Secure Energy Aware Anonymous Location Based Routing Protocol Formanet

[1]Mr.P.Ramesh, [2]Dr.H.Abdul Rauf, [3]A.kumar
[1]Teaching Fellow, [2]Principal, [3]P.G.Scholar
[1]Department of Computer Technology, [2]Dhaanish Ahamed institute of Technology, [2]Department of Computer Technology,

***Abstract*— In order to provide randomized routing ALERT (Anonymous Location-based and Efficient Routing) protocol is used. But the proposed protocol SEALERT will provide higher anonymity protection at lower cost. It also increases the nodal lifetime in the network. Thereby it increases the efficiency of transmission of packets. The proposed protocol dynamically partitions the network into area called zones and it randomly chooses a node as an intermediate relay node. This node forms a non-traceable anonymous route. Later this relay node chooses another node in the network which has least cost from the destination. The process of choosing relay node takes place until the destination can be reached at lower cost. Each time for choosing another node it uses EGPRS algorithm, a variant of GPRS (used in SEALERT to send data to relay node), to find a node with inherent battery backup. Since the data is broadcasted to k nodes in the destination zone, it can provide k-anonymity for the destination. The proposed also detects the Sybil attack in the network.**

***IndexTerms*— Mobile ad hoc networks, anonymity, routing protocol, geographical routing, ALERT**

I. INTRODUCTION (HEADING 1)

Wireless communication has shown its numerous advantages over wired communication since Guglielmo Marconi successfully transmitted signals across the Channel for the first time in 1898. From then, there came a great demand for wireless communication due to introduction of digital and Radio Frequency (RF) fabrication developments, portable mobile devices, such as cellular phones, personal digital assistants (PDA) and laptops.Wireless communication networks such as cellular networks, wireless LANs (WLAN), Bluetooth networks, Ultra-wide band (UWB) networks, Mobile Ad Hoc Networks (MANETs), and Wi-Max hath developed to a greater extent. Cellular networks, Bluetooth networks, and WLANs are the most widely used, than the other specified technologies. Since cellular networks and WLANs are centralized networks they incur morecostly infrastructure, also requires central administration.Bluetooth technology connects these networks in an adhoc fashion but it limit to shorter range. Therefore, a Wireless Mobile Ad Hoc Network is a distributed, self-organized and multi-hop network that has obtained tremendous attention in recent years. MANET, a distributed network which is not in need of centralized control, hence each can separately act as a source, sink and also as a router. For military communication or emergency searching operations, in which infrastructure can't be supported, this type of dynamic network is useful and further due to its simplicity ad hoc enables to share data in a convenient manner. Enabling multi-media applications such as video and audio communication in MANETs requires quality of service (QOS) support.

The use of Anonymous routing protocols are crucial in MANETs to provide secure communications by hiding node identities and preventing traffic analysis attacks from outside observers. Location anonymity [22] [23] of data sources and destination as well as route anonymity is included in MANET. "Identity and location anonymity of sources and destinations" means it is hard if possible for other nodes to obtain the real identities and exact locations of the sources and destinations. Since the route anonymity is a problem in MANET, our proposed protocol SEALERT provides a facility to identify these anonymity. SEALERT provides the[22] anonymous routing to the packet. And then ALERT is Resilience to intersection attacks andtiming attacks. The strategy of effective counter intersection attacks provided in SEALERT has proved to be a tough open issue. The proposed protocol provides [22] high anonymity protection (for sources, destination, and route) with low cost along with the increased nodal lifetime in the network. The proposed system considers the energy of the nodes involved in the communication. Greedy Perimeter Stateless Routing (GPSR) is a well-known and most commonly used position based routing protocol for MANETs. Energy-aware GPSR protocol, referred to as E-GPSR, operates as follows: a forwarding nodefirst determines a candidate set of neighbor nodes – the nodes that lie closer to the destination than itself. The sum of fraction function of initial energy currently available at the neighbor node and the progress obtained with the selection of the neighbor node is same as computed weight of each such candidate neighbor node [1]. To receive the data packet the candidate node with large weight value is chosen.

II. LITERATURE REVIEW

Sybil attack is one in which a malicious node on a network illegitimately claims to be several different nodes simultaneously. A Sybil attacker can either create more than one identity on a single physical device in order to launch a coordinated attack on the network or can switch identities in order to weaken the detection process, thereby promoting lack of accountability in the network**.** Here the relay node may act as the attacker and then, the node create the new identity and then act as the neighbor to the particular node ,it will send message to the relay node with the different identity , relay node route packet to the wrong relay node that does not nearer to the destination. If it occurs it will drains energy of the nodes involved in the network. Energy-aware GPSR protocol, referred to as E-GPSR, 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 [1] [3] [17]. 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. Compared to GPSR, with the use of E-GPSR, the unfairness in node usage would relatively reduce and the time of first node failure.

Wei Liu, Ming Yu et al (2014), proposed the Anonymous communications are important for manyof the applications of mobile ad hoc networks (MANETs) deployedin adversary Environments. But this proposed methodology does not satisfy the requirements needed.

Haiying Shenand Lianyu Zhao et al(2013) proposed the Mobile Ad Hoc Networks (MANETs) use anonymous routing protocols which has the ability to hide the node identities by relying on either hop-by-hop encryption or redundant traffic which either generates high traffic or high cost.

III. RELATED WORKS

II. ALERT has variety of advantages than other protocol since it uses anonymous routing protocols that have the ability to hide node, thereby providing anonymity. It has ability to partition zones dynamically. But ALERT fails to satisfy the need of preventing Sybil Attacks, which is a common problem in wireless networks. To overcome from this disadvantage, we provide an extend version of ALERT protocol know as SEALERT. SEALERT has ability to identify the Sybil Attacks and also calculate the energy dissipation value using the RSS value. Hence the data can be prevented from unauthorized access also leads to efficient transmission.

IV. PROPOSED WORK

In order to provide high anonymity protection (for sources, destination, and route) with low cost, this project proposes an Secure Energy Aware Anonymous Location-based Routing protocol (SEALERT). SEALERT dynamically partitions a network field into zones and randomly chooses nodes in zones as intermediate relay nodes forming a non-traceable anonymous route. In each routing step, a data sender and forwarder partition the network field in order to separate itself and the destination into two zones. Then randomly chooses a node in the other zone as the next relay node and uses the GPSR algorithm to send the data to the relay node. The data is broadcasted to k nodes in the destination zone, [23] [19] providing k-anonymity to the destination. ALERT has a strategy to hide the data initiator among a number of initiators to strengthen the anonymity protection of the source. It is resilient to intersection attacks and timing attacks this project analyze ALERT in terms of anonymity and efficiency. It also conducted experiments to evaluate the performance of SEALERT in comparison with other anonymity and geographic routing protocols. The contribution of this work includes: first one is Anonymous routing. [22] [17] ALERT provides route identity and location anonymity of source and destination. ALERT mainly uses randomized routing of one message copy to provide anonymity protection. Third one is Resilience to intersection attacks and timing attacks. It has a strategy to effectively counter intersection attacks, proved to be a tough open issue. .The proposed protocol provides [22] high anonymity protection (for sources, destination, and route) with low cost along with the increased nodal lifetime in the network. As like ALERT, and then The proposed SEALERT also dynamically partitions a network field into zones and randomly chooses nodes in zones as intermediate relay nodes, forming a non-traceable anonymous route. In each routing step, the data sender or forwarder partitions the network field in order to separate itself and the destination into two zones. The other zone as the next relay node and uses the EGPSR algorithm as a variant of GPSR in ALERT to send the data to the relay node. With this the inherent battery backup of the node is also considered during geographical forwarding. By this even though the node is the best forwarder by the distance factor, it is selected for forwarding only if it has the sufficient battery power to carry out the task of forwarding the data packets. In the last step, the data is broadcasted to k nodes in the destination zone where it provides k-anonymity to the destination [3]. In addition, the protocol has a strategy to hide the data initiator among a number of initiators to strengthen the anonymity protection of the source. Second strategy included in the protocol is towards the detection of the Sybil attacker nodes which aims at creating duplicate identities for themselves as different nodes at different locations thereby increasing the routing overhead and wasting the inherent battery power of the legitimate nodes by responding to these faulty identities. By this the battery draining of nodes due to unnecessary routing policies are avoided priory thereby increasing the overall lifetime of all the nodes in the network is

possible. Thus the proposed EALERT has the efficient strategy towards increased nodal life time in the low cost anonymous routing protocol

Architecture Diagram

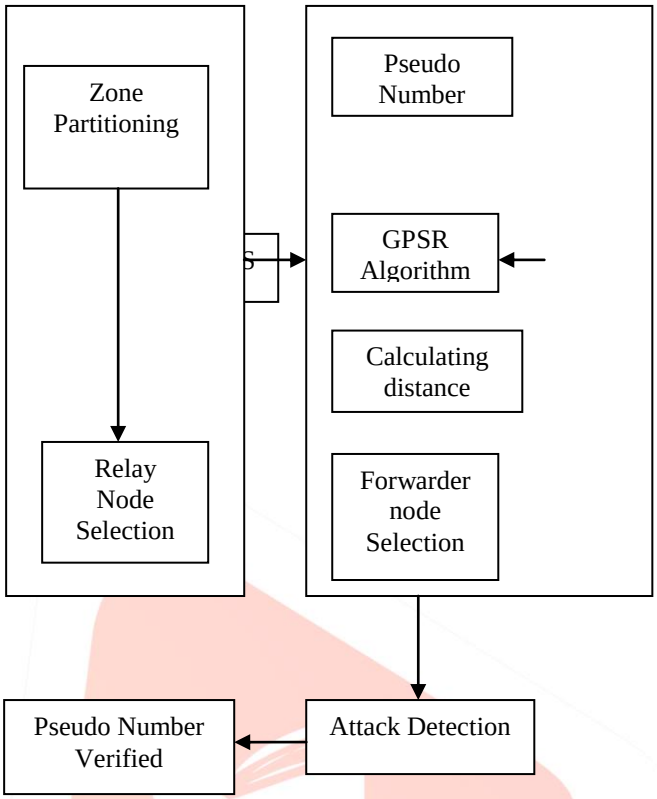

Figure 1 Architecture diagram

System Modules

The system comprises of the following modules which include,

1) Anonymous routing for MANET
2) Energy Aware
3) Against Attack

1. Anonymous routing for MANET

1.1. Network model

Network model consider the random way point model and the group mobility model Network are classified into Zone. Consider a MANET deployed in a large field where geographic routing is used for node communication in order to reduce the communication latency. This location of a message's sender may be revealed by merely exposing the transmission direction. Therefore, an [8][17] anonymous communication protocol that can provide un-traceability is needed to strictly ensure the anonymity of the sender when the sender communicates with the other side of the field. A malicious observer may try to block the data packets by compromising a number of nodes and intercept the packets on a number of nodes, even trace back to the sender by detecting the data transmission direction. Thus, the route should also be undetectable. Here malicious observer may also try to detect destination nodes through traffic analysis by launching an intersection attack. Thus the destination node also needs the protection of anonymity.

1.2. Zone partition

In ALERT the communication range is partitioned into the Zones. If the source and destination are not present in the same zone, the Zone partition the condition to be considered is, the forwarder and the destination not present in the same zone. This condition satisfied it will be portioned into horizontal and vertical zones. In this,[22[23] Random forwarder is selected randomly

in the zone. RF is selected in the following way. First the randomly the location is selected from the particular Zone. The nearest node to the location is elected as the Random Forwarder.

Input:Random Forwarder selection
Output: partitioned Network

Relay node selection:

AlgorithmGreedy forwarding based Relaynode
Input: NeighborTable, sender, destination;
Output: Greedy Relaynode;
ListN: Neighbor List
ListC: Candidate List, initialized as an empty list
ND: Destination Node
Base: Distance between current node and ND
Greedy forwarding based Relaynode
if find(ListN, ND) then
next hop ND
return
end if
for i=0 to length(ListN) do
ListN[i]:dist dist(ListN[i], ND)
end for
ListN: sort()
Relaynode?ListN[]
Assign weight w2 for the sorted list from high to low

2. Energy aware

Energy-aware GPSR protocol, referred to as E-GPSR, 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 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 has the largest weight value is the chosen next hop node to receive the data packet. The procedure is repeated at every hop where greedy forwarding is possible. Here greedy forwarding is not possible. Compared to GPSR, with the use of E-GPSR, the unfairness in node usage would relatively reduce and the time of first node failure EGPSR algorithm as a variant of GPSR in ALERT to send the data to the relay node, with this the inherent battery backup of the node is also considered during geographical forwarding. By this even though the node is the best forwarder by the distance factor, it is selected for forwarding only if it has the [20] sufficient battery power to carry out the task of forwarding the data packets. In the last step, the data is broadcasted to k nodes in the destination, providing k-anonymity to the destination. [7] [23] The protocol has a strategy to hide the data initiator among a number of initiators to strengthen the anonymity protection of the source.

Input: while selection of Random Forwarder energy of the node considered
Output: energy aware routing

3. Against attack

The proposed system detects the attacker using the received signal strength in the network. Relay node receives packets from the same node with different identity and transfer the packet to the destination. The Attack detection operation is performed in the following way. Relay Node calculates the Received signal strength of the nodes from those it gets the packets and it will detect the attacker nodes in the network. If nodes RSS value is low it will consider as the random node and it will allow that node to route the packet. Otherwise that node considers as the attacker and it will avoid the node to transfer the packet it will consider as the attacker. In SEALERT, the same operation performed for the ALERT.

A Sybil attacker node which aims at creating duplicate identities for themselves as different nodes at different locations thereby increasing the routing overhead and wasting the inherent battery power of the legitimate nodes by responding to these faulty identities. By this the battery draining of nodes due to unnecessary routing policies are avoided priory thereby increasing the overall lifetime of all the nodes in the network is possible. Thus the proposed EALERT has the efficient strategy towards increased nodal life time in the low cost anonymous routing protocol.

Input:Sybil attacker with different identity sent packet to relay node
Output: Energy drain of the nodes involved in the routing

The distinction between a new legitimate node and a new Sybil identity can be made based on their neighborhood joining behavior. While receiving the message from the same node with different identity, the RSS values for those neighbors are calculated. If the received RSS value is high it will be detected as attacker.

Input: RSS calculation
Output: detection of the attack presence

The proposed scheme utilizes the RSS (Received Signal Strength) in order to differentiate between the legitimate and Sybil identities. This scheme does not use localization technique for Sybil attack detection and hence does not need any directional antennae or any GPS equipment. The distinction between a [19] new legitimate node and a new Sybil identity can be made based on their neighborhood joining behavior. The Received signal strength values are varied for the neighbors act as the Sybil attacker from that of the legitimate node.

V RESULTS AND DISSCUSSION

Performance

The number of actual participating nodes:

These nodes include RFs and relay nodes that actually participate in routing. This demonstrates the ability of ALERT's randomized routing to avoid routing pattern detection.

b) The number of random forwarders:

This is the number of actual RFs in a S-D routing path. This proves routing anonymity and efficiency.

.

c) The number of remaining nodes in a destination zone:

This is the number of original nodes remaining in a destination zone after a time period. The larger number provides higher anonymity protection to a destination and to counter the intersection attack. This measure metric over time to show effectiveness on the destination anonymity protection.

.

d) The number of hops per packet

The accumulated routing hop counts divided by the number of packets sent, which shows the efficiency of routing algorithms.

e) *Latency per packet:*

This is the average time elapsed after a packet is sent and before it is received. This includes the time cost for routing and cryptography. The metric reflects the latency and efficiency of routing algorithms

f) Delivery rate:

This is measured by the fraction of packets that are successfully delivered to a destination. This shows the robustness of routing algorithms to adapt to mobile network environment

The proposed system performance evaluated while using the SEALERT routing. In this proposed system performance evaluated for the node's energy before the Sybil attack detection and after detection of Sybil attack in the network while using EALERT routing

Evaluation

To measure our success in meeting the design goals for GPSR AND EGPSR, we simulated the algorithm on a variety of static and mobile network topologies. We focus mainly on the mobile simulation results in this paper, as that part of the design space is more demanding of a routing protocol—link additions and removals are far more frequent under mobility

To use dynamic hierarchical zone partitions and random relay node selections and the strength the anonymity protection of source and destination and to detect the Sybil attack in the network and avoid the attack in the network. We also simulate Haiying Shen et al.'s ALERT, which has been shown to offer higher packet delivery ratios and lower routing protocol overhead than several other ad-hoc routing protocols.

2.1. Simulation Environment

We use ns-2 (version 2.35) as the simulator for our study. We implemented the GPSR and E-GPSR protocols in ns-2. The network dimension used is a 600m x 600m 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 onGPSR can be exploited to the maximum.

The average networkconnectivity 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. The Medium Access Control (MAC) layer model used is the IEEE 802.11 [6] model. Link bandwidth is 2 Mbps. The interface queue is FIFO-based with a queue size of 100.

2.2. *Simulation Model:*

SIMULATOR	Network Simulator 2
NUMBER OF NODES	Random
TOPOLOGY	Random
FIXED SETUP	Source,destination,random forwarder
INTERFACE TYPE	Phy/WirelessPhy
MAC TYPE	802.11
QUEUE TYPE	Droptail/Priority Queue
QUEUE LENGTH	200 Packets
ANTENNA TYPE	Omni Antenna
PROPAGATION TYPE	Tworay Ground
ROUTING PROTOCOL	AODV
TRANSPORT AGENT	UDP
APPLICATION AGENT	CBR
TRANSMISSION POWER	Vary at each Layer(0.2-1.0)
RECEPTION POWER	Vary at each Layer(0.2-1.0)

2.3. Implementation Results

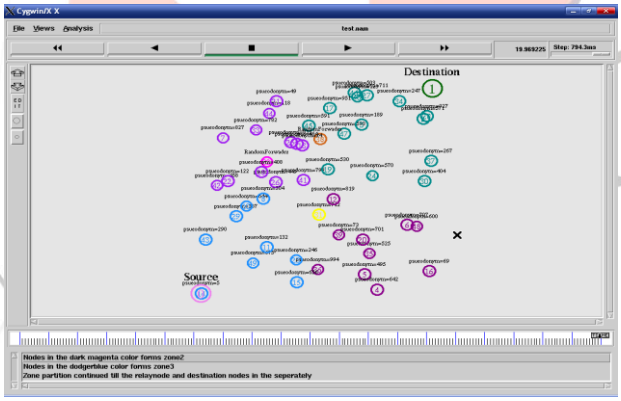

Figure 2.3.1 Output of SE-ALERT

2.4 Efficiency Comparison

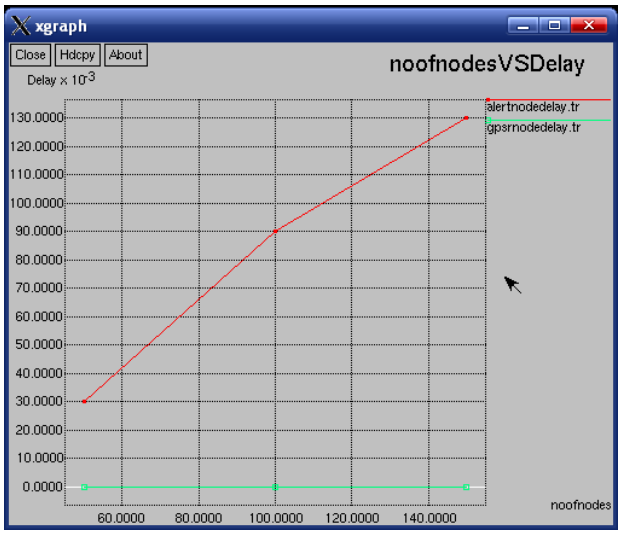

Figure 2.4.1 Output of Number Of nodes vsDelay

This graph shows the comparison between the Number of Nodes and delay in the network with the GPSR and ALERT. .while the number of nodes increases in the network the routing process taken place in the network. The communicating nodes increase in the network the delay to reach the destination increases in the network. If the packet reaches the destination greater than particular time specified as threshold time that is considered as the delay. Due to the support features of selecting the Random forwarder and the anonymity property it will increase the delay.

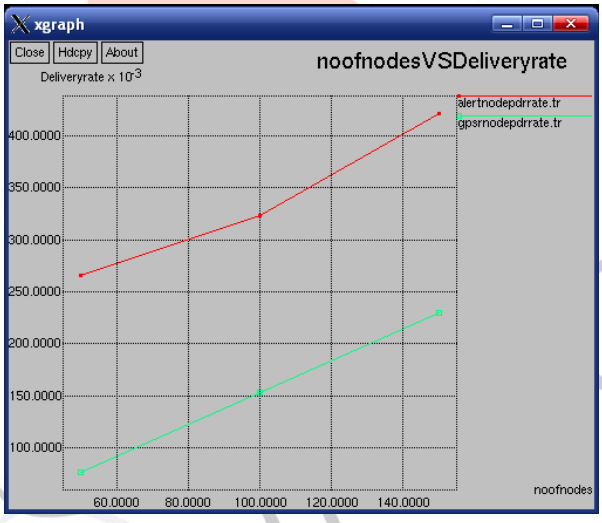

Figure 2.4.2 Output of number of node vs Deliveryrate

This graph shows the comparison between the Number of Nodes and PDR in the network with the GPSR and ALERT. .while the number of nodes increases in the network the routing process taken place in the network. The communicating nodes increase in the network the packet delivery rate of the destination increased in the network. The packets need to travel the more routing node and then it needs to reach the destination so the Packet delivery ratio in destination and also increased.

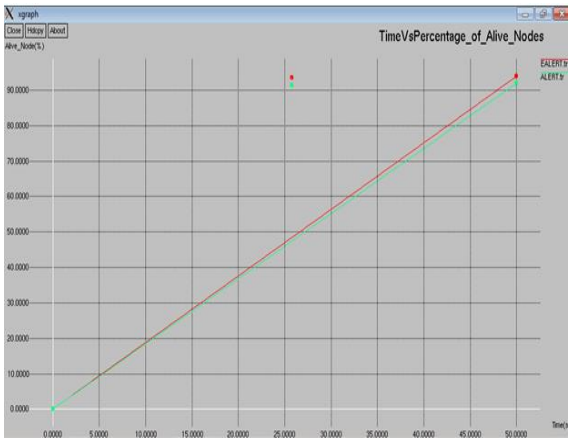

Figure 2.4.3 Output of Time vs percentage of Alive node In ALERT and SEALERT

This graph shows the Compare to Existing, Energy aware system contains the many number of Alive nodes. Energy is the important factor for the network, while Calculating the trust value of the system it also considers the energy of the node to transfer the data to the destination. It will increase the network lifetime.

VI CONCLUSION

SEALERT 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. 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.

This project contributes QoS in SEALERT, by selecting random position based on the minimum distance random position with respect to destination. Hence number of hops involved in data forwarding is reduced which in turn reduces and energy consumption in addition to anonymity. The proposed scheme proposes the energy aware Anonymous Location based routing; it considered the energy of the nodes involved in network. Apart from hiding details of the data sources, route information and location of nodes in such environments, the overall Network Life -time which in turn refers to the lifetime of nodes is also significant for the success of the network. Because, death of any node due to battery draining is very critical and recharging of such nodes is not possible or even very difficult in such hostile environments. With this input, the existing low cost anonymous routing protocol SEALERT for MANET is enhanced to support the increased network security. SEALERT is not completely bullet-proof to all attacks. Future work lies in reinforcing SEALERT in an attempt to thwart stronger, active attackers and demonstrating comprehensive theoretical and simulation results.

VII REFERENCES

[1] Dongkyun Kim, J.J. Garcia-Luna-Aceves "Routing Mechanisms for Mobile Ad Hoc Networks Based on the Energy Drain Rate " " IEEE TRANSACTIONS ON MOBILE
VOL 2 NO 2 ,2003
[2] Shengming and Jiang " Provisioning of Adaptability to Variable Topologies for Routing "Schemes in MANETs " IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 22, NO. 7 2004
[3]] Fan Bai and Bhaskar Krishnamachari "Modeling Path Duration Distributions in MANETs "" IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 22, NO. 7 2004
[4] Jian Chen and Yong Guan "Customizing GPSR for Wireless Sensor Networks "" IEEE International Conference on Mobile Ad-hoc and Sensor Systems 2004
[5]] Xiaoxin Wu and Bharat Bhargava "AO2P: Ad Hoc On-Demand Position-Based Private "" IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 4, NO. 4 2005
[6]] Lei Chen "QoS-Aware Routing Based on Bandwidth Estimation for Mobile Ad Hoc Networks "IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 23, NO 2005
[7] Giovanni Di Crescenzo "Securing Reliable Server Pooling in MANET Against Against Byzantine Adversaries " IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 24, NO. 2 2006
[8] Chao-Chin Chou "An Efficient Anonymous Communication Protocol for Peer-to-Peer Applications over Mobile Ad-hoc Networks "IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 25, NO 2007
[9] Xiaoxin Wu, Jun Liu "Anonymous Geo-Forwarding in MANETs through Location Cloaking" IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 19, NO. 10 2008

[10] Uichin Lee, Joon-Sang Park " Efficient Peer-to-Peer File Sharing Using Network Coding in MANETs "" JOURNAL OF COMMUNICATIONS AND NETWORKS, VOL. 10, NO. 4 2008
[11] Soonhwa Sung "Zone-Based Self-Organized Clustering with Byzantine Agreement in MANET "JOURNAL OF COMMUNICATIONS AND NETWORKS, VOL. 10, NO. 2 2008
[12] Chi Zhang "On the Improvement of Scaling Laws for Large-Scale MANETs with Network Coding " IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS 2009
[13] Behrooz Nakhkoob "Multi-Transceiver Optical Wireless SphericalStructures for MANETs "IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 27, NO. 9 2009
[14]Leonard Barolli "A Testbed for MANETs: Implementation,Experiences and Learned Lessons "IEEE SYSTEMS JOURNAL, VOL. 4, NO. 2,2010
[15]] Lanjun Dang and Jie Xu " DASR: Distributed Anonymous Secure Routing with Good Scalability for Mobile Ad Hoc Networks " IEEE Asia-Pacific Services Computing Conference 2010
[16] Karim El Defrawy "Privacy-Preserving Location-Based On-Demand Routing in MANETs" IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 29, NO. 10 2011
[17] Karim El Defrawy " ALARM: Anonymous Location-Aided Routing in SuspiciousMANEs" IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 10, NO. 9 2011
[18] wei Liu,and Chi Zhang " DELAR: A Device-Energy-Load Aware Relaying Framework for Heterogeneous Mobile Ad Hoc Networks" IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS VOL. 29, NO. 8 2011
[19] Tong Zhou and Romit Roy "P2DAP – Sybil Attacks Detection in Vehicular Ad Hoc Networks " IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 29, NO. 3 2011
[20] Floriano De Rango "Link-Stability and Energy Aware Routing Protocol in Distributed Wireless Networks " IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 23, NO. 4 2012
[21]] Sohail Abbas and Madjid Merabti "Lightweight Sybil Attack Detection in MANETs" IEEE SYSTEMS JOURNAL, VOL. 7, NO. 2, 2013
[22] Haiying Shen "ALERT: An Anonymous Location-Based Efficient Routing Protocol in MANETs " IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 12, NO 2013
[23] Wei Liu "AASR: Authenticated Anonymous Secure Routing for MANETs in Adversarial Environments " IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 63, NO. 9 2014
[25]] Yang Qin, Dijiang Huang "STARS: A Statistical Traffic Pattern Discovery System for MANETs " IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL11, NO. 2 2014
[26]] Behnam Hassanabadi and Shahrokh Valaee " " Reliable Periodic Safety Message Broadcasting in VANETs Using Network Coding "IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 13, NO. 3, 2014
[27] Balasubramanian Paramasivan "Development of a Secure Routing Protocol using Game Theory Model in Mobile Ad Hoc Networks " JOURNAL OF COMMUNICATIONS AND NETWORKS, VOL. 17, NO 1 2-015
[28] Jian-Ming Chang, Po-Chun " Defending Against Collaborative Attacks by Malicious Nodes in MANETs: A Cooperative Bait Detection Approach " Defending Against Collaborative Attacks by Malicious Nodes in MANETs " IEEE SYSTEMS JOURNAL, VOL. 9, NO. 2015
[29] Marwan Al-Jemeli "An Energy Efficient Cross-Layer Network Operation Model for IEEE 802.15.4-Based Mobile Wireless Sensor Networks" IEEE SENSORS JOURNAL, VOL. 15, NO. 2 2015