an advantage and the node gets more network life. While merging the data packets, they are compressed into a smaller size compared to its original size. The advantage in doing so is that we are now able to two to three packets of data at once. A hash method is also used; itfunctions used for math's calculations. It translates a given input in numbers into another numerical value by compressing it. The inputted value given to the hash function is random but the output is provided in fixed lengths.

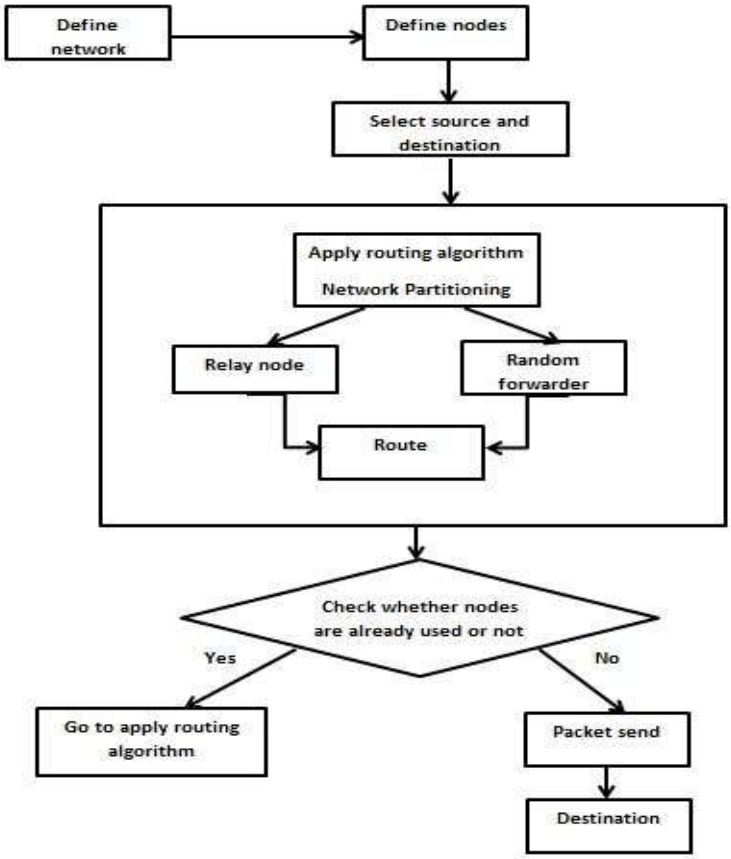

Figure 2 Flow diagram of Proposed System

IV. SIMULATION

Advanced location based efficient routing protocol's performance is evaluated using NS2 simulator. Nodes present in the rectangular network are placed to create a scenario as if the source wants to send its packets to the destination by providing anonymity to the route and the data packets in order to avoid the Sybil nodes from attacking the network. In order to evaluate the performance of the routing protocol, certain parameters are used to evaluate the efficiency of the ALER compared to the existing routing protocol. We used Throughput, Energy Consumption, Packet Loss, Packet Delivery Ratio, Delay and Overhead to evaluate the performance of the proposed system.

Table 1 Experiment Setup

Simulator	NS2
Network area	1000*1000
Channel Type 1	Channel/WirelessChanne
Propagation Model	Two Ray Ground
MAC Layer	IEEE 802_11
Max packet in ifq	50
Number of Nodes	40
Routing Protocol	AODV
Antenna Model	Omni Antenna
Communication Range	200

Screenshots of Simulation

In this project we have considered a network area with 40 nodes in NS2 and were successfully able to send data between the source and destination nodes by avoiding Sybil attack. Advanced location based efficient routingprotocol is used to establish anonymity conservation to sender, receiver and also to create a non-traceable anonymous route by using the. This implements the AODV routing protocol. It also provides effective remedy from Sybil attack.

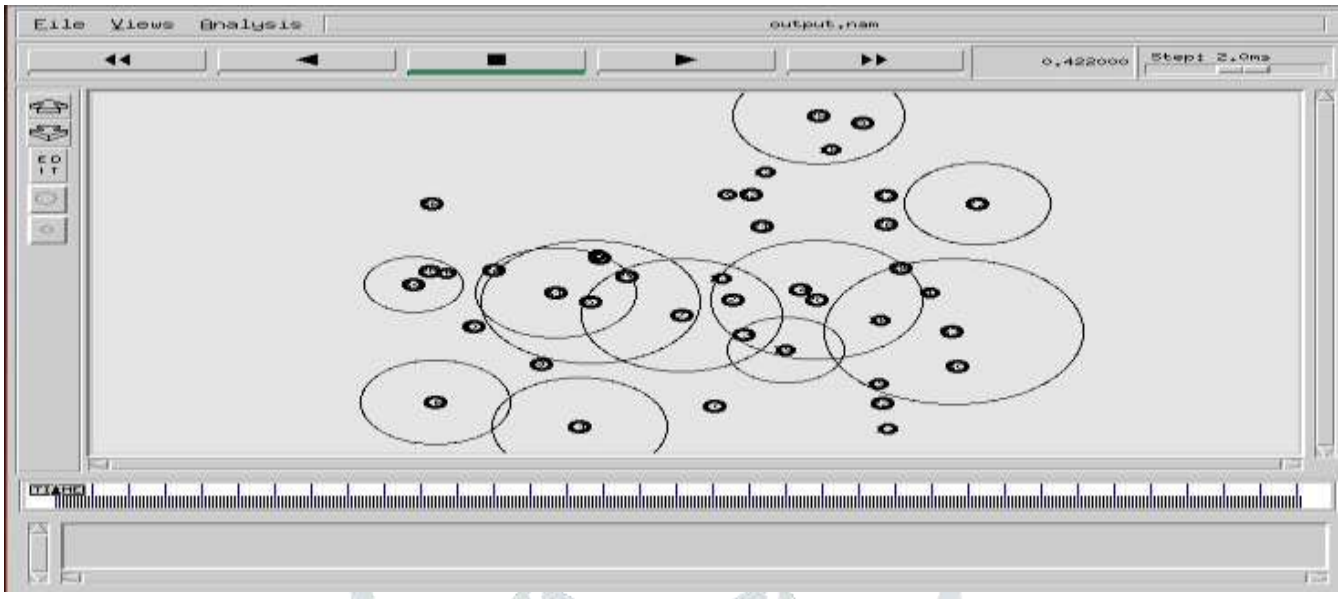

Figure 3 Initialization of nodes

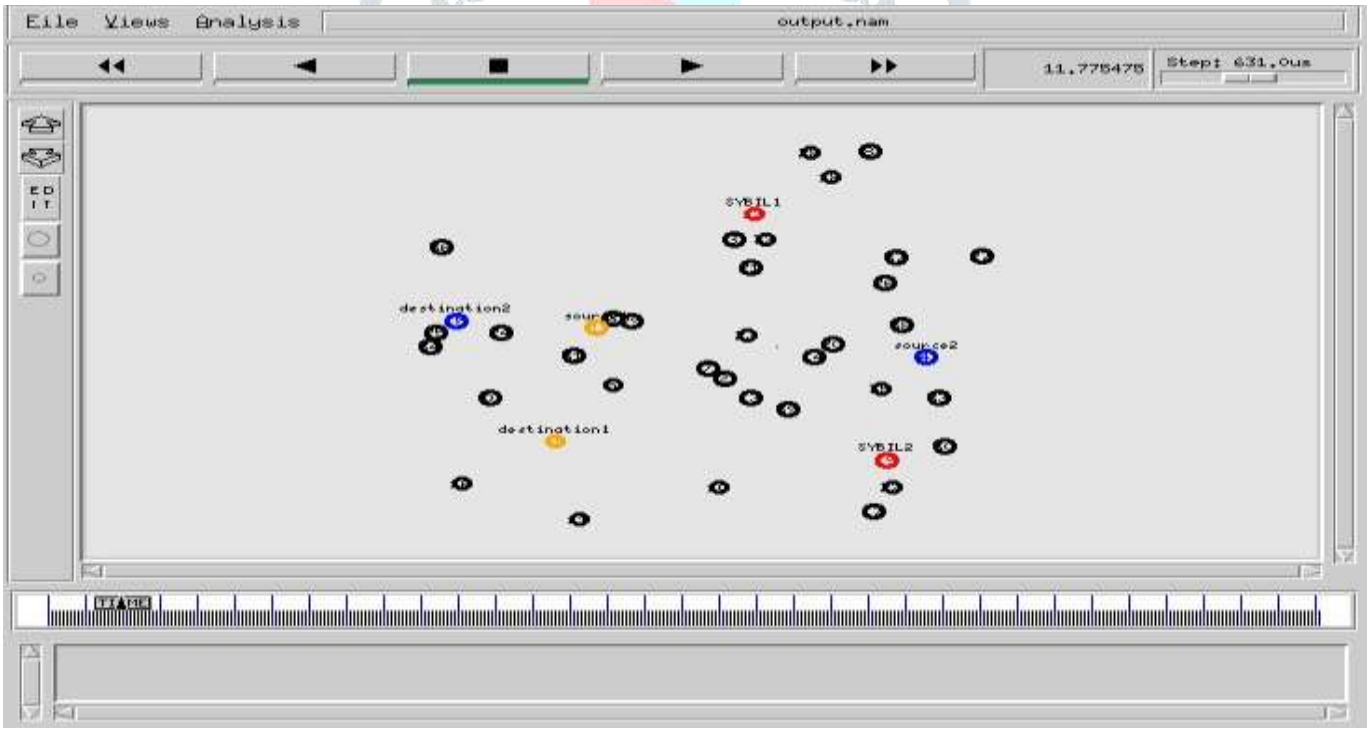

Figure 4 Identifying Sybil nodes

V. RESULT AND ANALYSIS

Figure 5 shows the graph for Packet Loss of ALER protocol and SYBIL_AODV protocol. We observe that as number of nodes increases the packet are also lost in an increasing manner. For SYBIL_AODV protocol, loss of packet is high compared to ALER protocol.

Figure 5 Graph for Packet loss

Figure 6 shows the graph for Throughput of protocol ALER and SYBIL_AODV protocol. We observe that the throughput of ALER protocol is consistently higher than that of SYBIL_AODV protocol. We observe that in both the protocols, ALER and SYBIL_AODV, with the increase in the number of nodes there has been a steady increase in the throughput value.

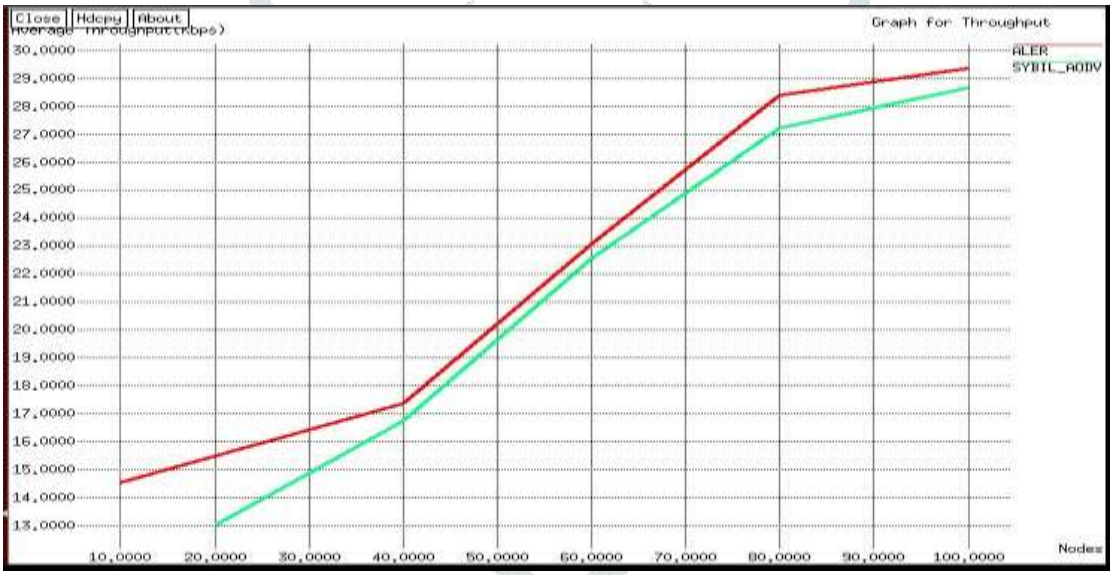

Figure 6 Graph for Throughput

Figure 7 shows the graph for Packet Delivery Ratio of ALER and SYBIL_AODV. We observe that the delivery ratio of transmission packets of ALER protocol is consistently higher than that of SYBIL_AODV protocol. We observe that in both the protocols, ALER and SYBIL_AODV, with the increase in the number of nodes there has been a steady increase in the delivery ratio of packet value.

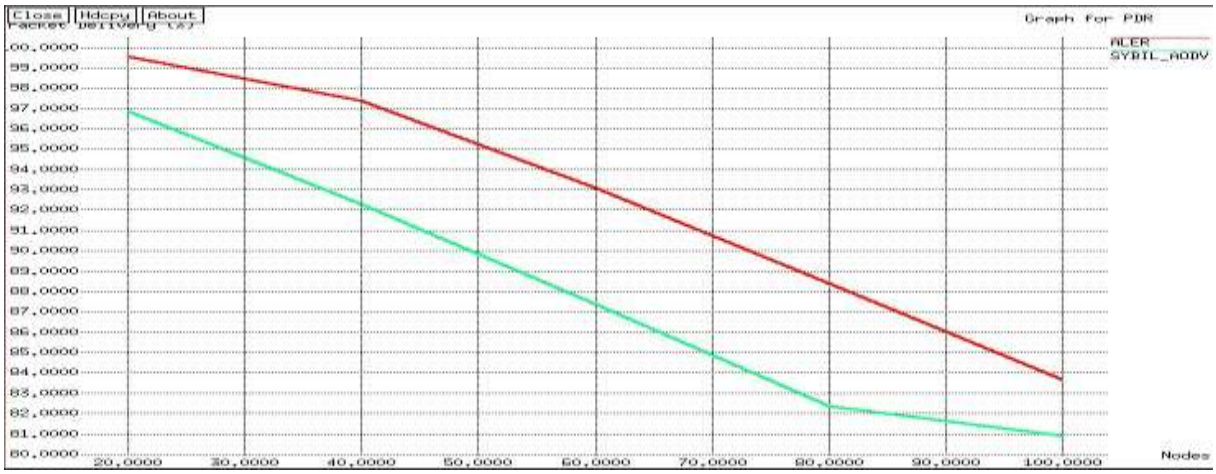

Figure 7 Graph for Packet delivery ratio

Figure 8 shows the graph for End to end delay of ALER protocol and SYBIL_AODV protocol. We observe that the delay of transmission packets of ALER protocol is consistently less than that of SYBIL_AODV protocol.

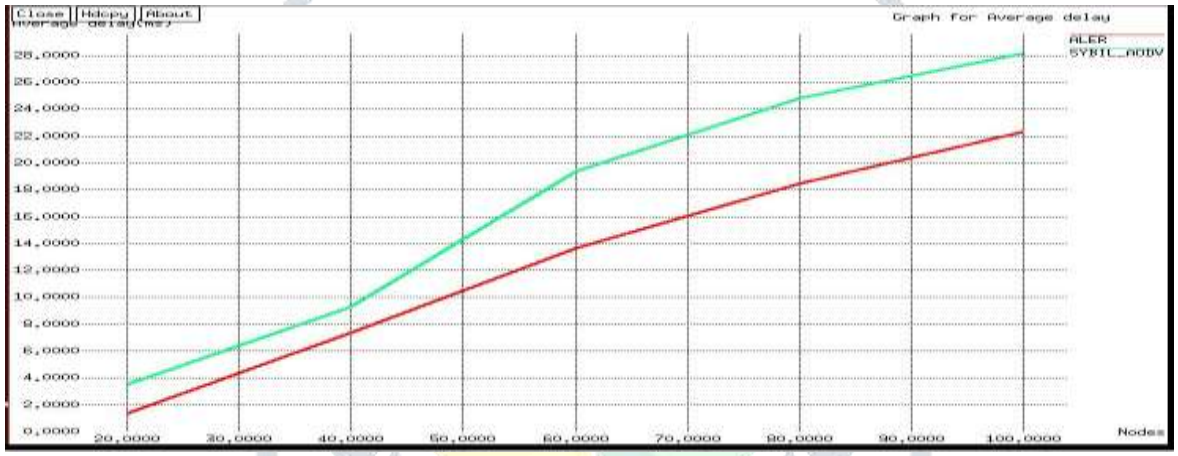

Figure 8 Graph for Average Delay

Figure 9 shows the graph for Energy consumed by ALER and SYBIL_AODV nodes respectively. We observe that the energy was depleted by the nodes using SYBIL_AODV protocol while compared to ALER. We observe that in both the protocols, ALER and SYBIL_AODV, with the increase in the number of nodes there has been a steady increase in the energy consumption by nodes.

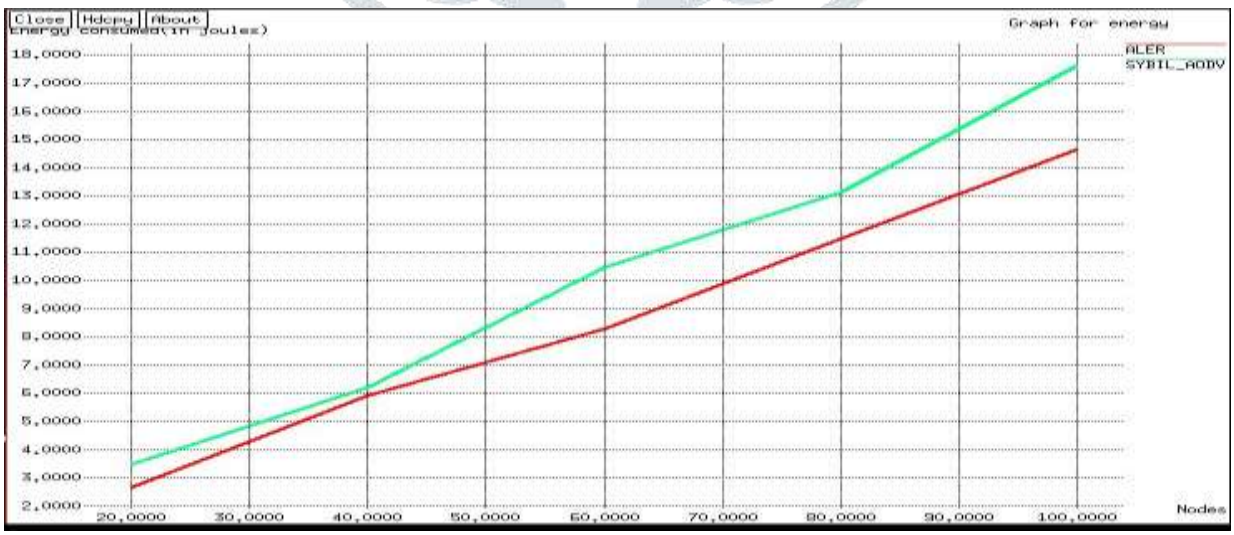

Figure 9 Graph for Energy consumption

Figure 7.10 shows the graph for Overhead of ALER protocol and SYBIL_AODV protocol. We observe that as number of nodes increases the overhead also increases. For SYBIL_AODV protocol, overhead is high compared to ALER protocol.

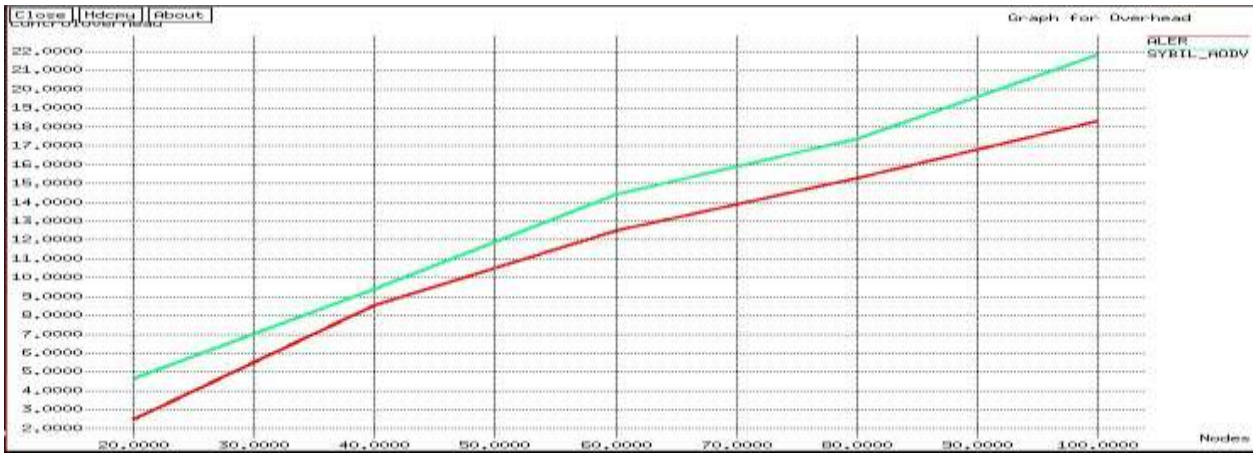

Figure 10 Graph for Overhead

VI. CONCLUSION

Present anonymous routing techniques either depend on hop-by-hop encryption or redundant traffic, both of them have a negative approach as it generate high cost. Not only that some of the existing protocols fail to provide complete protection to the network as some provide anonymity only to either source or destination nodes. Due to which complete protection of the network becomes a failure. But when a comparison is made between ALER technique and other existing ones, ALER is distinguished by others as it provides low cost and the anonymity protection is provided to the complete network from sender to the destination and also to the route the network follows. It uses a unique method of partitioning the zones in a dynamic hierarchical way which makes difficult to the outsiders to detect the route followed by the network and also the two end points i.e. the sender and the destination. ALER includes a packet rather than the position, which provides high protection in anonymity to the source and destination zones. ALER has characteristics to strengthen the anonymity by hiding the sender and the destination among a number of senders/receivers. In addition to that high privacy is provided inside the network. Two concepts are used and the first one is xoring method. This is used to reduce the overhead of the data packet transfers so hence it's an advantage and the node gets more network life.A hash method is also used; it functions used for math's calculations. It translates a given input in numbers into another numerical value by compressing it. The inputted value given to the hash function is random but the output is provided in fixed lengths.Hence by using both this methods an extra layer of protection is provided to the data packets and it also ensures anonymity to the network. The given system has also presented a novel approach on avoiding Sybil attack by checking the forwarding nodes in the route to avoid loop formations. When a loop is identified in a network it discards the existing route and creates a new route to forward the data packet. This helps to avoid the Sybil attack and also reduce the network lifetime and energy consumption level of nodes.

REFERENCES

[1] Sheikh Abdul Wajid ,Kiran Gupta ," E-SHARP: Enhanced Secured Hierarchical Anonymous Routing Protocol for MANETs", International Journal of Computer Applications, Volume 153 – No.1, November 2016.

[2] Namrata.R.Borkar, Avinash.P.Wadhe,"Implementation of an Anonymous Location – Based Efficient Routing Protocol in Mobile Ad-hoc Networks", International Journal of Advance Research in Computer Science and Management Studies, Volume 3, Issue 5, May 2015.

[3] DurgeshPyati, Rekha.S, "High Secured Location-based Efficient Routing Protocols in MANET's",International Journal of Recent Development in Engineering and Technology,Volume 2, Issue 4, April 2014.

[4] Nivodhaya.J, Ramyadorai.D, "Analysis of Sybil Impact on Network Life with Alert in Ad hoc Communication", International Journal of Engineering Research & Technology, Vol.3, Issue 1, January 2014.

[5] Mr. L Raja, Capt. Dr. S SanthoshBaboo," An Overview of MANET: Applications, Attacks and Challenges", International Journal of Computer Science and Mobile Computing (IJCSM), Vol. 3, Issue. 1, January 2014.

[6] L. Zhao and H. Shen, "ALERT: An Anonymous Location-Based Efficient Routing Protocol in MANETs", International Conference of Parallel Processing (ICPP), 2013.

[7] Vanita Rani, Dr.RenuDhir,"A Study of Ad-hoc Network: A Review", International Journal of Advanced Research in computer Science and Software Engineering, Volume 3, Issue 3, March 2013.

[8] Eugene Y. Vassermaand Nicholas Hopper Kansas State University University of Minnesota "Vampire attacks: Draining life from wireless ad-hoc sensor networks", Mobile (Volume: 12, Issue: 2), 20 December 2012.

[9] PriyankaGoyal, VintiParmar, Rahul Rishi, "MANET: Vulnerabilities, challenges, Attacks, Application", International Journal of Computational Engineering & Management (IJCEM), Vol. 11, January 2011.

[10] K.E. Defrawy and G. Tsudik, "ALARM: Anonymous Location-Aided Routing in Suspicious MANETs", IEEE International Conference Network Protocols (ICNP), 2009.

[11] X. Wu, J. Liu, X. Hong, and E. Bertino, "Anonymous Geo-Forwarding in MANETs through Location Cloaking", IEEE Trans. Parallel and Distributed Systems, vol. 19, no. 10, pp. 1297-1309, Oct. 2008.

[12] X. Wu, "DISPOSER: Distributed Secure Position Service in Mobile Ad Hoc Networks: Research Articles", Wireless Comm. and Mobile Computing, vol. 6, pp. 357-373, 2006.

[13] M.F. Mokbel, C.-Y. Chow, and W.G. Aref, "The New Casper: Query Processing for Location Services without Compromising Privacy", Proc. 32nd Int'l Conf. Very Large Databases (VLDB), 2006.
[14] 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.
[15] Z. Zhi and Y.K. Choong, "Anonymizing Geographic Ad Hoc Routing for Preserving Location Privacy," Third International Workshop Mobile Distributed Computing (ICDCSW), 2005.
[16] 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.
[17] K. El-Khatib, L. Korba, R. Song, and G. Yee, "Anonymous Secure Routing in Mobile Ad-Hoc Networks", International Conference Parallel Processing Workshops (ICPPW), 2003.
[18] L. Sweeney, "k-Anonymity: A Model for Protecting Privacy", International Journal Uncertainity Fuzziness Knowledge-Based Systems, vol. 10, no. 5,pp. 557-570, 2002.
[19] Y. Xue, B. Li, and K. Nahrstedt, "A Scalable Location Management Scheme in Mobile Ad-Hoc Networks", technical report, 2001.
[20] J. Li, J. Jannotti, D.S.J. De, D.S.J. De Couto, D.R. Karger, and R. Morris, "A Scalable Location Service for Geographic Ad Hoc Routing", Programmed Random Occurrence ACM MobiCom, 2000.
[21] J. Li, J. Jannotti, D.S.J. De, C. David, R. Karger, and R. Morris, "A Scalable Location Service for Geographic Ad Hoc Routing",Programmed Random Occurrence ACM MobiCom, 2000.