DESIGN AND DEVELOP EEMASP PROTOCOL AND EMMASP ALGORITHM TO PREVENT NETWORK DEGRADATION PROBLEMS IN WIRELESS SENSOR NETWORKS

[1]D.J Samatha Naidu, [2]Ande prasad
1 Research Scholar , Vikrama Simhapuri university Nellore.
2 Department of Computer Science,Vikrama Simhapuri university Nellore,

Abstract : Most of the research work focuses on path constrain issues, a mobile sink has limited communication time to collect data from the sensor nodes deployed randomly. These posses significant challenges in jointly improving the amount of data collected, reducing the energy consumption and to prevent security attacks need improved key management schemes while packet transmits over the network(s). **In Proposed Work**, To address this issues, designed and develop a new adversary model called **Source level Analysis to Manage and Reconfigure Adjusting cluster head Model** (SAMRAM Model) a novel data collection algorithms called Enhanced Min-Max shortest path(EMMASP) algorithms used to increases network throughput and , to provide multiple path discovery which computes primary path and alternate path. Energy efficient multi adjust scheduling path (EEMASP) protocol conserves energy by optimizing the assignment of sensor nodes in the network implementation. To design routing protocol for Wireless sensor networks to provide reliable data transmission with high packet delivery ratio and reducing delay. EEMASP implemented as a two phase locking communication protocol based on same cluster zone partition. The re-routing process costs in bandwidth and node energy consumption and the extra routing latency may affect QoS for network applications, degrading the network performance. It is also concretes on DoS attacks, jamming attacks and related security issues. Clustering is the art of homogeneous datasets in database. To provide high speed and high quality wireless services with secure way in wireless sensor networks. It focuses on, Sensor node Compromise, eaves dropping and modifying packets leads security problems and the allocation of traffic in multiple routing paths leads security vulnerabilities

IndexTerms: SAMRAM Adversary model, EEMASP protocol, EMMASP algorithm

I. INTRODUCTION

Wireless sensor networks is an integral part of our lives . However, these sensor networks needs to convince the constraints such as throughput fault tolerance , scalability , cost hardware, topology change, environment and power consumption. The constraints are highly stringent and specific for sensor networks, new wireless sensor routing has attracted lot of attention in an interesting issues for routing protocols is the consideration of node mobility. By applying the proposed algorithm Energy efficient multi scheduling shortest path(EEMASP) routing protocol and SAMRAM Enhanced Min-Max shortest path algorithm (for heterogeneous networks and homogeneous networks EMMASP, EEMASP protocol are used. It is possible to the solve above addressed issues.

II. RELATED WORK

The Research mainly focus on the design of an adversary model which k-means cluster used for data gathering from homogeneous and heterogeneous WSNs [15][14]. In such networks, The base stations are maintains a notion of packets discrete data gathering loops, during which all the nodes send the data to the respective Base Station (BS). The periodic measurements are used to draw conclusions about the distinguish activity in the selected region. The main motive of the clustered scheme is to send the measured data to the BS through elected Cluster Head (CH). This is because in most applications, there is likely to be some correlation between the measurements of adjacent nodes [13][12]. On one hand, it is possible to save node energy by using data fusion or aggregation, and reducing the amount of data which is sent to the BS. CH nodes could either be chosen from among the wireless sensor networks nodes (homogeneous networks), otherwise the nodes that are deployed for selected CH nodes (heterogeneous networks). Elected CH nodes could either use single hop or multi-hop communication approach to transmit their aggregated data to the BS [11][10]. The purpose of this work is to present new routing protocols for energy-efficient clustering and data aggregation within a cluster and reducing the load of aggregation at CH to provide energy efficiency for maximizing the network lifetime, stability and throughput [9]. In WSN communications, an adversary can gain access to private information by monitoring transmissions between nodes [8][7]. Encrypting sensor node communications partly solves eaves dropping problems but requires a robust key exchange and distribution scheme [6][7]. The large number of communicating nodes yields to provide end-to-end encryption mechnaisms. In case of adversary control over a communication node eliminates encryption’s effectiveness for any communications directed through the compromised node [5]. This situation could be worsen if an adversary manipulates the routing infrastructure to send many communications through a malicious node [3][4]. imperative routing protocols are one solution to this problem. Another solution is multi-path routing, which routes parts of a message over multiple disjoint paths and re-assembles them at the destination [2]. Efficient discovery of the best disjoint paths to use for such an operation is another research challenge [1].

III. PROPOSED FRAME WORK

(i) Architecture frame work of SAMRAM Adversary Model

In figure 1 the proposed methodology concentrate on prevention of different security attacks and how to reduce the network degradation problems in homogeneous and heterogeneous networks through SAMRAM adversary model through EMMASP protocol and APMRC algorithm with DRSODA key management scheme.

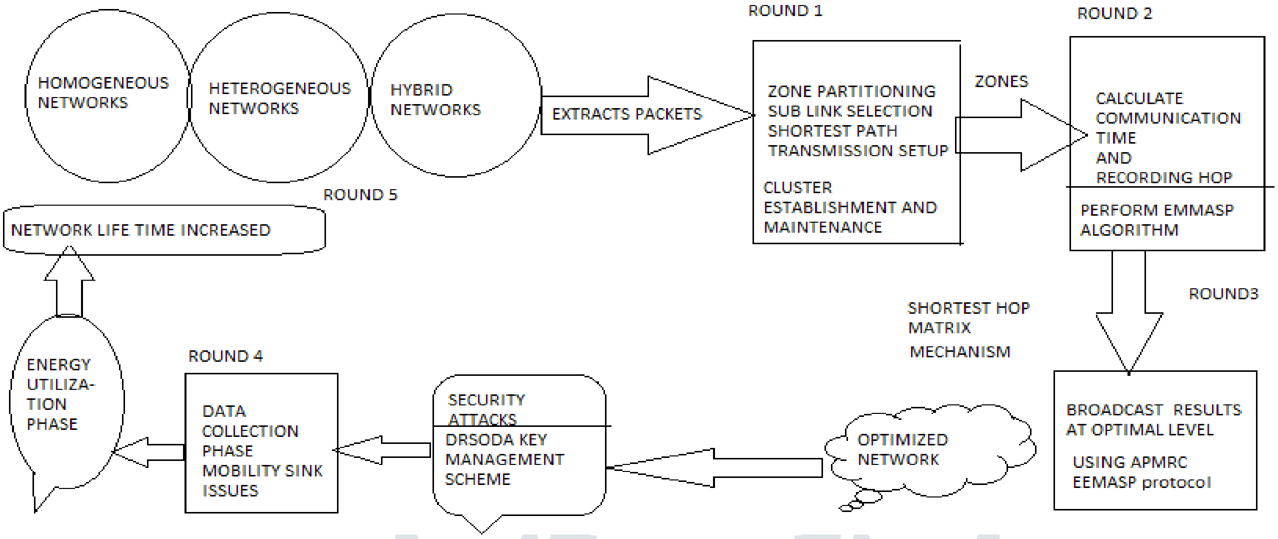

ROUND 1
ROUND 2
HOMOGENEOUS NETWORKS
HETEROGENEOUS NETWORKS
HYBRID NETWORKS
EXTRACTS PACKETS
ZONE PARTITIONING
SUB LINK SELECTION
SHORTEST PATH
TRANSMISSION SETUP
CLUSTER ESTABLISHMENT AND MAINTENANCE
ZONES
CALCULATE COMMUNICATION TIME AND RECORDING HOP
PERFORM EMMASP ALGORITHM
ROUND 5
NETWORK LIFE TIME INCREASED
ROUND3
SHORTEST HOP MATRIX MECHANISM
ENERGY UTILIZA-TION PHASE
ROUND 4
DATA COLLECTION PHASE MOBILITY SINK ISSUES
SECURITY ATTACKS
DRSODA KEY MANAGEMENT SCHEME
OPTIMIZED NETWORK
BROADCAST RESULTS AT OPTIMAL LEVEL
USING APMRC EEMASP protocol

Figure 1 Architecture frame work of SAMRAM Adversary Model

(ii)SAMRAM EEMASP protocol and EMMASP algorithm

Source level analysis to manage and reconfigure adjusting cluster head model (SAMRAM Model) and Energy efficient multi scheduling shortest path(EEMASP) routing protocol and SAMRAM Enhanced Min-Max shortest path algorithm (for heterogeneous networks and homogeneous networks) that increases network throughput as well as conserves energy by optimizing the assignment of sensor nodes in the network is implemented. SAMRAM adversary model is implemented as a multi-tier locking communication protocol based on same cluster zone partition. The re-routing process costs in bandwidth and node energy consumption and the extra routing latency may affect QoS for network applications, degrading the network performance.

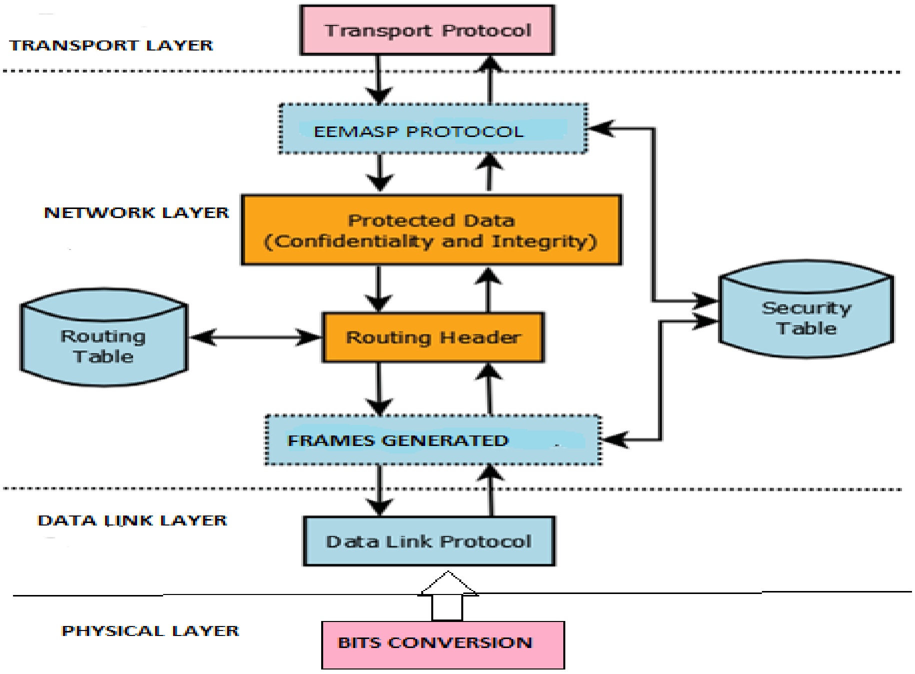


Figure 2 EEMASP protocol provides data confidentiality, data integrity and data authentication services for data packets

In Figure this proposed EEMASP protocol multi-tier architecture helps to provide data confidentiality, data integrity and data authentication services for data packets .

EMMASP algorithm

Definition 1: (Enhanced Min-Max shortest path):

Input Instance: MS_{ink}, a list of m nodes (M$s1$,...,Msm) in the network;

O, a list of n locations ($o1$,...,on) where oi is the initial position of node si for $1 \leq i \leq$ m;

M$Ssources$, a subset of MS representing the source nodes; r, a node in MS, representing the single sink;

$Msources$ = {Vi|si∈$Ssource$()_}, a set of data chunk sizes for all sources in $Ssources$;

We define Vi, which we compute later, to be the weight of node si which is equal to the total number of bits to be transmitted by node si.

We define a configuration <E,U> as a pair of two sets: E, a set of directed arcs (Msi,Msj) that represent the directed tree in which all sources are leaves and the sink is the root and U, a list of locations ($u1$,...,un) where ui is the transmission position for node si for $1 \leq i \leq n$. The cost of a configuration <E,U> is given by:

$$<E,U> = \sum (si,sj) \in Eami$$

$$<E,U> = (b\|ui - uj\|2mi + k\|oi) - ui\|$$

Output: <E,>, an enhances min max shortest path configuration that minimizes the cost c(<E,U>).

// Sub algorithm module

Definition 2: join network proxy location algorithm for EMMASP

Input : A WSN network topology with node set V;

The total number of nodes n;

Output: a set of join proxies cluster heads CP;

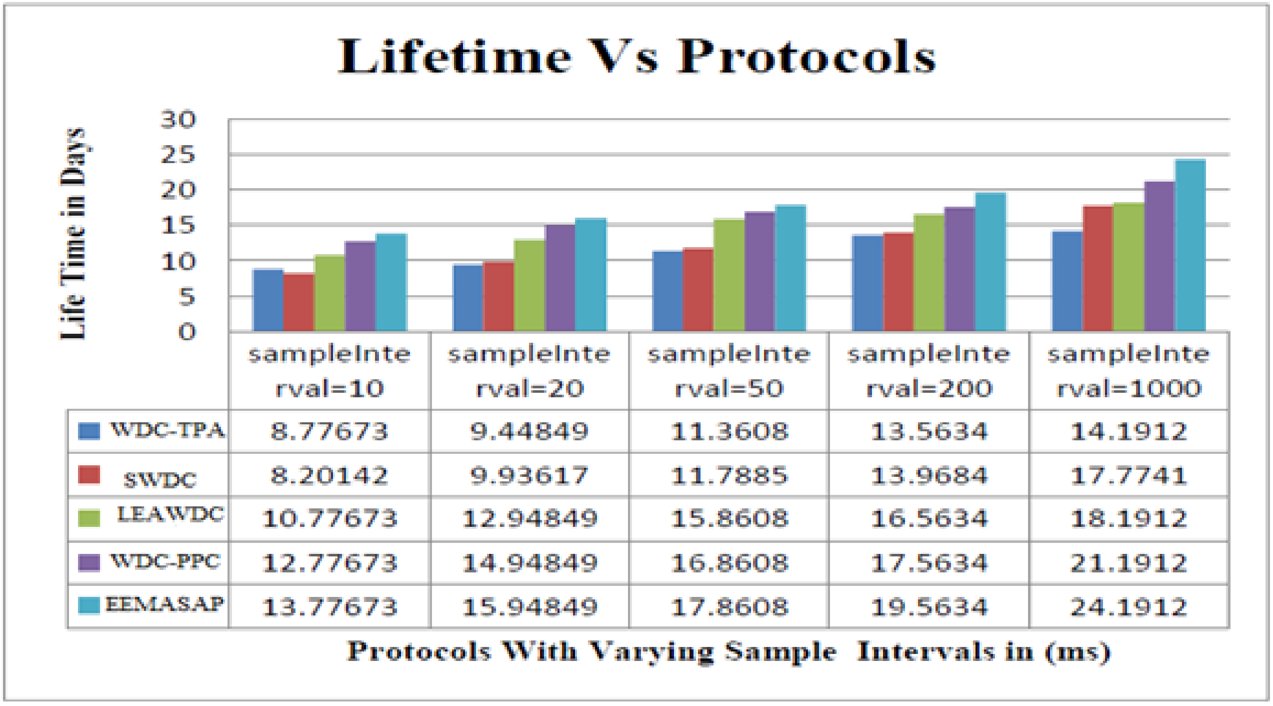
Procedure:

```
CP ←ϴ;{cost (ϴ)=∞}
For k←1 to n-1 do
Location(k);{update CP`}
If cost(CP`)<cost(CP) then
CP←CP`
end if
end for
return CP;
location(k)
CP`[0] ←BS;
for i←1 to k do
CP`[i] ←I;{initialize CP`[0]…….CP`[k]}
end for
for(i=CP`; j<CP`and I,j<V;i++)do
CP``←CP`-i+j;{swap I and j}
If cost(CP``)<cost(CP`) then
CP`←CP``;
End if
End for;
Note: loops ends after we try all the combinations of i and j
```

IV. COMPARATIVE ANALYSIS AND SIMULATION RESULTS

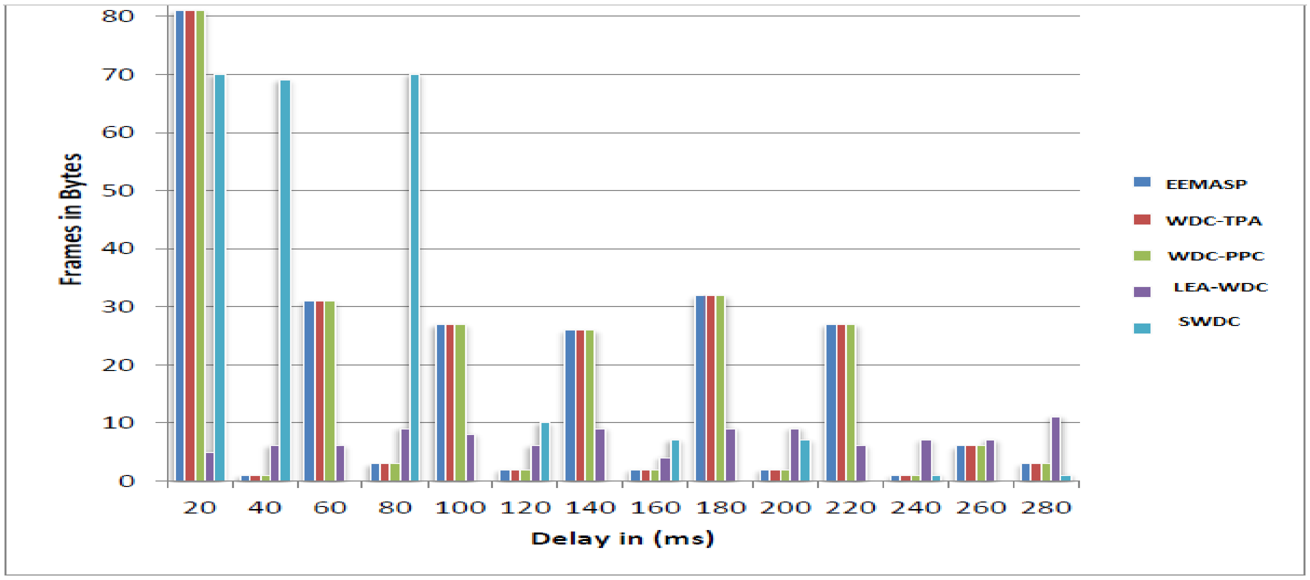
(i) Performance Metrics

Performance metrics like Packet deliver ratio and End-to-End delay etc. are also considered for comparative analysis among these protocols used SAMRAM EEMASP protocol introduced to increased network life time. Below we have compared with few existing protocols. Performance results of proposed model is compared with the existing sequential probability ratio test, by producing the 35 to 45% better reliability, 10 to 15% lesser energy utilization, 20 to 30% decreased traffic control rate and 50 to 60% lesser delay in packet loss. We run simulations in a 400X400m with randomly generated networks topology. Unless stated otherwise, we set the percentage of the bad nodes to 10% the network size to 100 sensor nodes, the per-node packet reporting interval to 3 to below 10 packets measured and averaged based on simulations over 15 random networks. We report the packet analysis information for some of the node intervals(in homogenous network in between comparison, in heterogeneous network outside the bounded clusters range can be consider for communication.

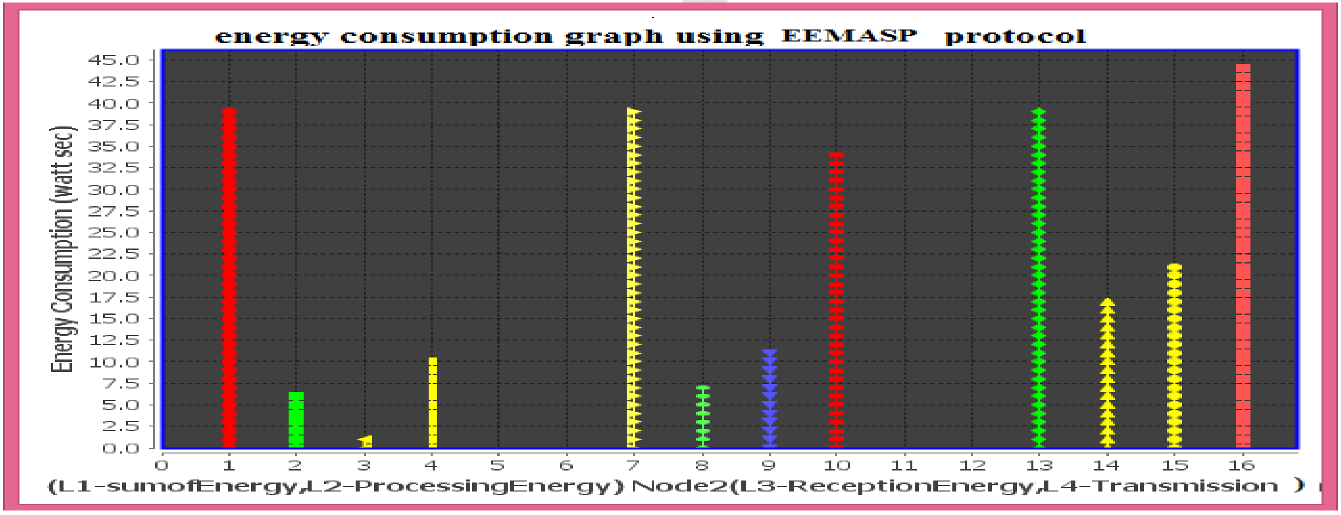


	sampleInterval=10	sampleInterval=20	sampleInterval=50	sampleInterval=200	sampleInterval=1000
🟦 WDC-TPA	8.77673	9.44849	11.3608	13.5634	14.1912
🟥 SWDC	8.20142	9.93617	11.7885	13.9684	17.7741
🟩 LEAWDC	10.77673	12.94849	15.8608	16.5634	18.1912
🟪 WDC-PPC	12.77673	14.94849	16.8608	17.5634	21.1912
🟦 EEMASAP	13.77673	15.94849	17.8608	19.5634	24.1912

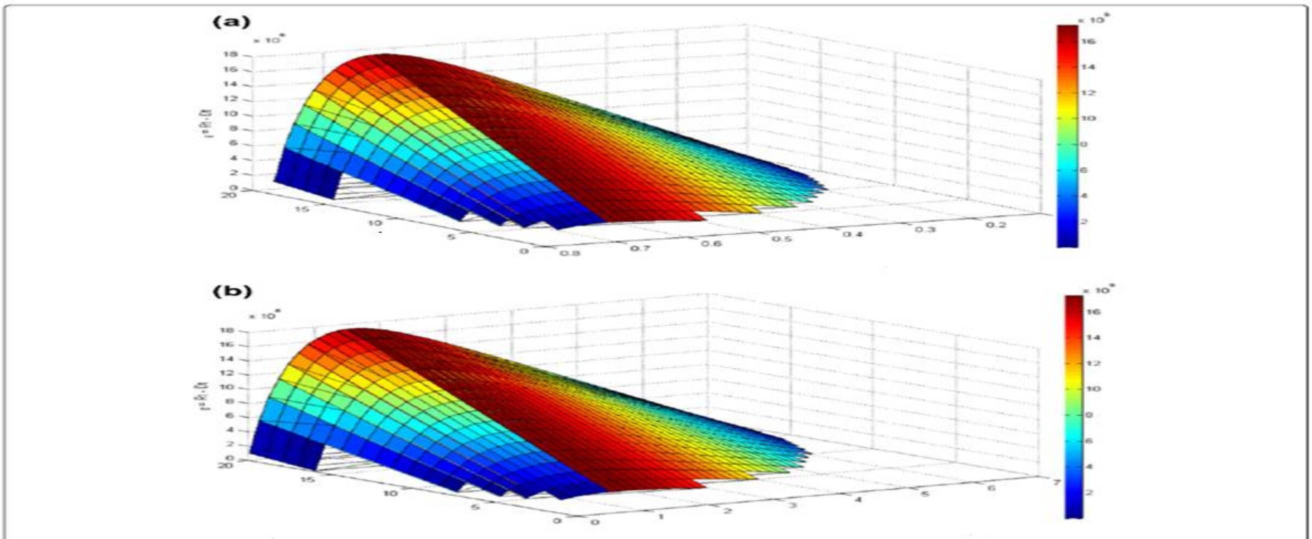
4.1 Life time Vs Protocols comparative analysis between EMMASP protocols with Existing Protocols



4.2Frames in bytes Vs Delay comparative analysis between EMMASP with existing protocols



4.3 energy consumption graph using EMMASP protocol EMMASP algorithm



the total achievable throughput for fault tolerance issue a) with respect to homogeneous b) heterogeneous

4.4 ***total achievable throughput for fault tolerance issue a)homogeneous networks b)heterogeneous networks using Glomosim simulator***

V CONCLUSION AND FUTURE WORK

The proposed work limited to homogeneous and heterogeneous networks only. In proposed work compared with proactive and reactive based routing protocols for homogeneous and heterogeneous networks but for hybrid networks the proposed protocol is limited. The proposed key management scheme works with Diffie-hellman key exchange algorithm for both networks but for hybrid networks need secure key exchange algorithms . The proposed algorithms APMRC and EMMASP algorithms supports both networks, Performance results of proposed model is compared with the existing sequential probability ratio test, by producing the 35 to 45% better reliability, 10 to 15% lesser energy utilization, 20 to 30% decreased traffic control rate and 50 to 60% lesser delay in packet loss**.** Apart from that, we also compare the performances of different multicast protocols namely ODMRP, Adaptive Demand-Driven Multicast Routing protocol (ADMR) and MAODV Routing protocol with EEMASP with some authenticate detection schemes. The analyses on effects of performances are studied for these protocols by further extending the number of receivers or sources and also increasing the number of nodes in various mobility scenarios using appropriate statistical methods / techniques. Performance metrics like Packet deliver ratio and End-to-End delay etc. are also considered for comparative analysis among these protocols.It gives evidence and leaves space for future hybrid network multicast routing as well.

REFERENCES

1. C.Sridevi (2018), "A survey on network security attacks and preventive measures", International journal of Computer Engineering and applications, volume XII, Issue 1, pp 338-345
2. Anuraj C.K., Dr.Shelbi Joseph(2017), "Analytical Study on Encryption Techniques and Challenges in Network security", International journal of emerging trends of technology in computer science(IJETTCS) volume 6, Issue 6. pp.153-162
3. J.Ajay Nayak, ch. Rambabu , Dr.V.V.K.D.V Prasad (2017), "Improving the network life time of wireless sensor network using EEEMR protocol with clustering algorithm", International Journal of Electronics, Electrical, and Computational System, volume 6, issue 6. pp.342-346.
4. anamika saini, Danish usmani (2017) "A Review on study of energy efficient clustering approaches for wireless sensor networks", International research journal of engineering and technology,pp.587-591.
5. Anamika saini, ashok kumar, H.L Mandoria and B.K. Pandey (2016)" A Study and analysis of DEEC protocols in heterogeneous WSNs using MATLAB", in international Research journal of engineering and technology vol 3, issue 8.
6. Bhuiyan Z. A. and G. Wang (2015). Local Area Prediction-Based Mobile Target Tracking in Wireless Sensor Networks, IEEE Transactions on Computer, Vol. 64, No.7, pp. 1968–1982.
7. Andreou, P. G., D. Zeinalipour-Yazti, G. S. Samaras and P. K. Chrysanthis (2014). A network-aware framework for energy-efficient data acquisition in wireless sensor networks, *Journal of Network and Computer Applications*, Vol. 46, No. 1, pp. 227– 240.
8. Saman Taghavi zargar(2013) A Survey of Defense Mechanisms Against Distributed Denial of Service(DDoS) flooding attacks, IEEE communications survey and tutorials,pp 1-23.
9. Bakaraniya, P. and S. Mehta (2013). K-LEACH: An improved LEACH protocol for lifetime improvement in WSN. International Journal of Engineering Trends and Technology, Vol 4, No. 5, pp. 1521-1526.

10. Khiati, M. and D. Djenouri (2012). Cluster-Based Fast Broadcast in Duty- Cycled Wireless Sensor Networks, *Proc. of 11th IEEE International Symposium on Network Computing and Applications,* Cambridge, pp. 249–252, 2012, United States of America.
11. Liu, A., Z. Zheng, C. Zhang, Z. Chen and X. S. Shen (2012). Secure and Energy-Efficient Disjoint Multipath Routing for WSNs, *IEEE Transactions on Vehicular Technology*, Vol. 61, No. 7, pp. 3255–3265.
12. Baroudi, U., (2007). EQoSa: energy and QoS aware MAC for wireless sensor networks, *9th International Symposium on Signal Processing and Its Applications,* Sharjah, pp. 1–4, 2007, United Arab Emirates.
13. Al-Karaki J.N. and E. Kamal (2004). Routing Techniques in Wireless Sensor Networks: A Survey, *IEEE Wireless Communication*, Vol. 11, No. 6, pp. 6–28.
14. Ahmed, A., H. Shi and Y. Shang (2003). A survey on network protocols for wireless sensor networks, *Proc. International Conference on Information Technology:Research and Education,* New Jersey, pp. 301–305, USA.
15. Akyildiz, F., W. Su, Y. Sankarasubramaniam and E. Cayirci (2002). "A survey on sensor networks", *IEEE Communications Magazine*, Vol. 40, No. 8, pp. 102–105.

.