www.ijecs.in

International Journal Of Engineering And Computer Science ISSN: 2319-7242
Volume 4 Issue 10 Oct 2015, Page No. 14717-14724

Energy Efficient Secure Routing in Manets Based on Multipath Erasure Coding

Sethulekshmi C G[1], Manoj Kumar G[2]

[1]PG Scholar, Computer Science and Engineering,
Poojappura, Trivandrum,
Sethu.lekshmi1@gmail.com

[2]Associate Professor, Computer Science and Engineering,
Poojappura, Trivandrum,
Manojkumar_gg@gmail.com

Abstract: ***Wireless networks can be mainly categorized as, infrastructure wireless networks and infrastructure-less wireless networks. MANET is a type of infrastructure-less wireless network. It is a collection of nodes that dynamically connected together to form a network without using any fixed infrastructure. As it is infrastructure less network, the information or data packets are send between the nodes with the help of radio signals and each node act as routers. Providing efficient networking services in MANETs is very challenging due to mobility and unpredictable radio channel: a significant number of packets can be corrupted or lost. To increase reliability, various measures have been proposed. A more efficient way is to use Network Coding on top of path redundancy and send different, encoded packets on each path. Network coding can improve throughput efficiency. In this work proposing Multipath Erasure Coding for high energy efficient. The use of erasure codes in networks has proved to be promising in order to make communication more robust against both independent and correlated data losses. In particular, erasure codes are an appealing solution to provide communications with increased reliability. Experimental results exhibit consistency with the theoretical analysis, and show that the proposed method achieves higher efficiency when compared to other routing protocol.***

Keywords: *GPSR, ALARM, PRISM, ALERT, Routing, Multipath Erasure Coding.*

1. Introduction

Rapid development of Mobile Ad Hoc Networks (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. MANETs feature self-organizing and independent infrastructures, which make them an ideal choice for uses such as communication and information sharing. Because of the openness and decentralization features of MANETs, it is usually not desirable to constrain the membership of the nodes in the network. In multi-hop wireless networks, the unreliable communication caused by the unstable wireless medium is one of the major challenges. Compared to other methods, such as retransmissions and backup paths, erasure coding has better performance in increasing packet delivery reliability.

Erasure coding is a coding technique that can convert a message into a larger set of coded blocks such that any sufficiently large subset of coded blocks can reconstruct the original message. In this paper integrating erasure coding into the routing problem in multi-hop wireless networks. Most existing works that have applied erasure coding to routing problems in unreliable environments assume that there is no limitation on the number of redundant erasure-coded packets for a message. This assumption is not realistic because the overhead of message transmission can be extremely high without proper restrictions on redundant packets. Therefore, considering an erasure-coding based routing scheme with a pre-defined quantity of redundant packets. The quantity of redundant packets should reflect the importance of corresponding packets because an important packet requires high reliability; and the increment of quantity on redundant packets can directly increase the transmission reliability. The challenge of integrating erasure coding into a routing scheme lies in the fact that the routing algorithm needs to determine not only the optimal quantity of redundant packets, but also the optimal routing path. The cost and the reliability depend on both the specific routing path and the quantity of redundant packets. In this paper, Multipath Erasure Coding for this assumption and integrate the packet quantity into a routing problem in order to achieve a good balance between energy cost and reliability (packet delivery ratio). In doing so, addressing two major challenges one is determining the optimal quantity of redundant packets and the other is determining the optimal routing path. Experimental results exhibit consistency with the theoretical analysis, and show that the proposed method achieves higher efficiency when compared to traditional routing protocol.

2. Mobile Adhoc Networks

S A mobile ad-hoc network (MANET is a self-configuring infrastructure less network of mobile devices connected by wireless links. ad hoc is Latin and means “for this purpose”. Each device 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. MANETs are a kind of wireless ad-hoc networks that usually has a route able networking environment on top of a Link Layer ad hoc network.

A "mobile ad hoc network" (MANET) is an autonomous system of mobile routers(and associated hosts) connected by wireless links - the union of which forms an arbitrary graph. The routers are free to move randomly and organize themselves arbitrarily; thus, the network's wireless topology may change rapidly and unpredictably. Such a network may operate in a standalone fashion or may be connected to larger-Internet. The strength of the connection can change rapidly in time or even disappear completely. Nodes can appear, disappear and re-appear as the time goes on and all the time the network connections should work between the nodes that are part of it. As one can easily imagine, the situation in ad hoc networks with respect to ensuring connectivity and robustness is much more demanding than in the wired case. Ad hoc networks are networks are not (necessarily) connected to any static (i.e. wired) infrastructure. An ad-hoc network is a LAN or other small network, especially one with wireless connections, in which some of the network devices are part of the network only for the duration of a communications session or, in the case of mobile or portable devices, while in some close proximity to the rest of the network. The ad hoc network is a communication network without a pre-exist network infrastructure. In cellular networks, there is a network infrastructure represented by the base-stations, Radio network controllers etc. In ad hoc networks every communication terminal (or Radio Terminal RT) communicates with its partner to perform peer to peer communication. If the required RT is not a neighbor to the initiated call RT (outside the coverage area of the RT), then the other intermediate RTs are used to perform the communication link. This is called multi-hope peer to peer communication. This collaboration between the RTs is very important in the ad hoc networks. In ad hoc networks all the communication network protocols should be distributed throughout the communication terminals (i.e. the communication Terminals should be independent and highly cooperative). Some of the characteristics of Manets are

- Communication via wireless means.
- Node can perform the roles of both host sand routers.
- No centralized controller and infrastructure.
- Dynamic network topology, frequent routing updates.
- Autonomous, no infrastructure needed.
- Can be set up anywhere.
- Energy constraints.

Generally, the communication terminals have a mobility nature which makes the topology of the distributed networks time varying. The dynamical nature of the network topology increases the challenges of the design of ad hoc networks. Each radio terminal is usually powered by energy limited power source (as rechargeable batteries). The power consumption of each radio terminal could be divided generally into three parts, power consumption for data processing inside the RT, power consumption to transmit its own information to the destination, and finally the power consumption when the RT is used as a router, i.e. forwarding the information to another RT in the network. The energy consumption is a critical issue in the design of the ad hoc networks. The mobile devices usually have limited storage and low computational capabilities. They heavily depend on other hosts and resources for data access and information processing. A reliable network topology must be assured through efficient and secure routing protocols for Ad Hoc networks.

3. Application Areas

Some of the applications of MANETs are:

- Military or police exercises.
- Disaster relief operations.
- Mine site operations.
- Urgent Business meetings.
- Robot data acquisition.

4. Advantages of MANETS

The following are the advantages of MANETs:

- They provide access to information and services regardless of geographic position.
- These networks can be setup at any place and time.
- These networks work without any pre-existing infrastructure.

5. Disadvantages of MANETS

Some of the disadvantages of MANETS are:

- Limited resources. Limited physical security
- Intrinsic mutual trust vulnerable to attacks. Lack of authorization facilities
- Volatile network topology makes it hard to detect malicious nodes.

6. Literature Survey

6.1 An Anonymous On-Demand Position-Based Routing.

Proposed a new position- based routing protocol, called an anonymous on-demand position based routing, which keeps routing nodes anonymous. In AODPR, the position of the destination is encrypted with a common key of nodes, and this encrypted position is used for the routing. The main disadvantage of this protocol is less efficiency.

6.2 ALARM:

In this paper [5], addressing some interesting issues arising in such MANETs by designing an anonymous routing framework (Anonymous Location-Aided Routing in Suspicious MANETs). It uses nodes current locations to construct a secure MANET. Based on the current map, each node can decide which other nodes it wants to communicate with. Poor Scalability is the limitation of this protocol.

6.3 PRISM: Privacy-Friendly Routing in Suspicious MANETs and VANETs.

This paper [6] focuses on privacy aspects of mobility. To this end, we construct an on-demand location-based anonymous MANET routing protocol (PRISM) that achieves privacy and security against both outsider and insider adversaries. Disadvantage of PRISM is Additional simulations with larger-scale parameters (more nodes, greater area of movement)
cannot be conducted.

6.4 Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks.

In this paper [7], presenting attacks against routing in adhoc networks, and we present the design and performance evaluation of a new secure on-demand adhoc network routing protocol, called Ariadne. This protocol provide less efficient than the other protocols.

7. Network Attack Models and Assumptions

In ALERT(An Anonymous Location Based Efficient Routing Protocol in MANETs) [9] can be applied to different network models with various node movement patterns such as random way point model and group mobility model. Consider a MANET deployed in a large field where geographic routing is used for node communication in order to reduce the communication latency. The location of a messages sender may be revealed by merely exposing the transmission direction. Therefore, an 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. Moreover, a malicious observer may try to block the data packets by compromising a number of nodes, intercept the packets on a number of nodes, or even trace back to the sender by detecting the data transmission direction. Therefore, the route should also be undetectable. A malicious observer may also try to detect destination nodes through traffic analysis by launching an intersection attack. Therefore, the destination node also needs the protection of anonymity. In this work, the attackers can be battery powered nodes that passively receive network packets and detect activities in their vicinity. They can also be powerful nodes that pretend to be legitimate nodes and inject packets to the network according to the analytical results from their eavesdropped packets. The assumptions below apply to both inside and outside attackers.

7.1 Dynamic Pseudonym and Location Service

As previous works, assume that the public key and location of the destination of a data transmission can be known by others, but its real identity requires protection. We can utilize a secure location service to provide the information of each nodes location and public key. Such a location service enables a source node, who is aware of the identity of the destination node, to securely obtain the location and public key of the destination node. The public key is used to enable two nodes to securely establish symmetric key Ks for secure communication. The destination location enables a node to determine the next hop in geographic routing. Specifically,

trusted normal nodes or dedicated service provider nodes are used to provide location service. Each node has a location server. When a node A wants to know the location and public key of another node B , it will sign the request containing Bs identity using its own identity. Then, the location server of A will return an encrypted position of B and its public key, which can be decrypted by A using the pre-distributed shared key between A and its location server. When node A moves, it will also periodically update its position to its location server. For high reliability, the location serves can replicate data between each other. Thus, the location servers are allowed to fail, because each node can be in contact with all location servers in range. For example, current location service solutions such are able to seamlessly let node switch between location servers. We assume that the attacker will not compromise and utilize the location to find out the real identities of nodes that contact with the compromised location server, which is the common assumption of current location services. We leave the work on secure location service as our future.

The existence of the location servers are opposed to the ad hoc property of MANETs, and it is not necessary to use location servers in a MANET without security consideration. However, anonymous communication requires third-party servers to reliably collect and transmit confidential information, and this solution was used in many of previously proposed works. With the advance of wireless access point (AP), the deployment of location services can be conducted by placing several APs in the whole WIMAX network of civil use at a reasonable cost. It is difficult to preserve all stable location servers in a battle field, but since the location servers are not necessarily be functional all the time and each node only needs to have one usable location server, the location servers can be buried under the ground where anonymous communication is needed.

7.2 The ALERT Routing Algorithm

Fig 1 shows an example of routing in ALERT. 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 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) shows an example where node N3 is the closest to TD, so it is selected as a RF. ALERT aims at achieving k-anonymity 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.

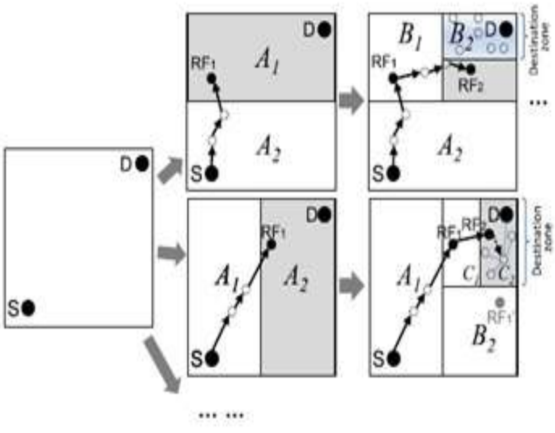

Figure 1: Example for different partitions

ALERT [9] features a dynamic and unpredictable routing path, which consists of a number of dynamically deter-mined intermediate relay nodes. As shown in the upper part, given an area, we horizontally partition it into two zones A1 and A 2. 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, thus dynamically generating an unpredictable routing path for a message.

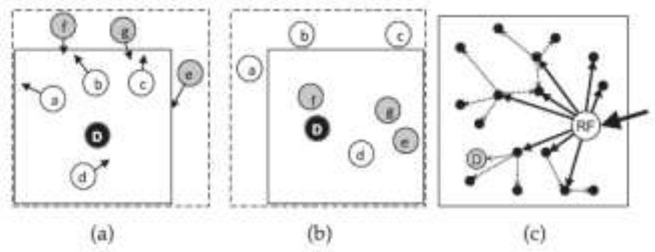

Figure 2: Routing among Zones

Given an S-D pair (Figure 3), the partition pattern in ALERT varies depending on the randomly selected TDs and the order of horizontal and vertical division, which provides a better anonymity protection, shows two possible routing paths for a packet issued by sender S targeting destination D in ALERT. There are also many other possible paths. In the upper routing flow, data source S first horizontally divides the area into two equal-size zones, A 1and A2, in order to separate S and ZD. S then randomly selects the first temporary destination TD1in zone A 1where ZD resides. Then, S relies on GPSR to send packet to TD1. The packet is forwarded by several relays until reaching a node that cannot find a neighbor closer to TD1. This node is considered to be the first random-forwarder RF1. After RF1receives packet, it vertically divides the region A1into regionsB1 and B2 so that ZD and itself are separated in two different zones. Then, RF1randomly selects the next temporary destination TD2 and uses GPSR to send packet to TD2. This process is repeated until a packet receiver finds itself residing in ZD, i.e., a partitioned zone is ZD having k nodes. Then, the node broadcasts the packet to the k nodes. A larger number of hierarchies generate more routing hops, which increases anonymity degree but also increases the delay. To ensure the delivery of packets, the destination sends a confirmation to the source upon receiving the packets. If the source has not received the confirmation during a predefined time period, it will resend the packets.

7.3 Number of Random Forwarders

In ALERT, a Random Forwarder Node is selected in each zone using which routing is done to the destination. There is an advantage of using random selection of a forwarder node; anonymity is provided to the route. Each RF node updates its current details as the source details while forwarding the data. The use of random function is implemented during the selection of the Random Forwarder node. The route anonymity due to chance communicate node selection in the ALERT prevents an interloper from intercepting packets or compromising weak nodes.

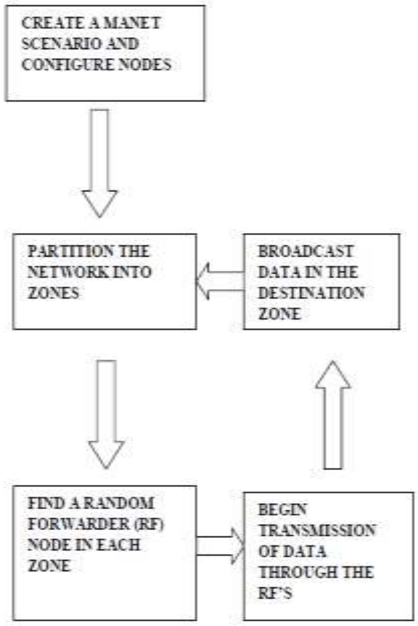
CREATE A MANET SCENARIO AND CONFIGURE NODES
PARTITION THE NETWORK INTO ZONES
BROADCAST DATA IN THE DESTINATION ZONE
FIND A RANDOM FORWARDER (RF) NODE IN EACH ZONE
BEGIN TRANSMISSION OF DATA THROUGH THE RF'S

Figure 3: Random Forward

If the routes between two communicating nodes are constantly changing process, so it is not first level headings: 1. Heading 1 easy for adversaries in an expect the route of the next packet for packet interception. It has sufficient number of nodes perform in the destination node. The number of random forward having different zone partition. The maximum number of partition for a source and destination pair. RF to be increase and linearly number of partitions increase. Route having higher anonymity production two end point. The zones for random forward having smaller to smaller. The random forward are decrease if the anonymity protection is enhanced which are decrease the speed.

8 Multipath Erasure Coding

The main objective of this thesis work is to provide energy efficient secure routing in Mobile Ad-hoc networks with high reliability and low cost. For providing this, a new scheme called Multipath Erasure Coding is included in the routing process. In this scheme instead of selecting one routing path, multiple paths can be selected using hierarchical zone partitioning and ALERT routing algorithm. The data or the packets that can be transferred via these routes are splits using multipath erasure coding. These packets or data are transferred from a node (source) to the detected paths and original data can be received at the destination side. The use of erasure codes in networks has proved to be promising in order to make communication more robust against both independent and correlated data losses. Experimental results exhibit consistency with the theoretical analysis, and show that the proposed method achieves higher efficiency when compared to other routing protocol.

Erasure code is a forward error correction (FEC) code for the binary erasure channel, which transforms a message of k symbols into a longer message (code word) with n symbols such that the original message can be recovered from a subset of the n symbols. The fraction r = k/n is called the code rate, the fraction k/k, where k denotes the number of symbols required for recovery. Erasure coding is a coding technique that converts a message into a set of coded packets such that any sufficiently large subset of the coded packets can be used to reconstruct the original message. In this paper, we assume that the original message has been split into k equal-sized packets. From the angle of linear algebra, each packet split from the original message can be regarded as a variable, and an erasure-coded packet is a linear combination of the k original packets. The quantity of erasure-coded packets is the key to balancing the trade-off between reliability and cost. In simple case, where sources can directly communicate with destination d, but packet loss exists. In order to increase the chance that d will receive the message block, s breaks the message block into k (fixed) packets and generates redundant packets through erasure coding. As long as d can receive at least k packets from the ts packets sent by s, d can restore the original message block through decoding, we assume that the probability of success of each transmission is independent.

8.1 System Architecture

The figure 4 shows the system architecture. In this system source node knows the details about the destination. It first do Ex-OR encryption for encrypting the data using the secret key generated from key rotation protocol. These encoded or encrypted data is send via multiple paths detected by using alert routing algorithm which means that forwarding the encoded data to the relay nodes, it then finds RF(Random forwarders)
nodes using GPSR algorithm. When the packet reaching to each RFs it will check whether to forward or drop the data. When the corresponding Ex-OR'ed encoded packet reaches the destination, it will reconstruct or merge the data as original by using destination's private key. The advantage of this system is if a data loss from any one path occur, the destination can predict the lost data by using error correction method.

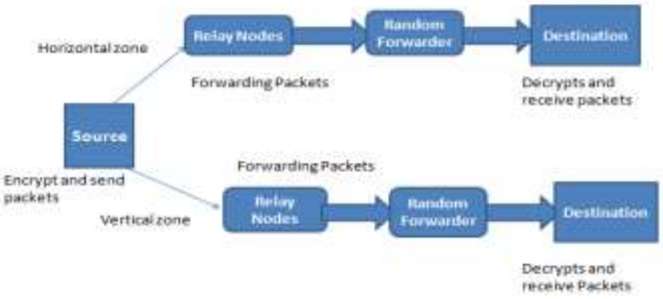

Figure 4: System Architecture

The data flow diagram for the proposed method is shown below:

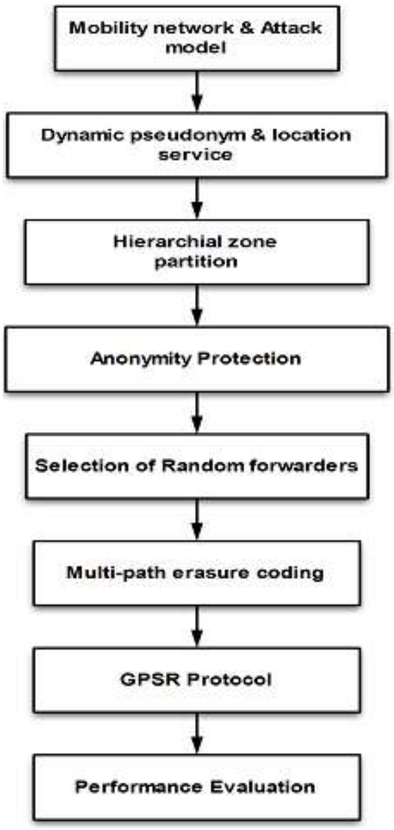
Mobility network & Attack model
Dynamic pseudonym & location service
Hierarchial zone partition
Anonymity Protection
Selection of Random forwarders
Multi-path erasure coding
GPSR Protocol
Performance Evaluation

Figure 5: Data flow diagram

9 Simulation Results

The tests were carried out on NS-2.33 simulator using 802.11 as the MAC protocol with a standard wireless transmission range of 250 m and UDP/CBR trace with a packet size of 512 bytes. The test field in our experiment was set to 1000m x 1000 m area with 200 nodes moving at a speed of 2 m/s, unless otherwise specified. The density was set to 50, 100, 150, and 200 nodes per square meters. The duration of each simulation was set to 100 s unless otherwise indicated. The number of pairs of S-D communication nodes was set to 10 and S-D pairs are randomly generated. S sends a packet to D at an interval of 2 s. The final results are the average of results of 30 runs. The encryption algorithm is single threaded, running along with other parts of the experiment on a 1.8 Ghz processor. A typical symmetric encryption costs several milliseconds while a public key encryption operation costs 2-3 hundred milliseconds.

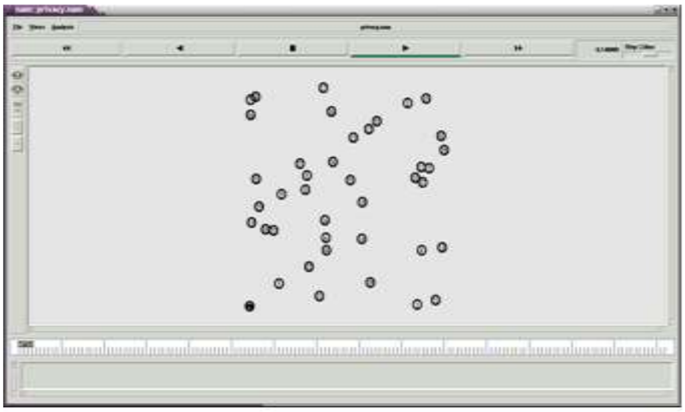

Figure 6: Nodes mobility before horizontal/vertical partition

Fig 6 shows the mobility of nodes during the start of simulation. Initially creating 100 nodes and shows the packet forwarding and packet loss during predefined time interval.

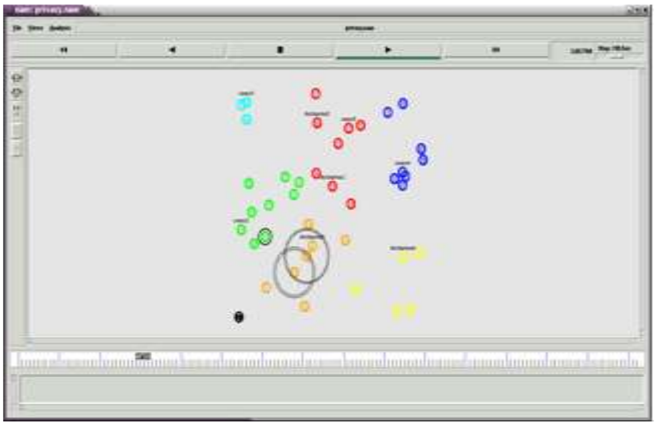

Figure 7: Packet forwarding and node mobility after zone partition based on multipath erasure coding.

10 Performance Evaluation

This work use the following metrics to evaluation the routing performance in terms of effectiveness on anonymity protection and efficiency:

- **The number of actual participating nodes:** These nodes include RFs and relay nodes that actually participate in routing. This metric demonstrates the ability of ALERTs randomized routing to avoid routing pattern detection.

- **The number of random forwarders:** This is the number of actual RFs in an S-D routing path. It shows routing anonymity and efficiency.

- **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. A larger number provides higher anonymity protection to a destination and to counter the intersection attack. We measure this metric over time to show effectiveness on the destination anonymity protection.

- **The number of hops per packet:** This is measured as the accumulated routing hop counts divided by the number of packets sent, which shows the efficiency of routing algorithms.

- **Latency per packet:** This is the average time elapsed after a packet is sent and before it is received. It includes the time cost for routing and cryptography. This metric reflects the latency and efficiency of routing algorithms.

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

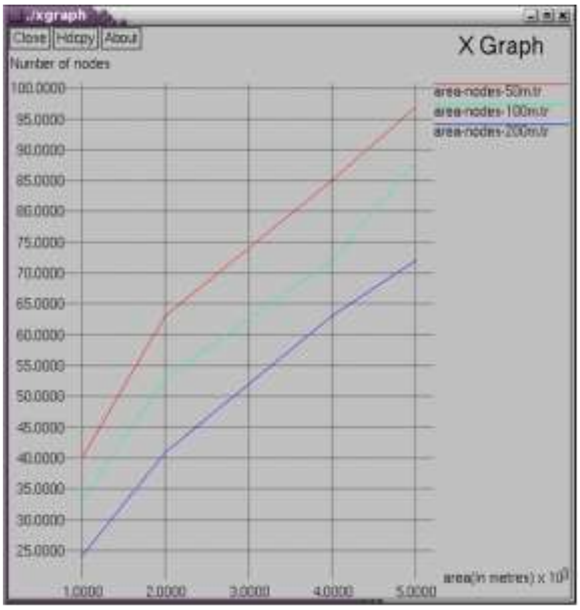

Figure 8: Area with respect to number of nodes.

Fig 8 shows when area of each region decreases the requirement for number of nodes decreases because of this mobility of node increases. When mobility increases number of nodes in the region decreases. So the performance level is high in the proposed method. Mobility of node or speed may be fast or slow. With respect to the mobility of node we can estimate the average node privacy. When mobility increases, privacy increases.

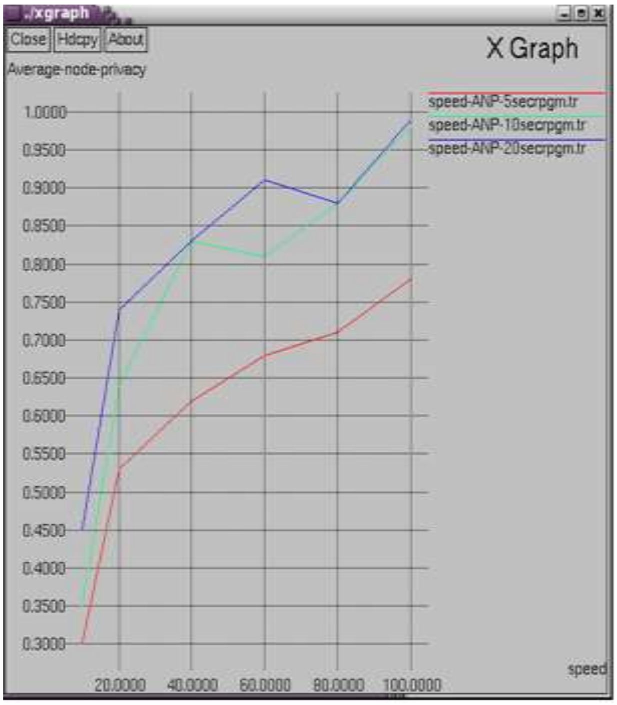

Figure 9: Privacy with respect to mobility of nodes.

In Figure 9: node count means, we first dividing the network area into zones, when number of partition increases privacy increases, otherwise privacy decreases.

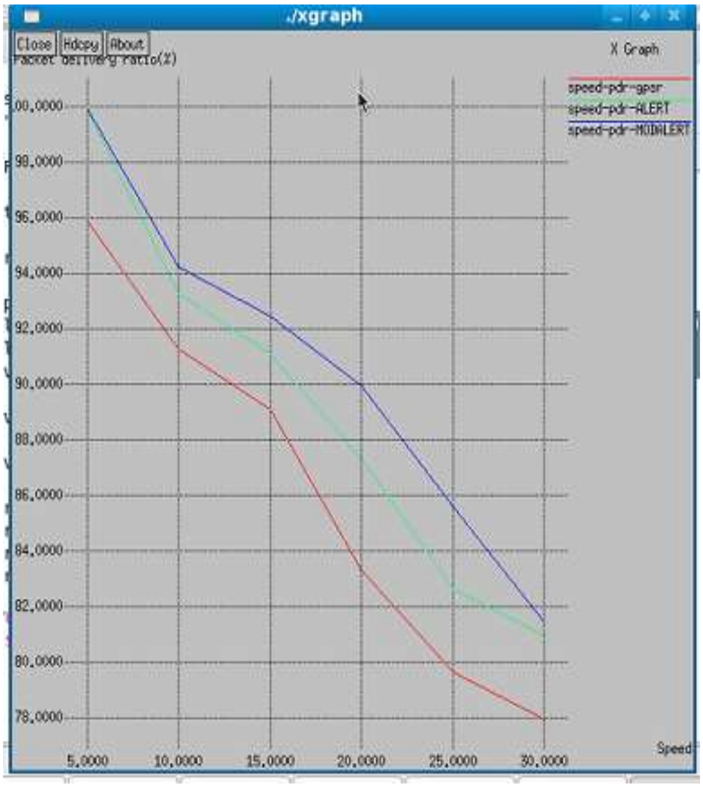

Figure 10: Performance of packet delivery ratio (Comparison)

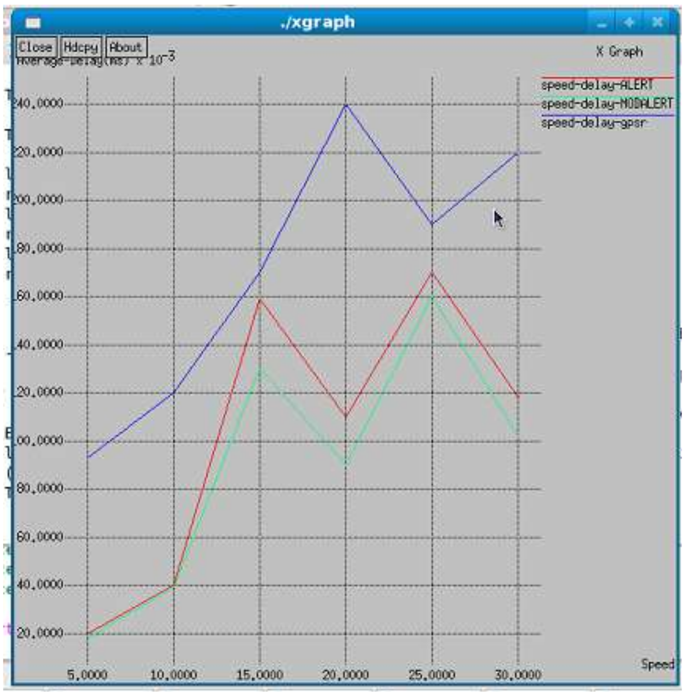

Figure 11: Comparison of Average delay

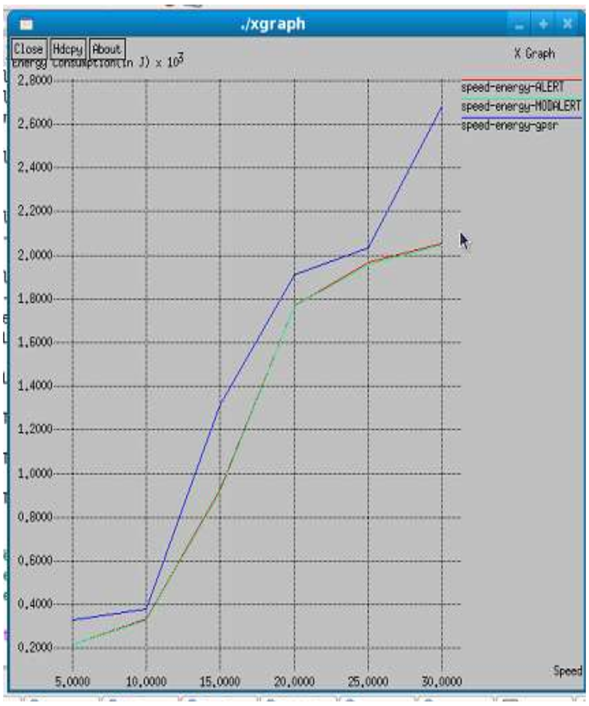

Figure 12: Energy Comparison in GPR,ALERT and Proposed System

Conclusion

Existing anonymous routing protocols depend on either hop-by-hop encryption or redundant traffic which generates high cost. In case of acknowledgement free communication the source doesn't know whether the data is reached to destination or not. So the source node continuously send data to the detected path, here comes the disadvantages of data loss, energy consumption and packet delivery ratio. The use of erasure codes in networks has proved to be promising in order to make communication more robust against both independent and correlated data losses. With the help of erasure codes data can be splitted and send to multiple paths ,there is no need for sending data continuously because the data will definitely reached to its destination via any one of the path. Erasure codes are an appealing solution to provide communications with increased reliability and high energy consumption.

References

[1] A. B. Zhu, Z. Wan, M.S. Kankanhalli, F. Bao, and R.H. Deng,Anonymous Secure Routing in Mobile Ad-Hoc Networks, Proc.IEEE 29th Ann. Intl Conf. Local Computer Networks (LCN), 2014.

[2] 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.

[3] Sk.Md.M. Rahman, M. Mambo, A. Inomata, and E. Okamoto, An Anonymous On-Demand Position-Based Routing in Mobile Ad Hoc Networks, Proc. Intl Symp. Applications on Internet (SAINT), 2006.

[4] Z. Zhi and Y.K. Choong, Anonymizing Geographic Ad Hoc Routing for Preserving Location Privacy, Proc. Third

Intl Workshop Mobile Distributed Computing(ICDCSW), 2005.

[5] K.E. Defrawy and G. Tsudik, ALARM: Anonymous Location-Aided Routing in Suspicious MANETs, , Proc. IEEE Intl Conf.Network Protocols (ICNP),, 2007

[6] K.E. Defrawy and G. Tsudik, PRISM: Privacy-Friendly Routing in Suspicious MANETs (and VANETs), Proc. IEEE Intl Conf. Network Protocols (ICNP),, pp. 285-295, 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] K. El-Khatib, L. Korba, R. Song, and G. Yee, Anonymous Secure Routing in Mobile Ad-Hoc Networks, Proc. Intl Conf. Parallel Processing Workshops (ICPPW), 2003.

[9] L. Zhao and H. Shen, ALERT: An Anonymous Location-Based E_cient Routing Protocol in MANETs, Proc. Intl Conf. Parallel Processing (ICPP), 2011.

[10] Haiying Shen and Lianyu Zhao ALERT: An Anonymous Location-Based Efficient Routing Protocol in MANETs, IEEE Transaction on Mobile Computing, vol. 12, no. 6, June 2013.

[11] JianWu,Stefan Dulman,Paul Havinga,Tim Nieberg "Multipath Routing with Erasure Coding for Wireless Sensor Networks" IEEE Conference, 2001 .