

Improving Performance with Security Mechanism for Wireless Multi-Hop Relay Network

Ambati Raghu

Abstract— Wireless relay network consist of distribution of network topology commonly used in wireless network. Where it sender and receiver are interconnected by mean some of mobile nodes. Relay technology are used enhance packet delivery and increase performance of wireless networks such as worldwide interoperability for microwave access and LTE-A. Later developed automatic repeat request (ARQ) [11] technique that to reduced packet lose and increase latency but we recognizes potential drawbacks of automatic repeat request techniques that's are ambiguous error report, packet overhead and number of acknowledgement in case of successful received data. Authentication schema is most important factor in relay network to secure, protect from attackers because of thousands of users are communicated each other's without any identification. Authentications in relay network have been proposed public-key cryptographic algorithm developed based on Diffie-Hellman key exchange algorithm. The process of Diffie-Hellman key exchange algorithm is two users to securely exchange a keys that keys ultimately using to encrypt the message. Our research is going on reduced workload in relay network and improve performance by consider some Components that mobility factor, battery power and workload. These components Consider to establishing reliable path to reduced delay and increase data transmission speed and finally data transmission is one of major problem in wireless network then we consider hop-by-hop scheme.

Index Terms—Authentication, establish reliable path, hop-by-hop communication

I. INTRODUCTIONS

Wireless relay network (Tzu-Ming Lin, Wen-Tsuen Chen and Shiao-Li Tsao 2013) consist of distribution of network topology commonly used in wireless network. Where it sender and receiver are interconnected by mean of some relay nodes. In such network the sender and receiver cannot communicate to each other directly because the distance between sender and receiver is greater than the transmission range therefore we need intermediate relay nodes. The development of these relay efficient way to communicated and secure to connecting millions of our customers at mobile stations as well as enhance packet delivery and efficient acknowledgement. Relay nodes with buffering Functions and packet decoding can improve efficient acknowledgement, throughput and capacity of relay node. Today such networks are Used in many companies to communicate customers that network are enhancing Packet delivery, efficient acknowledgement and improve throughput [11]. Earlier frame relay uses for faster growing wide area technology uses in large corporation, government and small business application and so on.

Manuscript published on 30 June 2014.

* Correspondence Author (s)

Ambati Raghu, Garudubhadra (Post), Vajrapukotturu, Srikakulam, Andrapradesh, India.

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an open access article under the CC-BY-NC-ND license <http://creativecommons.org/licenses/by-nc-nd/4.0/>

1) Mobile ad hoc network[13]: mobile ad hoc consist of a self-configuring infrastructure less network that group of mobile nodes connected wireless and it does not relay on prefixing infrastructure however each node participate in routing to forward data for other nodes instead it is decentralized type of wireless network. Mobile ad hoc can be used in variety of application such as air pollution it can facilitating collection of sensor data for data mining and mobile ad hoc including several application such as battlefield communication, emergency fire response. 2) Frame relay network: relay network is standard wide area network technology that described layered architecture of digital telecommunication channel using packet switching technology. Network providers developed frame wireless network for voice and data encrypted methodology used in local area network and wide area network. Frame relay network organized the transmission over different band with transparent to all end user using WAN protocol .Multi-hop. 3) Cellular network: This is wireless network distributed wide range area calls cells. In this wireless network each cell uses different frequencies from neighboring Cells to provide constant band with each cell and minimized interference. Multi-hop cellular architecture contain multiple hops for increasing throughput in this combined advantages of fixed infrastructure of base station and without infrastructure of ad hoc network **Relay client authentication type**[10] Relay network consist of each new user has unique private key to communicate with authentic manner in this network base station provide certificate signature (unique private key) and each user have public key certificate. These two public and private keys are using to communicate each other .Authentication is one of most important factor in relay network to secure, protect from attackers Because of thousands of users are communicated each other's without any identification.

Authentication Authentication schema is most important factor in relay network to secure, protect from attackers because of thousands of users are communicated each other's without any identification. Authentications in relay network have been proposed public-key cryptographic algorithm developed based on Diffie-Hellman key exchange algorithm. The process of Diffie-Hellman key exchange algorithm is two users to securely exchanges a keys that keys ultimately using to encrypt the message .it is implemented based on number theory to using prime number concept that each user has two key private and public these keys are act as primitive root conditions .the security of attackers very difficult to break the keys because in Diffie-Hellman using modular functions but brute-force attack and man-in-middle Attack are possibility to break the codes. In Diffie-Hellman algorithm using has functions to avoid the attacks.

Hop-by-Hop Relay Repeat Request Scheme

Hop-by-hop relay [9][11] repeat request schema are using to implement the relay network in this scheme packets are transmitting hop-by-hop from source to destination via using intermediate nodes. See below figure

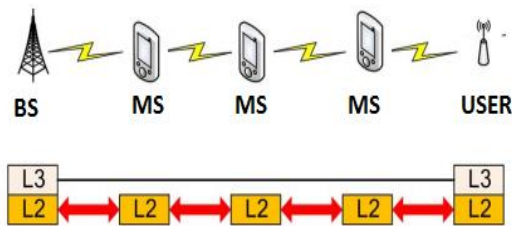


Fig (1) Hop-By-Hop Relay Repeat Scheme.

In this scheme every MS involved error control, response for detecting errors, acknowledgement and retransmission see above figure like as. When neighbor node received packets successfully then send Acknowledgement or loss packets then send negative acknowledgement these two operations are most important in relay network. In case loss packets then send retransmitted a data by using buffer storage management.

Establish Reliable path

In this section we consider reliable path by using components that are battery power, mobility factor and workload these components consider to select best nodes.

II. PRESENT WORK

Problem formulation: Relay network is one of major field in wireless network and better ways to enhance packet delivery in wiled area network. One of major problem in relay network to increase workload in case of data transmission and authentication problem .Our research is going on reduced workload in relay network and improve performance by consider some components that mobility factor ,battery power and workload. These components consider to establishing reliable path to reduced delay and increase data transmission speed and finally data transmission is one of major problem in wireless network then we consider hop-by-hop scheme. Authentication is second problem in relay network then we present proposed public-key cryptographic algorithm. This algorithm implemented based on Diffie-Hellman key exchange algorithm.

2.1 Proposed authentication algorithm.

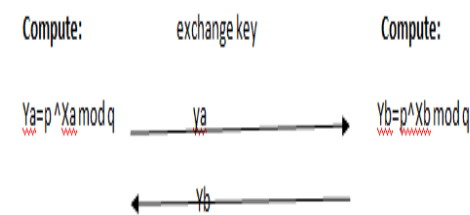
Let consider following steps for algorithm.

- Step 1) Select public-key (P, Q) Q->prime number and P-> primitive root of Q with condition (P < Q)
- Step 2) User A and User B know public values
- Step 3) User A select private number Xa, and compute Ya
Let consider $Y_a = P^{X_a} \text{ mod } Q$
Users A send Ya to User B
- Step 4) User B select private number xb and compute yb
Let $y_b = p^{x_b} \text{ mod } q$
User B send Yb to User A
- Step 5) Let consider ID, H values these values are ID, H>q
Let consider condition to Compute ID, H values and ID, H are relative prime of Q
That's $y_a * H \equiv 1 \text{ mod } q$

- $y_b * ID \equiv 1 \text{ mod } q$
- Step 6) Compute $Y_a' = P^{(X_a + ID + H)} \text{ mod } Q$
User A send ya' to User B
- Step 7) User B compute Ya' value by using Ya, ID, H values.
Expand equation like
 $(P^{Y_a} \text{ mod } Q) * (P^{ID} \text{ mod } Q) * (P^H \text{ mod } Q)$
If both values are equal user A is authorized otherwise reject

See below method exchanging keys:

USER A	USER B
Public(P, Q)	Public(P, Q)
Q->prime number	Q->prime number
P->primitive root of q	P->primitive root of Q
(P < Q)	
X_a ->private number of user A	X_b ->private number of user B



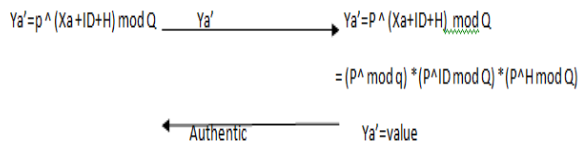
Let consider ID, H value

These are Id, H < Q

$Y_a * H \equiv 1 \text{ mod } Q$

$Y_b * ID \equiv 1 \text{ mod } Q$

Compute:



Let Consider Example of Key Exchange Algorithm:



USER A	USER B
Public(P, Q)	Public(P, Q)
Q->prime number=11	Q->prime number=11
P->primitive root of q =3	P->primitive root of Q=3
(P < Q)	
Xa->private number of user A	Xb->private number of user B
Xa=4	Xb=7

Compute: exchange key Compute:

$$Y_a = p^{X_a} \text{ mod } Q = 3^4 \text{ mod } 11 = 4$$

$$Y_b = p^{X_b} \text{ mod } Q = 3^7 \text{ mod } 11 = 9$$

Y_a → Y_b

These are Id, H < Q and primitive roots of Q

$$Y_a * H \equiv 1 \text{ mod } Q$$

$$4 * 3 \equiv 1 \text{ mod } 11$$

$$Y_b * ID \equiv 1 \text{ mod } Q$$

$$9 * 5 \equiv 1 \text{ mod } 11$$

Compute:

$$Y_a' = p^{(X_a + ID + H)} \text{ mod } Q$$

$$= 3^{(4 + 3 + 5)} \text{ mod } 11$$

$$= 9$$

Y_a' →

$$Y_a' = p^{(X_a + ID + H)} \text{ mod } Q$$

$$= (P^A \text{ mod } q) * (P^{ID} \text{ mod } Q) * (P^H \text{ mod } Q)$$

$$= 4 * 1 * 5$$

$$= 4 * 1 * 5$$

$$= 9$$

← Authentic Y_a'=value (show that both values equal)

2.2 Reliable path established using node selection method

In this section we consider reliable path by using components that are battery power, mobility factor and workload these components consider to select best nodes. See below flow chart to select nodes. We consider threshold values for each component these threshold values based to select a node. See below Figure reliable path established flow chart.

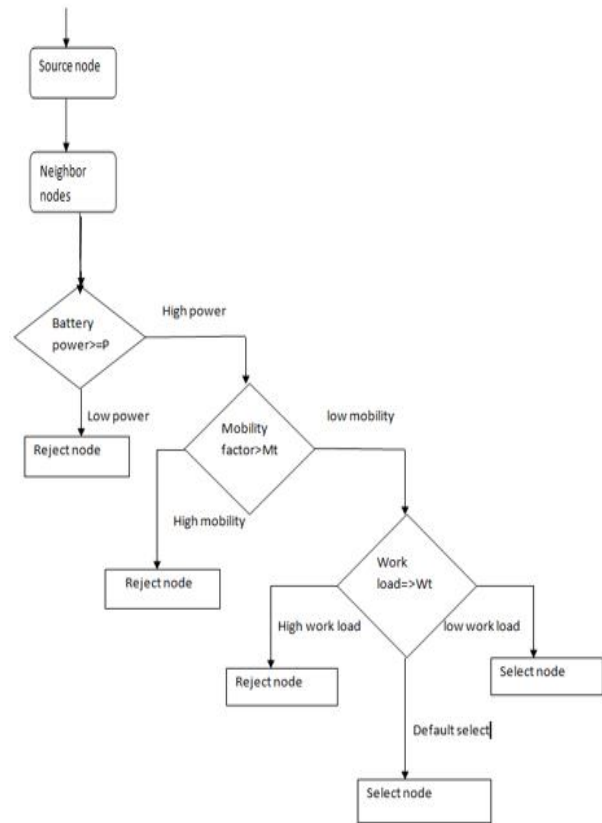


Fig (2) Reliable Path Established Flow Chart.

2.3 Problem objectives

Our research consider three objectives 1) first phase is establish reliable path in relay network to consider some components like mobility factor ,battery power and workload ,we will not consider shortest path 2) Second phase improve security using proposed authentication algorithm and 3) Third phase efficient way to data transmission by using hop by hop method. See below diagram for. Objective phases.

Our research following steps:

1. Randomly placing number of mobile nodes in network
2. All mobile node have mobility factor, battery power and workload except source node and base station
3. Proposed authentication algorithm using to exchange keys for authentic purpose.
4. Node selection method using to select a node
5. sending data using hop-by-hop communication

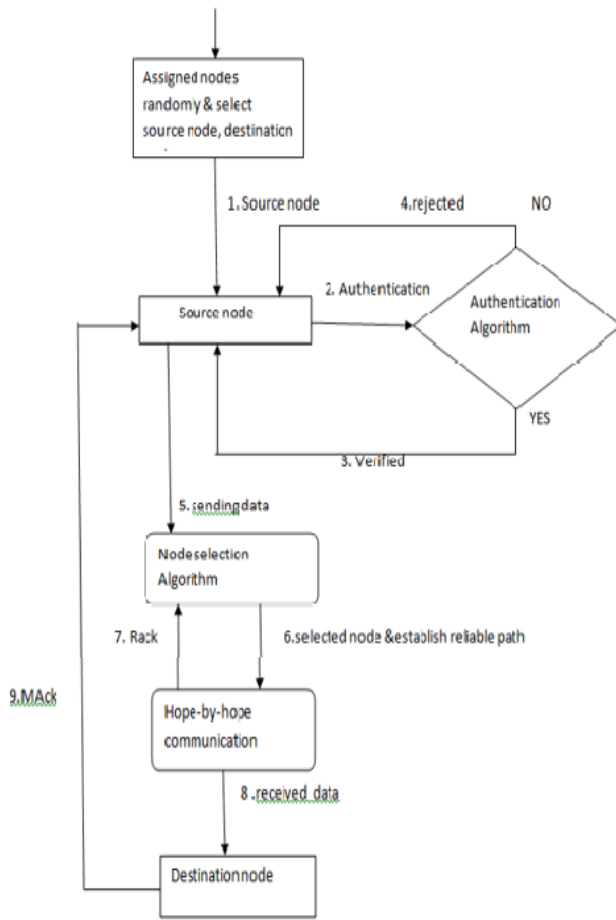


Fig (3) Problem Objective Phases.

2.4 Methodology

In this section we are explained proposed technology to achieve our objectives. First of all gathering information from various optimized techniques and results is done to decide which technique should be used in this work .present proposed algorithm is best optimized solution. Let consider methodology **Let consider example table 3.3 to establish reliable path by using node selection method** Minimum battery power=5V, minimum node speed=10 m/s, minimum work load=75% with transmission range of each node At T1 time

STEP 1) Create Relay Network: There are number of relay nodes are assigned randomly in network and each node consider mobility factor, Battery power and workload (change position after t time)except source node and base station see below diagram fig(4) to randomly assigned mobile nodes

node	Inside(range) boundary	Outside(range) boundary	Battery power	mobility	workload
M	A,B,D,C	F,E,H,G	4v	10m/s	65%
A	B,F,D	C,G,H,E,I,J	6v	5m/s	44%
B	F,D,G,H,E	I,J	6v	7m/s	32%
C	C,D	G,H,F,E,I,J	7v	8m/s	45%
D	G,H,F	E,I,I	6v	5m/s	65%
E	E,H	IJ	6v	4m/s	45%
F	E,H	LJ	7v	0m/s	66%
G	H,J	I	8v	4m/s	34%
H	I,J		11v	7m/s	22%
I	S		10v	15m/s	66%
J	S		12v	10m/s	23%
S					

Table 3.3 sample example to consider node properties

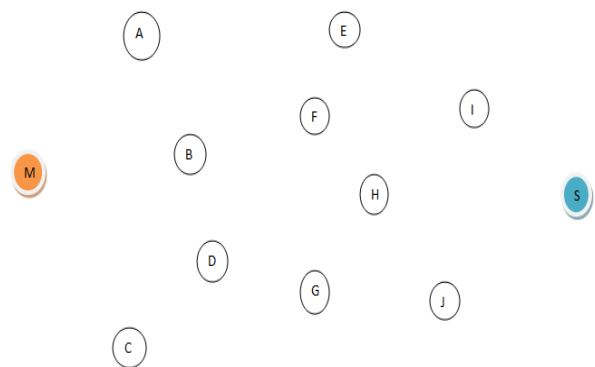


Fig (4) Assigned Random Nodes

STEP 2) Authentication: Second step is authentication to exchange the keys in which randomly selected paths there is no conditions as show below diagram.

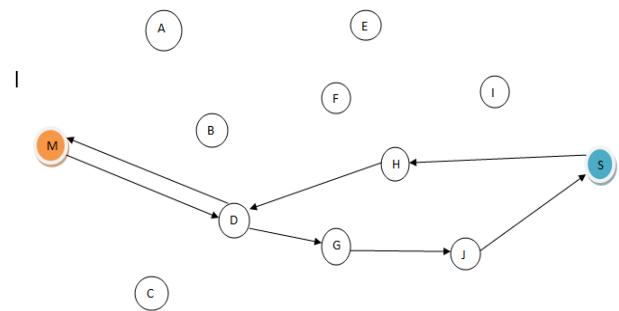


Fig (5) Authentication between Source and Destination

STEP 3) Select the Nodes and Send Data: Select the nodes by using node selection method and send data source to destination by using hop-by-hop communication as show below diagram. in this step node C,J are rejected nodes because didn't satisfied condition see above table .Acknowledgement when neighbor node received data successfully then replay acknowledgement or in case failure data then send negative acknowledgement again retransmit the data.

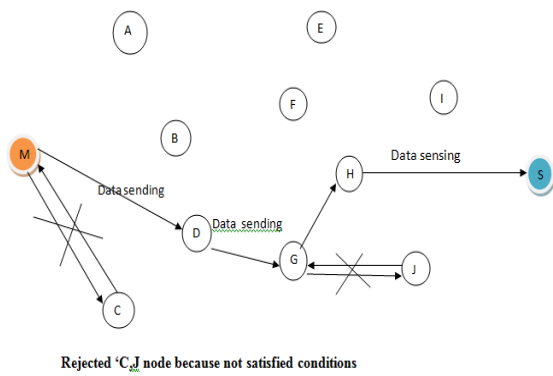


Fig (6) Select Nodes in Relay Network.

STEP 4) acknowledgement path: When base station received data successful then send mobile acknowledgement see below diagram like as.

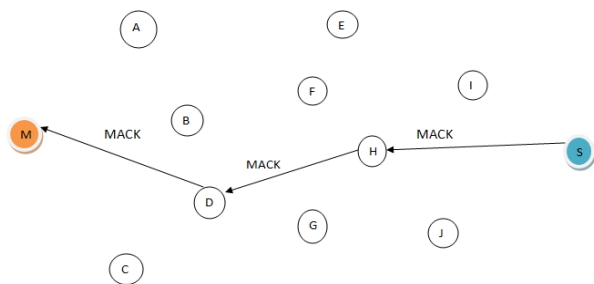


Fig (7) Acknowledgement Path

STEP 5) data sending hop-by-hop repeat request schema: Hop-by-hop relay repeat request schema are used to implement the relay network. In this scheme packets are transmitted hop-by-hop from source to destination via using intermediate nodes. In this scheme every MS involved error control, response for detecting errors, acknowledgement and retransmission see above figure like as. When neighbor node received packets successfully then send Acknowledgement or loss packets then send negative acknowledgement these two operations are most important in relay network. In case Loss packets then send retransmitted a data by using buffer storage management.

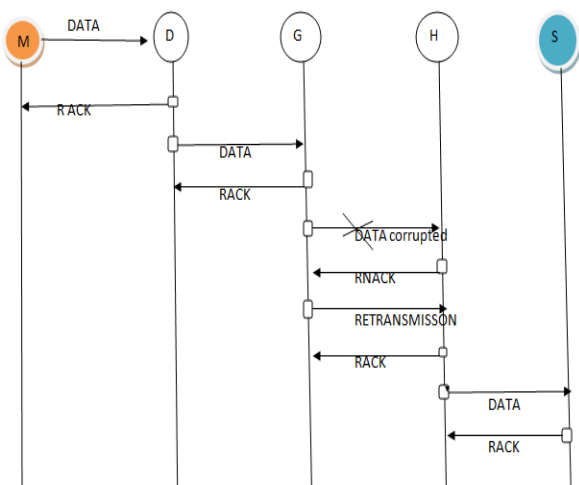


Fig (8) Sending Data Hop-By-Hop Scheme

Network performance for proposed methodology.

Throughput the graph showed throughput of proposed methodology. Network throughput is the average rate of successful packet delivery over a communication channel

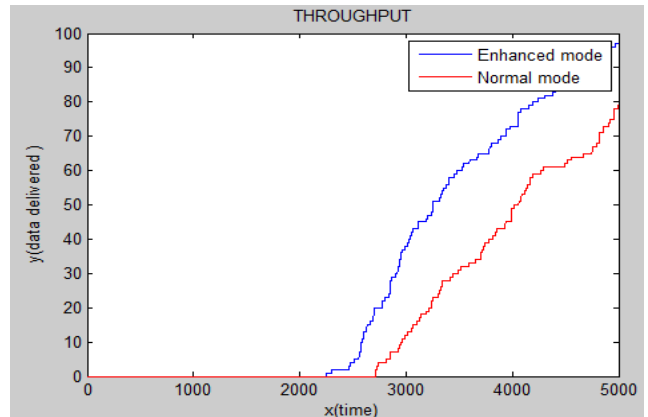


Fig (9) Throughput.

Energy consumption mobile nodes consider battery power, workload and mobility factor these components based on established reliable path and these factors based on calculating energy consumption of successful packet delivery over a communication channel.

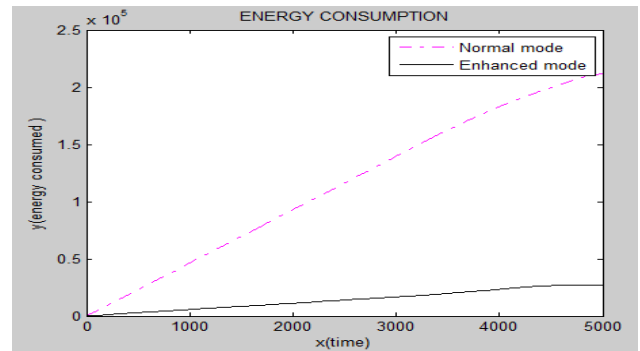


Fig (10) Energy Consumption.

Packet delivery ration the graph showed packet delivery ratio of proposed methodology. In data are sending hop-by-hop method. The graph shows average rate of successful packet delivery over a communication channel.

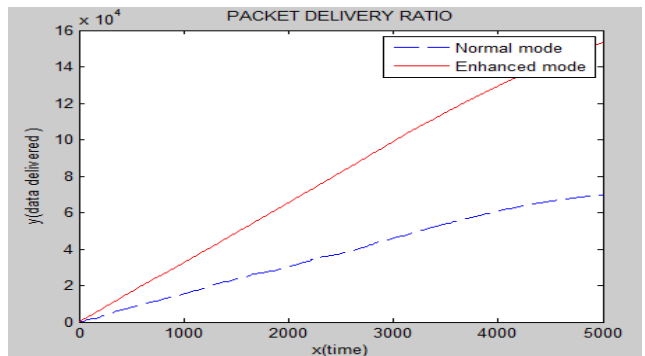


Fig (11) Packet Delivery Ration.

2.5 Result and Discussion

Change battery power Each Mobile node consider battery power consumption depending on transmission range, received data packets, processing and mobility factor. Let see below graph change battery power. See figure 11

Change workload each mobile node consist of cpu usage is mainly due to each process execution time, retransmission data in case loss packets and mobility factor. See below figure 12 how to change cpu utilization.

III. CONCLUSION AND FUTURE

In our research is going on reduced workload in relay network and improve performance by consider some components that mobility factor, battery power and workload. These components consider to establishing reliable path to reduced delay and increase data

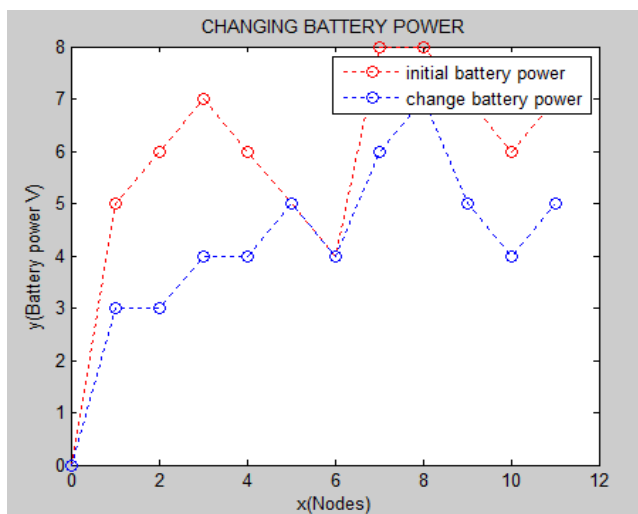


Fig (11) Changing Battery Power.

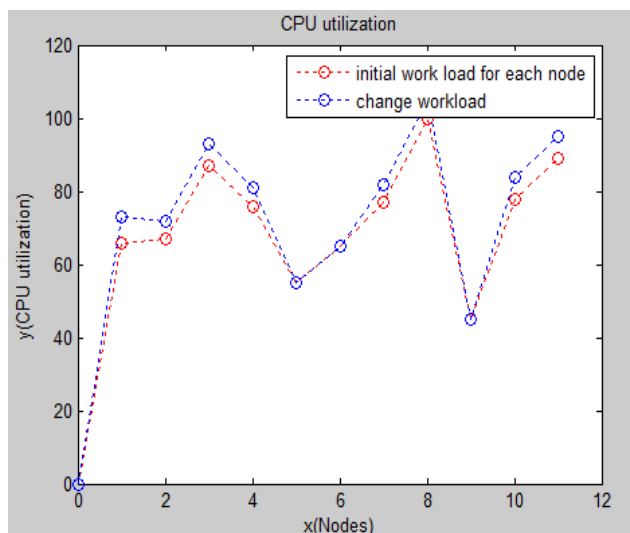


Fig (12) Change Workload.

Transmission speed and finally data transmission is one of major problem in wireless network then we consider hop-by-hop scheme. Authentication is second problem in relay network this algorithm working on key exchanging between source and destination. Finally our proposed result is optimized solution compare to previous techniques and

proposed analysis work is fine. In our project minor packet loss, error control but it does not affected over services.

Future scope

Authentication and performance are important in Relay network .Further performance can improve by keeping the computation overheads simple.

- 1) Further security can be improved by using has functions or any other public key cryptographic algorithms
- 2) There are many other components like bandwidth, co-coordinators etc. consider to improved performance in relay network.

REFERENCES

- [1] A. B. Saleh, O. Bulakci, and J. Hamalainen(2012), "Analysis Of the impact of site planning on the Performance of relay Deployments," *IEEE Trans. Veh. Technol.*, vol. 61, no. 7, pp. 3139–3150
- [2] A. Sunny, J. Kuri, and S. Aggarwal (2011) "Delay modeling for a Single-hop wireless mesh network under light aggregate traffic," *Proc. IEEE ICCSP, Kerala, India*, pp. 271–275
- [3] Chu Y H, Rao S G, Seshan S, Zhang H (2000). "A Case for end System multicast." *Proceedings of the ACM SIGMETRICS*. Santa Clara, USA, 2000.
- [4] D. Soldani and S.Dixit (2008) "Wireless relays for Broadband Access [radioCommunications series]", *IEEE Commun. Mag* vol.46 no. 3, pp. 58– 66.
- [5] F. Ono, K. Sakaguchi(2009) "STBC MIMO Network Coding for Bi-Directional Multi-Hop Relay Networks," *IEICE Trans. Commun. Vol. E92-B*, no. 12, pp. 3676–3682.
- [6] I. F. Akyildiz, T. Melodia, and K. R. Chowdhury (2007) "A survey On wireless Multimedia sensor networks," *Computer Networks* vol. 51, no. 4, pp. 921–960.
- [7] H. Wiemann, M. Meyer, R. Ludwig, and O. Chang Pae(2005) "A Novel multi-hop ARQ concept," *Proc. IEEE 61st VTC, Stockholm, Sweden*, pp. 3097–3101.
- [8] K. Mizutani, K. Sakaguchi, K. Araki (2009) "MIMO-OFDM two-Way multihop network and Network synchronization scheme," *IEICE Tech. Report on Software Radio*, vol. 109, no. 61SR2009-7, pp. 43-49, May.
- [9] Li Bo, Yin Hao(2007) "The peer-to-peer live video Streaming in The Internet: Issues, existing Approaches and challenges". *IEEE Communications Magazine*, 45(6): 94-99.
- [10] LIU Xuening , YIN Hao , LIN Chuang , DU Changlai(2009) "Efficient User Authentication and Key Management for Peer-to Peer Live Streaming Systems" *ISSN 1007-0214 13/18 Volume 14, Number 2*, pp234-241
- [11] R. Vaze(2011) "Throughput-delay-reliability tradeoff with ARQ In wireless ad hoc networks," *IEEE Trans. Wireless Commun.* vol. 10, no. 7, pp. 2142– 2149
- [12] S. Misra, M. Reisslein, and X. Guoliang(2008) "A survey of Multimedia streaming in wireless sensor networks," *IEEE Commun. Surveys & Tutorials*, vol. 10, pp. 18–39.
- [13] Shivashankar, Suresh H.N, Varaprasad Golla, Jayanthi G (2013) "Designing Energy Routing Protocol with Power Consumption Optimization in MANET" *IEEE Transactions on Emerging Topics in Computing*,
- [14] T. Issariyakul, E. Hossain, and A. S. Alfa (2006) "End-to-end Batch transmission in a multihop and multirate wireless network Latency, reliability, and throughput analysis," *IEEE Trans. Mobile Comput*, vol. 5, no. 9, pp. 1143–1155.