Middle-East Journal of Scientific Research 25 (2): 260-267, 2017
ISSN 1990-9233
© IDOSI Publications, 2017
DOI: 10.5829/idosi.mejsr.2017.260.267

An Eminent Protocol for P2P File Sharing adopting Anycast Routing Strategy in MANET

K.B. Gurumoorthy, R. Jenifer Prarthana, B. Anandhaprabakaran and K. Rajeshwaran

Department of Electronics and Communication Engineering,
Sri Ramakrishna Engineering College, Coimbatore, Tamilnadu, India

Abstract: Ad hoc Network (MANETs) is the recent and emerging trend in all sorts of hotspots that are disseminated in the distributed domain. A proficient yet a modest routing that makes use of the any cast based routing protocol is designed exclusively for MANETs that are to be employed in P2P applications. A presumption taken over is that the number of anycast groups is steady in the ad hoc network considered here. So we cogitate for an instance that, when a mobile node seams with an anycast group or leaves an anycast group, it is done with an accomplishment of an additional service such as a file or a particular data. It pledges a request packet and sends it to the network layer and then shares its resources to added nodes. The anycast group ID is restructured correspondingly and broadcasts the contents with relevance to the updating information. This anycast based protocol is designed exclusively for P2P applications in mobile wireless ad hoc networks that have their roots based with on-demand routing protocols. The traffic load can be well-adjusted by cutting down the transmission delay and by rather enhancing the route utilization which proves to be superior for P2P application. All the members in an anycast group would share its unique anycast address and would be identified by that particular unique anycast address. This empowers them with the ability to take the same priority in the route searching process. Therefore, this approach promises a transmission path with the shortest distance. The traffic load is apparently distributed in the network with the aid of the fact that the anycast server is scattered over the given geographical area. All these properties work together in a chain to enhance the QoS parameters of the network.

Key words: MANETs · Anycast · QoS · DSR routing · P2P

INTRODUCTION

In this modern era of communication and technological advancements, smart phones and laptop have taken over the massive onlookers. Indeed, the number of smart phone utility have increased to 1.31 billion worldwide in 2013 and is expected to mount into a double rate of around 2.16 billion by 2020. This massive hike in the number of mobile users is forgoing to a desirable future, where people could easily transfer or share documents and files within a fraction of second whenever and wherever it is possible / on demanded. Moreover, the ease of file sharing is expected to be dramatically enhanced in the whole aspect. In the present scenario, the mobile users connect or interlude with each other through a geographically disseminated base stations. The current communications of mobile users is through infrastructures built by geographically distributed base stations. Such an infrastructure based network may not be applicable at all instant of places over the issue of the fact of unavailability (e.g., mountains) & cost.

In such cases hefty scale networks takes the benefit of P2P file sharing method, in which file sharing takes place directly instead of using a centrally federal source. Since P2P method has become a successful system it is complemented with MANET together to form a good infrastructure based network in the current and contemporary scenario. MANET is a self forming, self configuring or self healing network in contrast to a mesh network which has a centralized controller.

- Each device in MANET must forward traffic unrelated to its own use and therefore it acts as a router. Such a device must unceasingly maintain the information required to properly route traffic. By all these factors a MANET network results to be highly dynamic and autonomous topology.

Corresponding Author: K.B. Gurumoorthy, Department of Electronics and Communication Engineering,
Sri Ramakrishna Engineering College, Coimbatore, Tamilnadu, India.

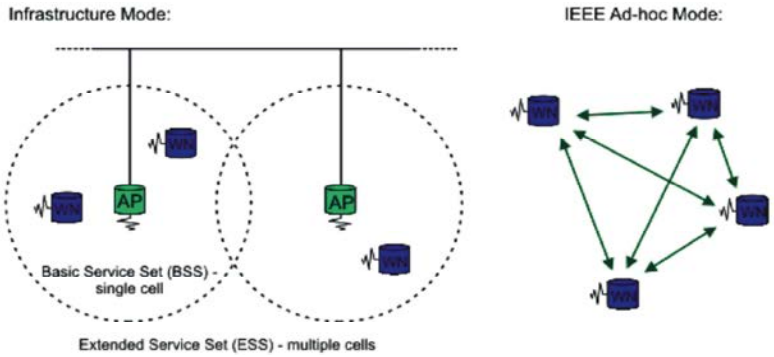
Infrastructure Mode:
IEEE Ad-hoc Mode:
WN
AP
Basic Service Set (BSS) - single cell
Extended Service Set (ESS) - multiple cells

Fig. 1: Infrastructure & Infrastructure-less wireless network

- A mobile ad-hoc network is an ad-hoc network but an ad-hoc network necessarily needs not be a MANET. MANETs communicate at radio frequency 30 Mhz – 5 GHz.
- MANETs are said to have PGP –Pretty good Privacy and trust based security. None of the protocol have made a decent tradeoff between security and performance.

Attacks in MANET- Attacks on MANETs defy the mobile infrastructure in which nodes can join and leave easily with dynamic requests without a static path of routing. The various attacks on each layer is classified as below.

- Application layer: Malicious code, Repudiation.
- Transport layer: Session hijacking, flooding.
- Network layer: Black hole, grey hole, worm hole, link spoofing, location disclosure.
- Data Link/MAC: Malicious behavior, selfish behavior.
- Physical: Interference, traffic jamming, eavesdropping.

Related Work: In former methods file sharing be contingent on numerous methods such as flooding-based, advertisement-based and social contact-based. The expanded details of the above are enlisted below:

Flooding-based: Flooding based method is the first method to docks p2p technique in mobile environment. It exploits the property of mobility in nodes and thereby it disseminates the web contents. Here the foremost important algorithm is passive distributed indexing, which is a general purpose distributed file searching system. But a dramatically high overload occurs in broadcast.

Advertisement-based: This method is used where there is a need for efficient content discovery in location-aware ad hoc networks do exists. Every file holder periodically broadcasts an advertisement message to intimate the neighbouring node regarding files. But they spawn high overheads for the advertising & cannot guarantee the success of file searching due to node mobility.

Social contact-based: The former methods have high chances of overhead and low scalability. They take the advantage of connected manets in which the end-to-end connectivity is maintained. But in this method takes the resourceful nature of detached manets. This method fails in taking up the social interest of the nodes spoon. The social interest in mobile nodes is being exploited in this method and the file sharing efficiency is being improved. Interest extraction algorithm is used to implement content based file sharing in mobile nodes.

Acknowledgement Based Peer to Peer Networks(appn) Work: In this work, an elaborate new ideology of implementing p2p file sharing in disconnected MANETs with mobile users, using anycast method have been proposed. This methodology adapts a constant anycast group and the nodes enter and exit a group in order to expand a service of sharing the data. To accomplish this, a node initially sends a request packet to the network layer and the resources will be shared to the neighboring nodes in the group. By this the information updating table and the anycast group id listing will be done successively.

Anycast Method: Anycast method is a network addressing and routing methodology. Here the datagram from a single sender are routed to the topologically adjacent node in a group of prospective receiver, though it may be sent to several nodes. In this method numerous nodes are recognized by the same destination address. Any cast addressing method is labelled as *one-to-nearest association.* Border gateway protocol is utilized to implement any cast method on internet to concurrently announce the same destination IP address range from many dissimilar places on the internet.

Regarding the developments in anycast, it is its contemplation of network and server load and guaranteeing successive packets reach same replica. The proxies proclaim common IP prefix and tunnel packets to group members. It gathers networks and server load information and determines which replicated one receives the requests; this gives the route control platforms. Anycast allows every operator whose routing information is recognized by an intermediate router to hijack any number of packets anticipated for the anycast address. This is in no different from the routing of conventional IP packets. This kind of BGP route hijacking could be prevented by

- Group of nodes that collectively announce prefix
- Formation of overlay to deliver to the destination.

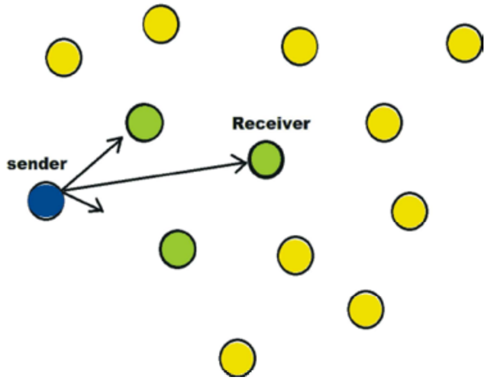

Fig. 2: Any cast technique implemented in nodes

Automatic Failover is provided in anycast and this makes anycast methodologies to be much more reliable. Major application of anycast is to externally monitor the server function and to withdraw route announcement when server fails. The most serious mode of failure in anycast method is “black hole” this is avoided by stopping the announcement.

Advantages:

- Totally translucent to clients and routers.
- Scales well for a hefty group of replicas
- Automated Efficient End-to-end paths

Disadvantages:

- Pollutes the global routing system
- Separate /24 for each replicated service
- Does not contemplate server load
- Dissimilar packets may reach as different replicas
- Slow BGP convergence after a removal

Acknowledgement Based Peer to Peer Networks (APPN): A novel intrusion detection system named Acknowledgement based Peer to Peer Networks (APPN) in which complete transmission and acknowledgement data packets should be cryptographically signed. Swarm Based Detection procedures for multiple paths establishment among source to destination and random casting is used during intrusions in MANETs. Snooping in MANET is scheduled based on the number of acknowledgements received at every occurrence in the network. The refrain of this proposed work is to provide a seamless message delivery in a MANET despite its threats using random casting and the existing mechanisms like multi-hop acknowledgement or source directed acknowledgement does not hold when a network topology changes frequently or when a node is compromised. These drawbacks are to be addressed ensuring secured connecting edges between source and destination. The source collision, exposure to vulnerability is also minimized using this mechanism.

Methodology: A new communication mechanism namely Random Cast (any cast) is used in which a sender can specify the desired level of overhearing, making a judicious balance between energy and routing performance. In addition to this it also cuts down the redundant rebroadcasts for a broadcast packet and thus, hoards more energy.

Digital signatures have always been a vital part of cryptography in the past history. Cryptography is the study of mathematical techniques allied to various aspects of information security such as confidentiality, data integrity, entity authentication and data origin authentication.

The security in MANETs is defined as a combination of processes, procedures and systems. This is mainly done to ensure confidentiality, authentication, integrity, availability and non-repudiation. Digital signature is a widely adopted approach to ensure the substantiation, integrity and non-repudiation of MANETs.

It can be generalized as a data string, which associates a message (in digital form) with some originating entity, or an electronic analog of an emblazoned signature. The disconnected MANETs are featured by sparse node density and intermittent node connection, which makes hitherto familiarized methods infeasible in such networks. Two categories of P2P file sharing methods for disconnected MANETs.

The overall system explain bi directional bandwidth acknowledgment (BSA) for intrusion detection (all transmission packet data and acknowledge should be cryptographically signed) random casting algorithm is used for multiple path selection making a prudent balance. As a bonanza it do reduces laid off rebroadcasts for a broadcast packet and thus, holds back more energy.

For multiple paths establishment among source to destination, swarm based recognition techniques are castoff to perceive malevolent nodes. Nodes with highest trust value, residual bandwidth and residual energy are designated with the aid of swarm based intelligence optimization technique. Each active node monitors its neighbor nodes and guesstimates the trust value.

In random casting, the server acquires request from the client and gives response back through the IP address. In peer to peer networks (PPN), each node eavesdrops every data transmission occurring in its locale and thus, consumes energy unnecessarily. However, some routing protocols such as Dynamic Source Routing (DSR) amasses route statistics via overhearing and they would suffer if they are used in combination with PSM. Completely barring overhearing may unsympathetically worsen the performance of the underlying routing protocol, while unrestricted overhearing may counterpoise the benefit of using PSM.

It pledges starts from source to destination then it crisscrosses for multiple path bandwidth in an intermediate node. If multipath then it calculates the bandwidth for each multiple path. If incoming bandwidth is greater than that of the sum of multiple path then it shares inward data based on frequency are else it fragments the data from the previous input. Then it patterns for the least bandwidth and assists & distributes the same amount of data through bandwidth till minimum bandwidth lasts. It do transfers at constant rate and constant delay.

Swarm Based Detection technique and Intra community File Searching for efficient node searching algorithm, the nodes with highest trust value, residual bandwidth and residual energy are selected as active nodes using swarm intelligence. Each active node monitors its neighbor nodes and estimates the delay is constant. It pledges data from intermediate node to destination and then calculate allocated bandwidth between the node to calculate delay for one packet trough bandwidth.

Calculation of Parameters: The parameters are calculated using the following steps:

Step 1: Calculate data from intermediate node to destination.

Step 2: Calculate allocated bandwidth between the node and also the delay for one packet through bandwidth.

Step 3: Repeat step 1Until all intermediate data is transferred to the destination.

Step 4: Compute entire delay for (n-1) packet if (first delay ~ (n-1) packet delay) Use the same path & split the data.

Step 5: Else reroute

Step 6: The reliability factor is introduced to prevent misbehaving nodes from modifying primary data packets. Node *p* procures a packet transmitted by *q* randomly and makes the comparison with its own data. If the source node of this packet is in the same area of node *p* and the diversity rate maintains in the interval $(-\zeta_1, \zeta_2)$, the number of accordant packets increases. Elsewise, if the source node does not belong to the area of node *p*, the reliability factor between node *p* and node *q* would not be adopted. $AP_{p,q}(\tau)$ is the number of accordant packets, $IP_{p,q}(\tau)$ is the irreconcilable one. The Reliability factor ($RF_{p,q}(\tau)$) is as follows.

$$Rf_{p,q}(\tau) = AP_{p,q}(\tau) / IP_{p,q}(\tau) + AP_{p,q}(\tau)$$

Step 7: Evaluating the recommendation is given by R_B^A which is node A’s evaluation to node B by collecting recommendations

$$R_B^A = \Sigma_{VE} \gamma V|A \rightarrow C| * V|C \rightarrow B| / V|A \rightarrow C|$$

is a group of recommenders.
$V|A \rightarrow C|$ is trust vector of node A to C.
$V|C \rightarrow B|$ is trust vector of node C to B.

Step 8: Probability that data packets received can be defined by,

$$R_B^A = (1 - p_{A,B}) * (1 - p_{B,A})$$

$p_{A,B}$ is packet loss probability from node A to node B, while, $p_{B,A}$ is packet loss probability from node B to node A.

Step 9: For a node n_k, if $Tv_k < Tv_{thr}$, where Tv_{thr} is the thrust threshold vector value, then that node is considered and marked as misbehaving node. If the source does not get the RREP packet or RERR packet for a time period of t seconds, it will be considered as a node failure or link failure. Then the route discovery course is initiated by the source again. The same procedure is repeated for the other routes R2, R3 etc and either a route without a mischievous node or with least number of misbehaving node, is selected as the reliable route.

RESULTS AND DISCUSSION

Introduction: The simulation process is carried out in NETWORK SIMULATOR (NS2) under FEDORA platform for analyzing and studying the energy consumption, network life time and data integrity problems in mobile adhoc networks. Various methods are compared to analyze the performance of the network. The table below shows the major parameters chosen for the simulation:

Table 1: Parameters implemented in NS2 modeling

S.No	Parameters	Type
1	Number of Nodes	50
2	Coverage Area	1000*1000 m sq
3	Queuing Type	Drop Tail
4	Buffer Length	50 packets
5	Antenna	Omni Directional Antenna
6	Propagation Type	Two Ray ground
7	Mobility Model	Random Way Point
8	MAC	IEEE 802.11
9	Protocol	AODV

Node Formation: The initial setting up of 50 nodes is done in an area of 1000m*1000m. The nodes are indiscriminately placed so that, they could move freely in arbitrary directions.

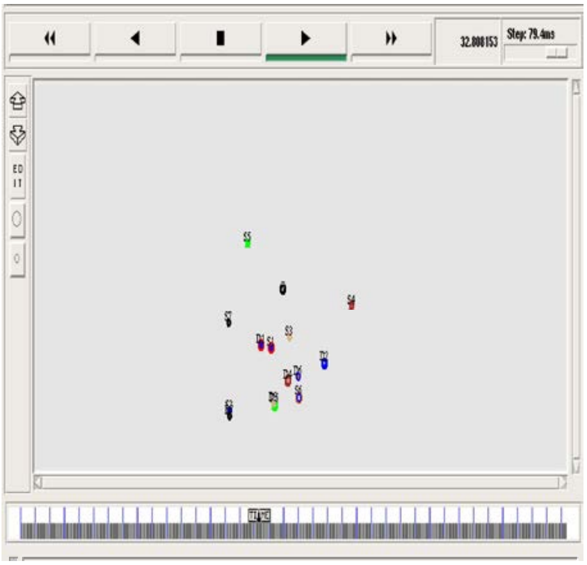

Fig. 3: Node Formation

These nodes move randomly in different directions and velocities. There is no quantified place to be given to the nodes as they are randomly placed here and there. On the dislodgment of the time the nodes starts moving and transmitting there by establishing routes between source and the destination.

Node to Node Transmission: Figure gives the transmission of packets between the nodes. Here, the transmission is from node 0 to 49 through the intermediate node is given. Circles indicate transmission range for those nodes. AODV is used as a routing protocol and the propagation model is two ray ground. On movement of nodes different multipath based on the channel are determined and the path is set to reach the destination accordingly. The path may be changing accordingly to the node movements which could be determined using frequent exchange of “hello” packets.

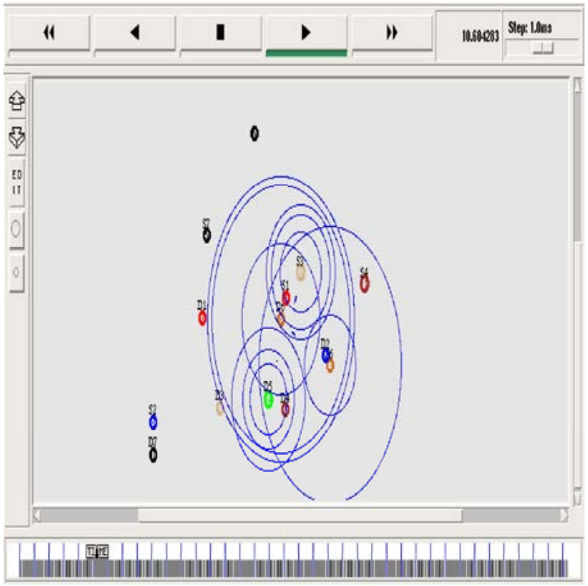

Fig. 4: Data transmission in nodes

Energy Consumption: Energy consumption is more important aspect because Ad hoc networks are composed of devices that rely on batteries. APPN protocol shows better performance in energy consumption by reducing the transmission power will directly increase the battery life of the nodes and also the network lifetime.

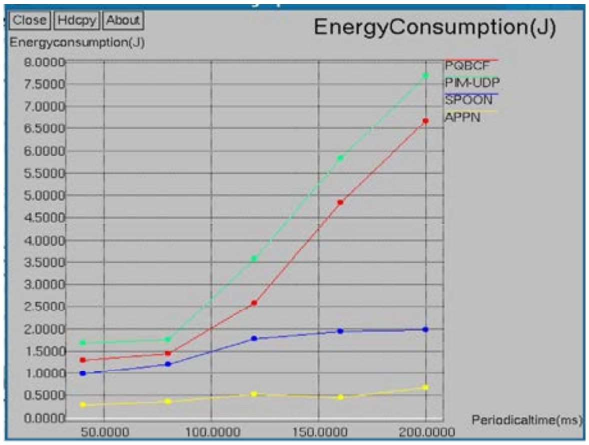

Fig. 5: Energy Consumption

The comparison of energy consumption for APPN with that of SPOON protocol is shown. It is clearly seen that the energy consumed by Acknowledgement based Peer to Peer network protocol is less compared to other protocol schemes.

Goodput: Goodput is generally described as the application level throughput i.e. the number of useful information bits delivered by the network to a certain destination per unit of time. The amount of data considered excludes protocol overhead bits as well as retransmitted data packets. This is related to the amount of time from the first bit of the frst packet sent until the last bit of the last packet is delivered.

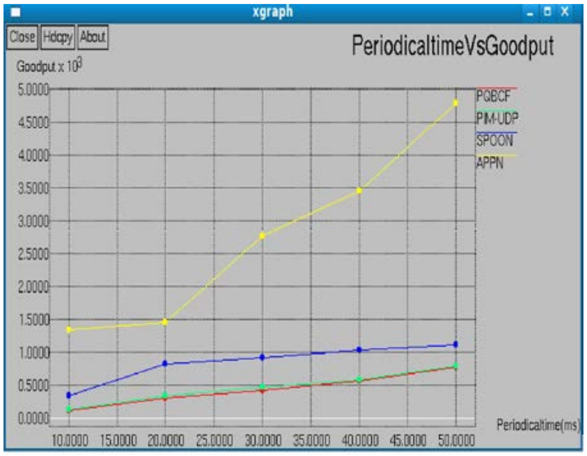

Fig. 6: Goodput

The goodput value is progressive as the periodical time of the network is being increased. Whereas the goodput change is very gradual so that the overall efficiency is slow when compared to APPN approach.

Data Integrity: Data integrity refers to maintaining and assuring the accuracy and consistency of data over its entire life cycle. This technique intent to ensure the data is recorded exactly as intended and upon later retrieval ensures the data is the same as it was when it was sent. It aims to prevent unintentional changes to information.

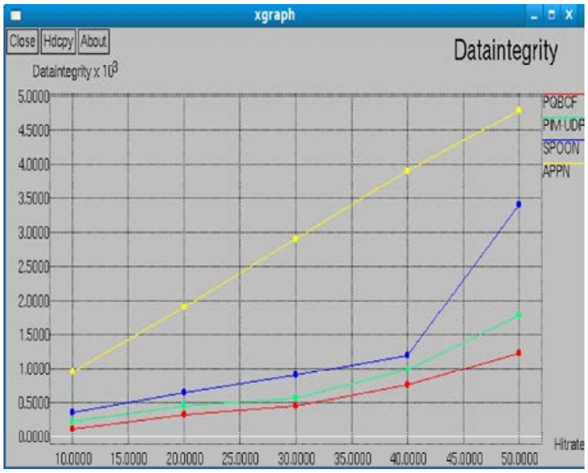

Fig. 7: Data integrity

The sharp changes in the characteristics of data integrity reduces the performance speed in SPOON, whereas the smooth change in data integrity versus hit rate graph shows the performance improvement criteria in our protocol as 1implemented in the network.

Average Delay: This factor specifies how long it takes for a bit of data to travel across the network from one node/endpoint to another. It is typically measured in multiples or fractions of seconds. Delay may differ slightly, depending on the location of the specific pair of communicating nodes.

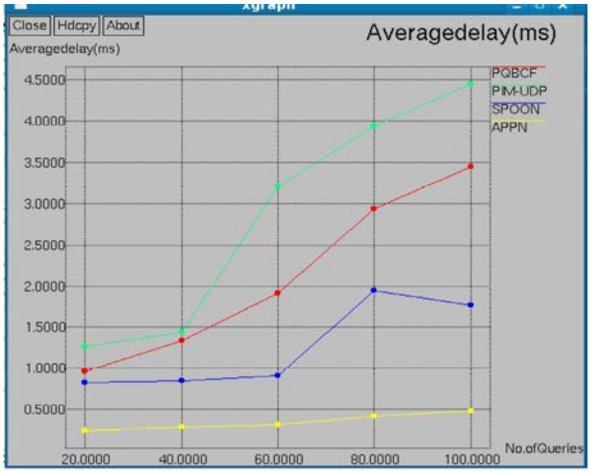

Fig. 8: Average delay

The numbers of queries represent the interactions between the sender and the receiver nodes. Its nothing but the transaction messages that take place prior in order to send a data through the network to the specified destination. Obviously the average delay increases as the number of queries is increased. But comparatively reduced in case of the other techniques.

Authenticity: Authentication is the process of actually conforming the identity received. It is the act of conforming the truth of an attribute of a single piece of data or entity. It do involves verifying and validity of at least one form of identification.

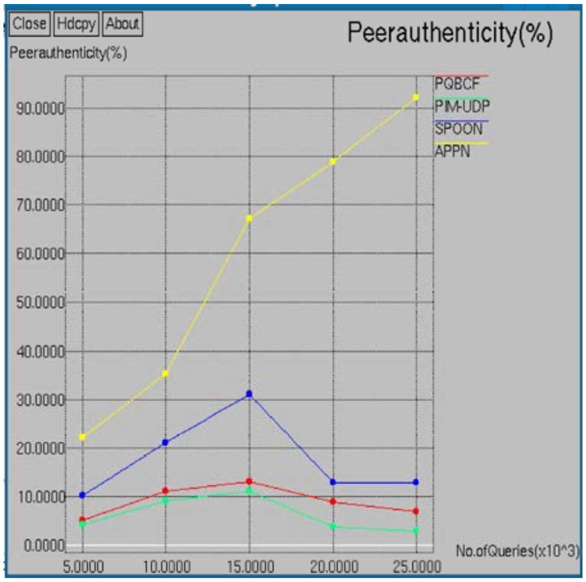

Fig. 9: Authenticity

The unwanted peaks in the characteristics of SPOON with regard to the authenticity to the number of queries are avoided in APPN approach. The number of queries and the peer authenticity is directly proportional to each other. This can be individually reduced only by reducing the number of queries which is not possible in its worst case scenario.

Network Lifetime: Its nothing but the time until the first group of nodes in the network runs out of energy to send a packet, it can also be said that in which some nodes could die or run out of battery power, whenever other network nodes could be used to capture desired information. It is the time that a network would be fully operative.

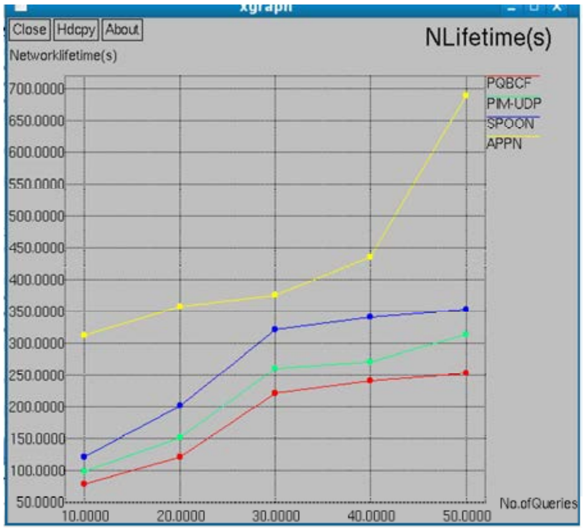

Fig. 10: Network life time

Network Life time is either specified by user, or often calculated by the network itself while the data rate, speed of sender and receiver nodes is mentioned in the transmission process. As the number of queries or transmission is increased the network life time must be held high till the last packet is being received.

CONCLUSION

Energy consumption is a significant parameter as far as battery lifetime is concerned. And also MANETS are more susceptible to attacks. The acknowledgement based p2p protocol crops enhanced results when compared to that of the existing protocols. The simulation results have indicated that the APPN protocol has better performance than that of the SPOON approach in terms of peer authenticity, network lifetime, Data Integrity and average delay. It saves power and energy in networks. In near future, a timer based byline scheme could achieve better performance in terms of the network delay, packet delivery ratio and the network cost.

REFERENCES

1. “A flooding based routing algorithm for mobile ad hoc networks, 1998. by Cokuslu, D. Bilgisayar Muhendisligi Bolumu, Izmir Yuksek Teknoloji Enstitusu, Izmir Erciyes.
2. “Construction of collaborative virtual learning communities in peer-to-peer networks, 2000. by Chun-hong Hu; Ming Zhao.

3. “Social aspects for oppurtunistic communication” (2001) by Ciobanu. R.I, Dobre. C, Cristea.V, AL-Jumeily, D.
4. “Leveraging social networks for p2p content based file sharing in disconnected manets” 2014. by Kang Chen, Student Member, IEEE, Haiying Shen, Senior Member, IEEE and Haibo Zhang.
5. “Social structure based routing of intermittently connected network using contact information, 2013. by Muyuan Wang Dept. of Comput. Sci., Univ. of Illinois at Urbana-Champaign, Urbana, IL Nahrstedt, K. (2003)
6. “Link-state advertisement based source routing protocol for manet with unidirectional links” by Yifei Wei Corresponding Author Department of Electronic Engineering.
7. “An efficient packet sensing mac protocol for wireless networks” by Muir.A and Garcia-Luna-Aceves. J., ACM J. Mobile network. Appl.
8. “A heterogenous-networ aided public-key management scheme for manets” 2006. by Tseng,Y.Min published inWiley Interscience, Int. J. Net. Mgmt., 17: 3-15.
9. “Kerboros assisted authentication in mobile adhoc networks” by Pirzada,A.,Mc Donald., C; 27th Australian Computer Science Conference (2004).
10. “The importance of being opportunistic:practical network coding for wireless environments” by S.Katti,D.Katabi,W.Hu,H.Ragul and M.Medard in Proc. Allerton (2005).
11. “A special purpose p2p file sharing system for mobile adhoc network” by A.Klemm,C.Lindemann and O.Waldoris In Proc.VTC (2003).
12. “Adhoc on-demand distance vector routing” by C.E.Perkins and E.M.Royer in Proc.IEEE WMCSA (1999).