GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

EFFICIENT NEIGHBOR ROUTE DISCOVERY PROTOCOL [ENRDP] FOR POSITION VERIFICATION IN MANET

J. Kavitha[1] and Dr.Mrs.P.Krishnakumari[2]
M Phil Research Scholar, RVS College of Arts & Science, Coimbatore , India[1]
Director MCA Department, RVS College of Arts & Science, Coimbatore , India[2]

ABSTRACT

Energy awareness and protocol management is becoming an important factor in the design of MANET protocols. Because of mobility, it needs the support of scalable routing strategies. These protocols try to consider the path duration in order to respect some QoS constraints and to reduce fake neighbor position for route discovery. In the existing system communication and packet delivery ratio decreases when neighbor discovery fails. The proposed ENRDP protocol selects the stable path to reduce the fake position and communication overhead. It selects the stable path, so neighbor discovery failure decreases and there by increases the packet delivery ratio and reduces energy consumption, End-to-End delay and packet lost. The effectiveness of ENRDP protocol is demonstrated through NS2 stimulation.

Keywords: MANET, ENRDP, Neighbor discovery, Secure neighbor Discovery, Neighbor position verification.

I. INTRODUCTION

Wireless Mobile Ad Hoc Networks (MANETs) have emerged as an advanced networking concept based on collaborative efforts among numerous self-organized wireless devices. MANET is a network where no fixed infrastructure exists. Such networks are expected to play vital role in future civilian and military settings, being useful to provide communication support where no fixed infrastructure exists or the deployment of a fixed infrastructure is not economically profitable and movement of communicating parties is possible. The topology of MANETs is dynamic, because the link among the nodes may vary with time due to device mobility, new device arrivals, and the possibility of having mobile devices. Hence, any routing protocol design must consider the physical limitations and constraints imposed by the ad hoc environment so that the resulting routing protocol does not degrade system performances. Since in MANET, there is no fixed-infrastructure such as base stations, mobile devices need to operate as routers in order to maintain the information about the network connectivity, as a result the Conventional routing protocols cannot be supported easily by ad hoc networks. Several research studies have been launched to study this issue, those defined by the IETF MANET group can be classified into two categories: proactive protocols and reactive protocols. MANET's technology offers both new challenges and opportunities for many applications [14].

The major challenges for ad hoc technology is secure and efficient routing, due essentially to MANET features (e.g., open medium, lack of centralized management, nodes mobility). Several approaches have been introduced to secure ad hoc routing. Some existing solutions in wireless networks employ mechanisms used to protect routing protocols in wired networks that are based on the presence of a centralized infrastructure. These solutions are not appropriate for a decentralized ad hoc network. In mobile ad hoc networks, neighbor discovery is the process by which a node in a network determines the total number and identity of other nodes in its vicinity [14]. It is a fundamental building block of many protocols including localization, routing, leader election, and group management. Time-based communications and many media access control mechanisms rely on accurate neighbor information.

Neighbor discovery is especially important to the proper functioning of wireless networks. In wireless networks, neighbors are usually defined as nodes that lie within radio range of each other. Thus, neighbor discovery can be considered as the exploration of the volume of space or "neighborhood" immediately surrounding a wireless node [13]. Nodes found within the neighborhood are neighbors and, depending on network configuration and topology, may cooperate in the performance of various tasks including communications, routing and localization. However, wireless communications are vulnerable to attacks. Attackers have the freedom to perform malicious activities ranging from simple denial of service to sophisticated deception. In this paper, so here explore the security problem and neighbor selection in route discovery in mobile ad hoc networks by proposing a new security aspect for DSR on-demand protocol.

The ENRDP protocol is specifically designed to an open ad hoc network where each node must verify the identity of the node with which it communicates. This allows nodes to be authenticated before taking into account any information during the route discovery. In ENRDP focus on attacks carried out by traditional external illegitimate nodes which do not have the access rights to the network. Taken into consideration several attacks carried out by internal malicious nodes which inject false information about their position. Moreover, the ENRDP solution ensures the reliability and stability of the route discovery process. The contributions are illustrated in what follows:

- A new secure and efficient route discovery based on DSR
- ENRDP protocol will ensure the establishment of a route between two nodes if it exists
- Detecting and rejecting adversaries
- Select the most stable path for transmitting data among remaining true neighbors based on path stability, residual energy and total energy needed to process and transmit the data

II. RELATED WORK

Most of the routing algorithms proposed for MANETs are based on reactive routing strategy, in which route is established only when there is a need to transmit a packet. In these protocols route recovery and maintenance procedures are initiated only after a route break. This procedure consumes extra bandwidth and power at processing nodes and also increases the delay. It is important to find routes that last longer, to reduce the route breakage and consumption of resources.

T-Cabrera, A., N-Perez, proposed Link stability is defined as a measure of how stable the link is and how long the communication will endure. Signal Strength is one of the parameter used to estimate the stability of links [1]. C-K. Toh, proposed the route discovery is based on signal strength and location stability of nodes [2], [3]. SSA, a mobile node determines the average signal strength at which the packets are exchanged between Nodes and location stability is used to choose longer-lived route. Sulabh Agarwal and Pal Singh proposed RABR [4], in which the route selection is done based on the intelligent residual lifetime assessment of the candidate routes. This major challenge with this protocol is, to choose the optimal threshold values. Hwee Xian et.al the authors estimated the link stability based on the signal strength [5]. If the received signal strength is greater than a certain threshold, the link is considered to be stable.

Min-Gu and Sunggulee proposed a route selection based on Differentiated signal strength [DSS], [6]. DSS indicates whether the nodes are getting closer or getting farther apart. If the signal strength is getting stronger, the link is considered to be stable. If the signal strength is getting weaker in case of node moving away is considered to be unstable link. N.Sharma and S.Nandi proposed RSQR in which the link stability and route stability are computed using received signal strength. Based on the threshold values the links are classified as stable or unstable link. Link stability and link uncertainty values are used for stable route selection among all the feasible routes. Gun Woo and Lee proposed EBL [8], in which the authors give importance to both link stability and the residual Battery capacity. The EBL not only improve the energy efficiency but also reduce network partition.

Floriano and Guerriero proposed LAER [9], in which they consider joint metric of link stability and energy drain rate into route discovery, which results in reduced control overhead and balanced traffic load. The expected route lifetime is mainly predicted with the parameters node battery energy and link stability. It is preferable to select stable links i.e. links having longer predicted lifetime, instead of selecting weak links which break soon and introduce routing overhead [10]. Guerriero proposed PERRA, a reactive routing protocol, which accounts both link stability and power efficiency [11]. Intermediate nodes in PERRA propagates route request, only if it meet the energy requirement specified by the source node. Thus, the path established is a stable path that incurs residual energy, path stability and estimated energy for data transmission. It also maintain alternate path, which can be used before link break occurs to reduce the path breakage.

Ahamed nabet et.al is proposed an efficient secure routing protocol (ASRP) to ensure the routing security in ad hoc networks. ASRP provides powerful security extensions to the reactive AODV protocol, based on modified secure remote password protocol and Diffie-Hellman (DH) algorithms.

III. EXISTING SYSTEM

Neighbor discovery is the process by which a node in a network determines the total number and identity of other nodes in its vicinity. It is a fundamental building block of many protocols including localization, routing, leader election, and group management. Time-based communications and many media access control mechanisms rely on accurate neighbor information. Neighbor discovery is especially important to the proper functioning of wireless networks. In wireless networks, neighbors are usually defined as nodes that lie within radio range of each other. Thus, neighbor discovery can be considered as the exploration of the volume of space or “neighborhood” immediately surrounding a wireless node [15]. Nodes found within the neighborhood are neighbors and, depending on network configuration and topology, may cooperate in the performance of various tasks including communications, sensing and localization. However, wireless communications are susceptible to abuse. Attackers have the freedom to perform malicious activities ranging from simple denial of service to sophisticated deception.

Location-based Technique

It offer neighbor discovery protocols to ensure that nodes claiming to be neighbors share the same neighborhood. It uses localized beacons to detect wormholes while executing a localization protocol for statically deployed nodes [13]. A mechanism for geographically assigning local broadcast keys was used to limit the range of communications. However, location-based protocols assume the availability of localization information, at least for a subset of participating nodes, making them unsuitable for scenarios without this information [15].

Secure neighbor discovery (SND) Technique

It deals with the identification of nodes with which a communication link can be established or that are within a given distance. SND is only a step toward the solution, so simply put, an adversarial node could be securely discovered as neighbor and be indeed a neighbor (within some SND range), but it could still cheat about its position within the same range. In other words [13], SND is a subset of the NPV problem, since it lets a node assess whether another node is an actual neighbor but it does not verify the location it claims to be at.

Neighbor position verification (NPV) Technique

It was studied in the context of ad hoc and sensor networks; however, existing NPV schemes often rely on or mobile trustworthy nodes, which are assumed to be always available for the verification of the positions announced by third parties. In ad hoc environments, however, the pervasive presence of either infrastructure or neighbor nodes that can be aprioristically trusted is quite unrealistic [15]. This protocol is autonomous and does not require trustworthy neighbors.

NPV routing protocol

NPV protocol is first lets nodes calculate distances to all neighbors, and then commends that all triplets of nodes encircling a pair of other nodes act as verifiers of the pair’s positions. This scheme does not rely on trustworthy nodes, but it is designed for static sensor networks, and requires lengthy multi round computations involving several nodes that seek consensus on common neighbor verification [13]. Moreover, it aims at assessing not the position but whether the node is within a given region or not.NPV solution, instead, allows any node to validate the position of all of its neighbors through a fast, one-time message exchange, which makes it suitable to both static and mobile environments.

IV. PROPOSED WORK

To ensure the reliability and stability of the routing process here Efficient Neighbor Route Discovery Protocol (ENRDP). First it is provide a distributed, lightweight solution to the neighbor position verification problem that need not require infrastructure or a priori trusted neighbors and is robust against several different attacks, including coordinated attacks by independent and colluding adversaries. Next, it provides best selection of neighbor based on the stability of the link. The working procedure of ENRDP protocol is described in the Fig.1.Dividing the ENDRP protocol in to two tasks.

1) Distributed cooperative NPV
2) Path stability prediction technique

Distributed cooperative scheme for NPV

A fully distributed cooperative scheme for NPV, which enables a node, called verifier, to discover and verify the position of its communication neighbors. A verifier can initiate the protocol at any time, by triggering the message exchange called POLL, REPLY, REVEAL and REPORT, within its 1-hop neighborhood.
To check with their neighbor position and secure transmission of content to the proper
Destination.

Step 1: discover nodes in range.

Step 2: send request to nodes

Step 3: wait for connection

Step 4: get location from peers with time.

Step 5: maintain location table
Step 6: broadcast the location to other nodes
Step 7: get response from other
Step 8: verify the destination location and response from other nodes
Step 9: check for location data at every request or operation
Step 10: if the location of peer is invalid mark it as spam (by its mac id)
Step 11: broadcast the spammed peer mac id to all other nodes.

Discover own location and neighbor location:

Discovering own location and neighbor location is tedious task in mobile ad hoc network. In this stage of process it’s used to find the own location and Neighbor location through the wifi integrated service. These findings are used to involve in the neighbor position verification.

Connection between neighbor nodes

Connection establishment with neighbor and accept connection by their neighbors made a connection more secure. In this stage it’s used to follow initial security mechanism through the cryptography techniques. Connections with their neighbors are established here using AES cryptography technique. Connection need to be accepted in both ends then only source can sent secure message transaction. Neighbor position verification algorithm used to check all with their neighbor through above mentioned steps to verify their neighbors.

Secure content transaction

Secure content transaction to secure discovered neighbor destination. Position verification done through NPV algorithm and the message and attachments, whatever I need to send to the secure neighbor are happened to be here. Use send option after attachments and secure neighbor node selected.

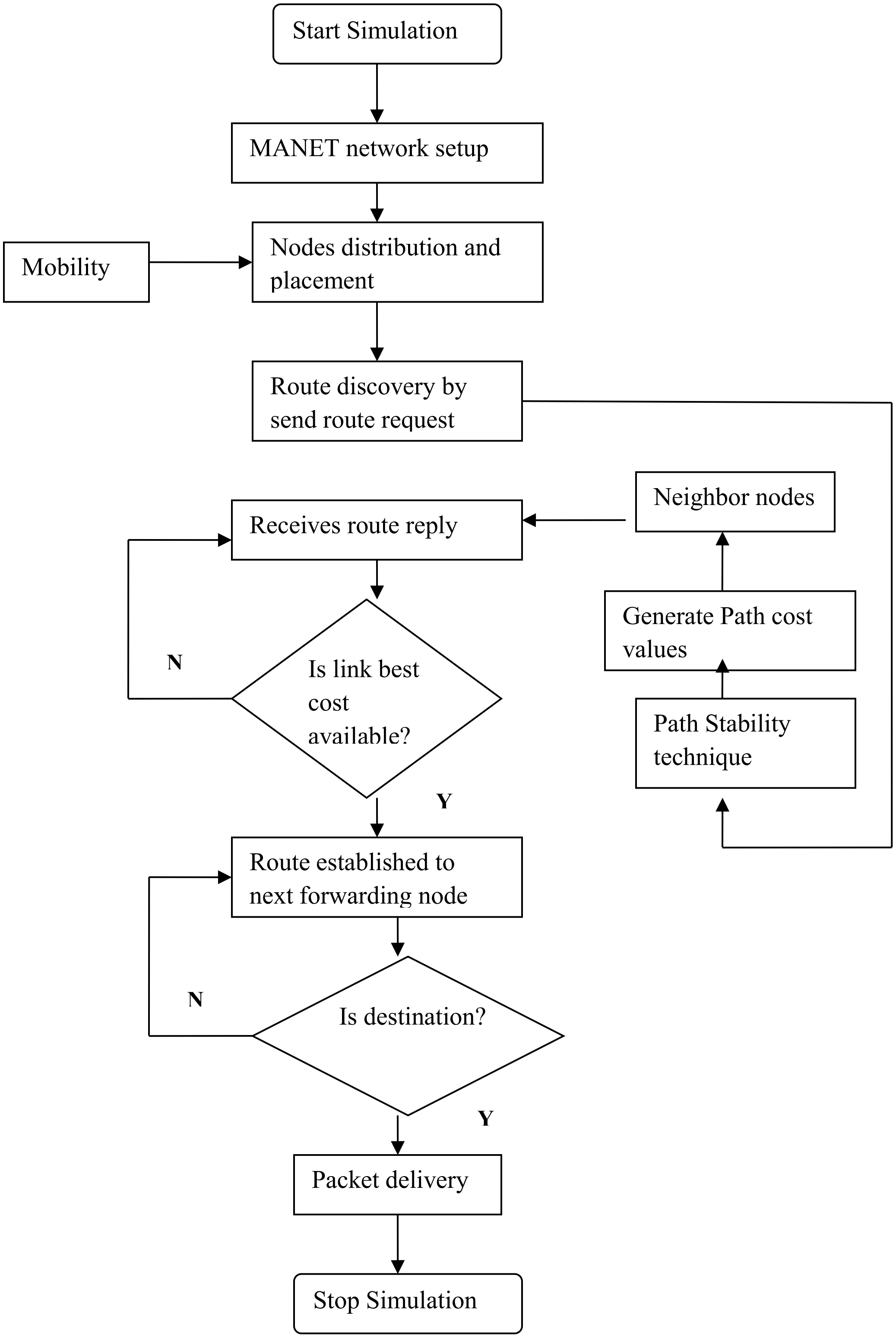
Start Simulation
MANET network setup
Mobility
Nodes distribution and placement
Route discovery by send route request
Neighbor nodes
Receives route reply
Generate Path cost values
N
Is link best cost available?
Path Stability technique
Y
Route established to next forwarding node
N
Is destination?
Y
Packet delivery
Stop Simulation

Fig.1.ENRDP protocol

The aim of the message exchange is collect information that it is used to compute distances between any pair of its communication neighbors. The POLL and REPLY messages are first broadcasted by verifier and its neighbors, respectively. These messages are anonymous, allowing nodes to record reciprocal timing information without disclosing their identities. Then, after a REVEAL message broadcast by the verifier, nodes disclose to verifier, through REPORT messages. The REPORT messages are secure and authenticated. Neighbor nodes identities as well as the anonymous timing information are collected. The verifier uses such data to match timings and identities; then, it uses the timings to perform ranging and compute distances between all pairs of communicating nodes in its neighborhood. Propose a lightweight, distributed, and efficient protocol that enables each node to discover and verify the position of its neighbors. The protocol can be executed at any point in time, without prior knowledge or assumed trustworthiness of the other nodes that participate by any node.

A fully distributed cooperative scheme for NPV protocol allows any node in the network to discover and verify the position of its communication neighbors that participate in the protocol message exchange. The procedure is performed in a reactive manner, i.e., it can be run by any node at any time instant, by initiating the message exchange. Such node will be referred to as the verifier. Based on this knowledge, the verifier performs security tests to tag its communication neighbors as:

· Verified, i.e., nodes the verifier deems to be trustworthy; · Faulty, i.e., nodes the verifier deems to have announced an incorrect position;

· Unverifiable, i.e., nodes the verifier cannot prove to be either correct or faulty – this may happen due to lack of sufficient information on these nodes or because the verifier cannot form a clear opinion on their behavior. Clearly, the objective of the protocol is to be robust to adversarial nodes in that it minimizes the number of unverifiable nodes and the number of positive/negative false.

Path stability prediction technique

A fundamental issue arising in mobile ad hoc networks (MANETs) is the selection of the optimal path between two nodes. Ensuring a path to be valid for adequately longer period of time is a very difficult problem in MANET due to its high mobility nature. A method that has been advocated to improve routing efficiency is to select the most stable path so as to reduce the latency and the overhead due to route reconstruction. As per Distributed cooperative scheme for NPV technique, solves the neighbor verification and this scheme does not concentrate on link failures which is more often in MANET network so neighbor position verification is not get optimized results thus provide solution to link breakages through path quality technique and enhance neighbor position verification technique as per path quality technique which delivers results in efficient manner.

Route maintenance and route discovery procedures are similar to the DSR protocol, but with the route selection based on the three aforementioned metrics. Delivery probabilities are synthesized locally from context information's like value describes the above metrics. A delivery probability of each node is used to select link stability path over dynamic route discovery.

ENRDP routing protocol

Efficient Neighbor Route Discovery Protocol (ENRDP) is very evident that two major factors neighbor position verification, mobility and energy efficiency need to be considered to assure better network performance. Especially while assuring QoS in MANET environment nodes should not die due to power constraint or the links should not expire due to mobility in the middle of the transmission. So the target is to choose a more stable path considering higher link stability and less cost along predicted higher life path. It combines the idea of link stability calculation based on mobility prediction and best neighbor selection in terms of cost and lifetime along with QoS support.

Table.1.Stimulation Parameters

Parameter name	Parameter value
Stimulation tool	NS2
Antenna	Omni antenna
Channel	Wireless
Routing protocol	DSR
Number of Mobile nodes	40
Interface	CMUPri queue
Communication agent	TCP
MAC type	802-11
LL	Link layer type

V. PERFORMANCE EVALUATION

The metrics used in evaluating the performance are:

Packet Delivery Ratio: The ratio between the, number of received data packets to the number of total data packets sent by the source.

Packet delivery ratio=Number of packet received /Number of packet send into 100

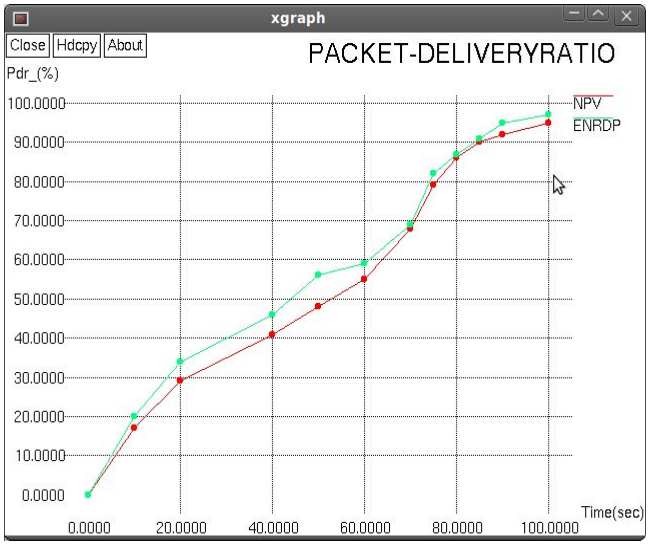

Fig.2 Packet Delivery Ratio

Average End-to-End delay: The average time elapsed for delivering a data packet within a successful transmission from source to destination.

End to end delay=Inter arrival of 1st packet time& 2nd packet time /
Total packet data delivery time.

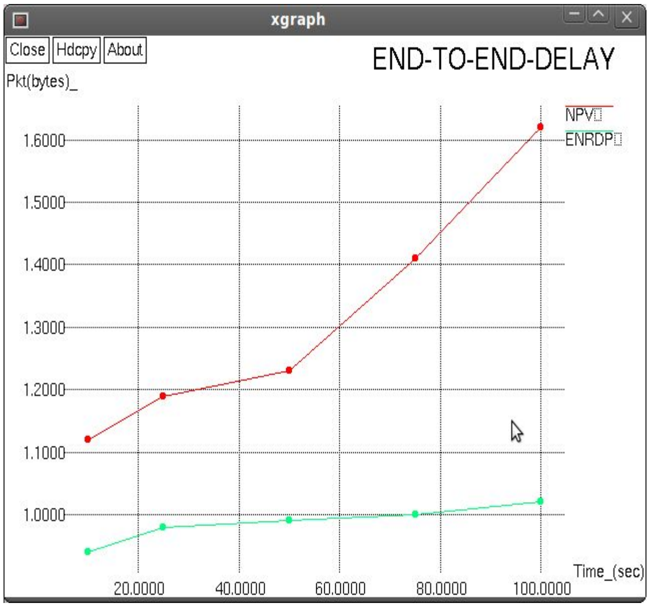

Fig.3 End_End Delay

Packet Lost:

The discarding of data packets in a network when a router, is overloaded and cannot accept any incoming data at a given moment.
Packet lost=total number of packet received-Send

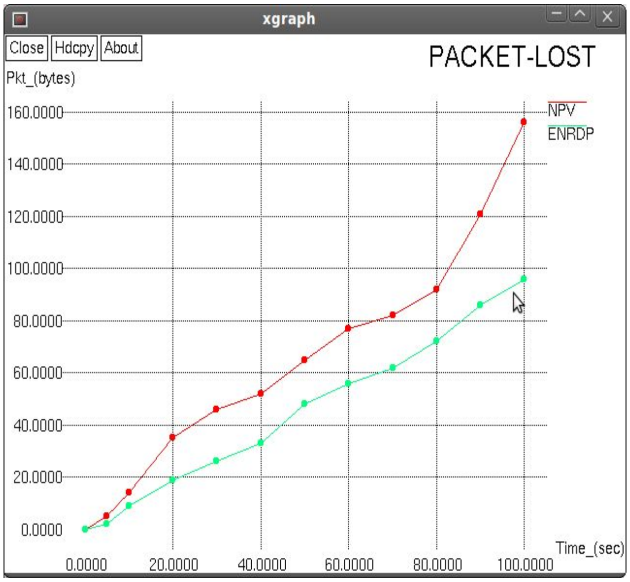

Fig.4 Packet Lost

Energy consumption

The energy consumption for the entire network, including transmission and processing energy consumption for both the data and control packets.
Energy consumption=Energy consumed on IDL sleep, transmit and receive/
Total energy consumed

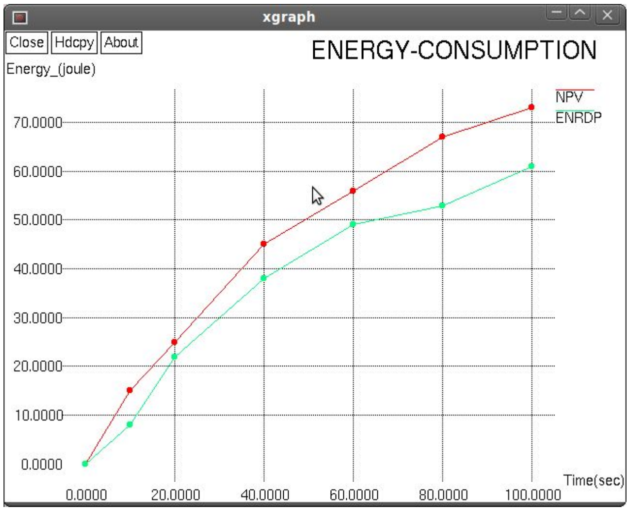

Fig.5. Energy consumption

VI. CONCLUSION

Mobile ad hoc networks, knowledge of neighbor positions are important task. Distributed techniques to perform secure neighbor position discovery, suitable for highly mobile ad hoc environments, ENRDP system under discovery of neighbor by avoiding false positions neighbors and also addressed the selection of stable path among the neighbors which not only describes the selection of correct position neighbors but also best link stability neighbors. Thus overcome the adversary and also link failures. both the availability and the duration probability of a routing path that is subject to link failures caused by node mobility in terms of malicious activities. Then ENRDP protocol is simulated the in NS-2. The parameters like throughput, delay, packet lost and packet delivery ratio of the proposed protocol are compared with that of existing and ENRDP. This performance has reduced the packet lost, delay and increases the delivery ratio, throughput of the network.

VII. REFERENCES

[1] Ahmed Nabet, RidaKhatoun, LyesKhoukhi, Juliette Dromard and Dominique Gaïti "Towards Secure Route Discovery Protocol in MANET," IEEE 2011.

[2] C. LOURDU RAJA "Neighbor Position Verification in Mobile Ad Hoc Network", ISSN (Online): 2320-9801, Vol.2, Special Issue 1, and March 2014.

[3].C-K. Toh, "Associativity-Based Routing for Adhoc Mobile Networks," IEEE Personal Communications, Vol.4, No. 2, pp.103 – 139, March 1997.

[4] F.D. Rango, F. Guerriero, "Link Stability and Energy Aware Routing Protocol in Distributed Wireless Networks", IEEE Transactions on Parallel and Distributed systems, vol.23, no. 4, April 2012.

[5] F.Guerriero "ABiojective Optimization Model for Routing in Mobile Ad-hoc Networks", IEICE Trans. Comm. Pp 4588- 4597.

[6] G.W. Park, S.Lee, "A routing protocol for Extent Network Lifetime through the Residual Battery and Link Stability in MANET", ACC '08, Istanbul, Turkey, May 27-30, 2008.

[7] Hwee Xian, Winston Seah, "Limiting Control Overheads Based on Link Stability for Improved performance in Mobile Adhoc Networks", Springer, UNCS3510, pp.258-268. WWIC 2005.

[8] Lee, M.-G., & Lee, S. "A link stability model and stable routing for mobile ad-hoc networks", LNCS4096, Seoul, Korea, pp. 904–913, in EUC.2006.

[9] Marco Fiore, Claudio EttoreCasetti, Carla-FabianaChiasserini, and PanagiotisPapadimitratos, "Discovery and Verification of Neighbor Positions in Mobile Ad Hoc Networks", IEEE Transactions on Mobile Computing, VOL. 12, No. 2, February 2013.

[10] NityanandaSarma, Sukumar Nandi, "Route Stability Based QoS Routing in Mobile Ad Hoc Networks", Springer, March 2009.

[11] Priyanka Goyal1, Vinti Parmar, and Rahul Rishi "MANET: Vulnerabilities, Challenges, Attacks, Application". ISSN: 2230-7893, January 2011.

[12] R.Dube, C.D. Rais, K. Wang and S.K. Tripathi, "Signal Stability Based Adaptive Routing for Ad-Hoc mobile network IEEE Personal Communication, Feh 1997.

[13] S. Singh, M. Woo, and C.S. Raghavendra, "Power-aware routing in mobile ad hoc networks," in Proc. Int. Conf. Mobile Computing and Networking, pp. 181-190, 1998.

[14] SulobhAgorcvol, AshishAhujo, Jorinder Pol Singh, "Route-Lifetime Assessment Based Routing (RABR) Protocol for Mobile Ad-Hoc Networks".

[15] T-Cabrera, A., N-Perez, I., Casilari, E., F. J &Ganete. "Ad hoc routing based on the stability of routes", in MobiWAC'06, Terromolinos, Spain, pp. 100–103. 2006.