IFERP
connecting engineers... developing research

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering
(IJERCSE)
Vol 5, Issue 4, April 2018

SAMRAM Adversary Model to Reduce Network Degradation problems in Wireless Sensor networks using APMRC Algorithm

[1] D J Samatha Naidu, [2]Dr.Ande Prasad
[1] Research Scholar, [2] Principal
[1][2] Vikrama Simhapuri University, Nellore

Abstract: To address this issue of network degradation problem in wireless sensor networks, Source level analysis to manage and reconfigure adjusting cluster head model(SAMRAM adversary Model) 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 two phase locking communication protocol based on same cluster zone partition using centriod and partitioning based databases related networks. 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. 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 packet dropping and link and node failures, to solve the problems uses inter cluster and intra cluster mechanism for multi-hop packet transmission it allows hop-to-hop distribution of packet load and localize security control for clustered based networks. APMRC ALGORITHM is proposed to overcome network degradation problems in wireless sensor networks. We can solve following issues in wireless sensor networks like issue 1:Mobility of sink , issue 2:Fault Tolerance, Issue 3: Authentication, Issue 4: Multipath Scheduling.

Keywords: Wireless Sensor Network, SAMRAM adversary model, APMRC algorithm, Methodology

INTRODUCTION

Past recent years, Wireless Sensor Network is defined unstructured huge number of nodes which are as being deployed and every time its monitors the route node abnormalities while collecting data and also routes the data to sink or source stations. Conditionally wireless sensor networks having several limitations with respect towards energy efficiency, power supply, regarding bandwidth issues while connecting sensor nodes. Some of the design challenges ar e arise with regard of energy efficiency utilization in both homogeneous and heterogeneous network lifetime, hardware utility constraints, data aggregation level, data fusion issues, network cost, fault tolerance, stability, reliability etc.[1]
We categorize the WSN in two architectures:

(1) homogeneous and
(2) heterogeneous.

Under homogeneous architecture
we have proposed Improved Energy Efficient Clustering Hierarchy and Data Accumulation (IEECHDA) scheme for homogeneous WSNs. The main focus of IEECHDA scheme is to analyze the optimal probability with which a node will become a CH in order to minimize the network's energy consumption.[9][10] It Proposes Alternative reconfiguration technique that allows the router to take individual prior type of decisions without having overheads of network [2] degradation packets like packet dropping, node failures, weak link failures etc. Under heterogeneous architecture, we have assumed two approaches: single hop approach and multi-hop approach

A. Problems with existing algorithms

(i) It has less coverage area and low throughput will lead the damage of packets.
(ii) This system provides less security from security vulnerabilities leads with security attacks
(iii) It contains overall authentication overheads.
(iv) It reserves only for either central, distributed, hybrid.

II PROPOSED WORK

In existing work, packet dropping attack has always been major threat to the security in WSNs, because the sensor node easily compromised with attackers which deals with Denial of service based attacks and jamming attacks. The proposed mechanism of a novel IDS named as Active pro self configure routing algorithm specially design to gather the information from different networks .[3-8]. The main challenges are how to select Cluster Heads (CHs) in efficient manner to provide maximum lifetime, stability to network and how to provide maximum throughput and scalability to the network.

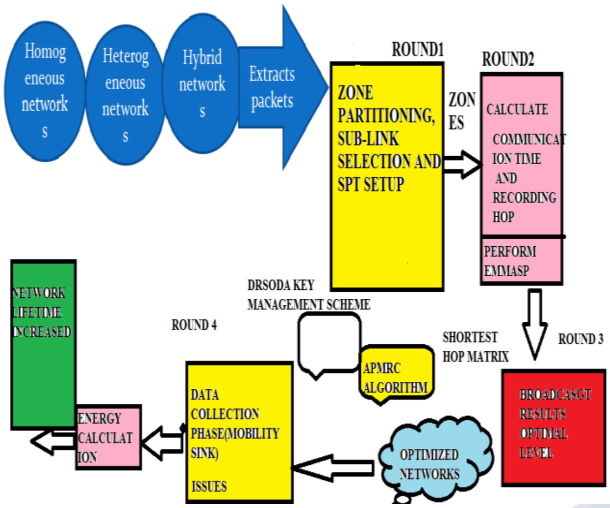

Homogeneous networks
Heterogeneous networks
Hybrid networks
Extracts packets
ROUND1
ZONE PARTITIONING, SUB-LINK SELECTION AND SPT SETUP
ZONES
ROUND2
CALCULATE
COMMUNICATION TIME AND RECORDING HOP
PERFORM EMMASP
ROUND 3
BROADCASGT RESULTS OPTIMAL LEVEL
SHORTEST HOP MATRIX
DRSODA KEY MANAGEMENT SCHEME
APMRC ALGORITHM
OPTIMIZED NETWORKS
ROUND 4
DATA COLLECTION PHASE(MOBILITY SINK)
ISSUES
ENERGY CALCULATION
NETWORK LIFETIME INCREASED

FIG 1 : Proposed architecture of SAMRAM MODEL

III ActivePro Multiple Routing Configurations(APMRC)

we present a new algorithm called ActivePro Multiple Routing Configurations (APMRC). In this paper we present APMRC, and analyze its performance with respect to scalability, backup path lengths with edges , backup path lengths with weighted edges, load on individual links to reduce network degradation, recovery local distribution algorithms through APMRC, theorem and proofs and thus reduce the chances of congestion problems when APMRC is used. [3][4]

Recovery load distribution through APMRC

(a) The link weight assignment used in the normal configuration The structure of the backup configurations, i.e., which links and nodes are isolated in each .The specific node link weight assignments used in the duplicated backup configurations.
(b) Mobility of sink problems can be reduced.
(c) fault tolerance issues are overcome.
(d) Mutlipath scheduling issues
(e) Authentication based problems are overcome.

IVAPMRC Algorithm for Network Classification

The Classification of nodes can be taken in any one of the following cases.
Packet dropping is Conform.
Packet Suspected to drop

Theorem

The bad nodes eventually identifies with high detection rate and Nack. The Proposed Schemes can be extended for identifying packet modifiers or packet droppers. Packet modifiers or packet droppers. It Provides hop-by-hop authentication scheme.

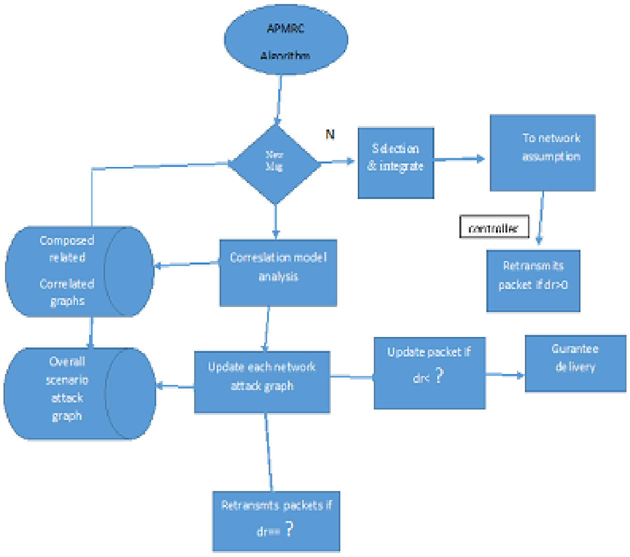
Proof

(i) With Respect to homogeneous networks each sensor node V, The mobile sink node S keeps track of the Total packets sent from V and the total packets received by S.
(ii) With respect to heterogeneous networks, each end of the round, the mobile sink node S calculates the dropping ratio (or) delay ratio for each sensor node V. Nsend is the number of transmitted packets, Nrec is the number of received packets. The dropping or delay ratio (dr) can be calculated for each round as follows:

$$(Nsend - Nrec \ast Nsend) - dr$$
-- -
$$Nsend + Nrec + (Nsend \ast Nsend - Nrec) \text{-}\rightarrow (1)$$

Based on the dropping ratio or delay ratio of each node and the complete tree topology is used, the mobile sink categories the nodes based upon the APMRC algorithm for network classification. This algorithm identifies the sensor networks ɵ is first introduced ,possibly droppers and suspected droppers. So, Hence threshold can be maintained.

V Work flow of APMRC algorithm


APMRC Algorithm
New Msg
N
Selection & integrate
To network assumption
controller
Retransmits packet if dr>0
Composed related Correlated graphs
Correslation model analysis
Overall scenario attack graph
Update each network attack graph
Update packet if dr< ?
Gurantee delivery
Retransmts packets if dr== ?

Algorithm

APMRC Algorithm : Tree Based Networks Classification Algorithm

```
Input : Network Tree NT, with each sensor node V, and its dropping or delay ratio dr, threshold value ɵ , mobile sink node S.
Output : Identified dropped packets and collisions malicious nodes to retransmit packets.
Method:
Step 1. For every mobile sink node is T do
Step 2  find dropping or delay ratio dr
Step 3 a if dr < ɵ   then b Set  V as food for guarantee transmission otherwis suspected bad transmission
Step 4: if dr  = = ɵ  then
Set   as good for guarantee transmission
else
Step:5 if dr > ɵ then
Set   as suspected bad transmission or packet dropped, delay may occurred
Step:6 else
        Break
Step:7 set        as suspected bad for good guarantee transmission
Step 8:repeat
Step 9:select a packet and check the value
Step 10:if ack==0 then
Success(positive acknowledge successfully generated)
else
Step 11:if ack==1 then
(negative acknowledge successfully generated) Fail

Step 12 if(ack==1)&&(packet=-1)then
retransmit the packet
Heterogeneous networks
Step 13: repeat step 01 to step 02
Step 14: categorize all networks in equi-partition
Step 15:apply clustering technique to classify nodes
Step 16:in each round group of sensor elects a (common node)shortest common path node to transmit packets.
Step 17:if  dr > ɵ then Node consists dropped packets due to traffic, collisions and malicious nodes.
Step 18: if dr < ɵ  then sensor node packets not dropped(good),or suspected dropped packet(not good)
Step 19: if dr== ɵ then sensor node has not dropped packets
Step 20:if((dr< ɵ) && (dr> ɵ))then sensor node is packet not  transmitted due to dropped packets.
Step 21: retransmitted damaged or dropped packets
Step 22: stop
```

Theorem 2

We assume that if mobile sink node packets are delayed or dropped intentionally by forwarding group of nodes, then dropping ratio should not be greater than ɵ.

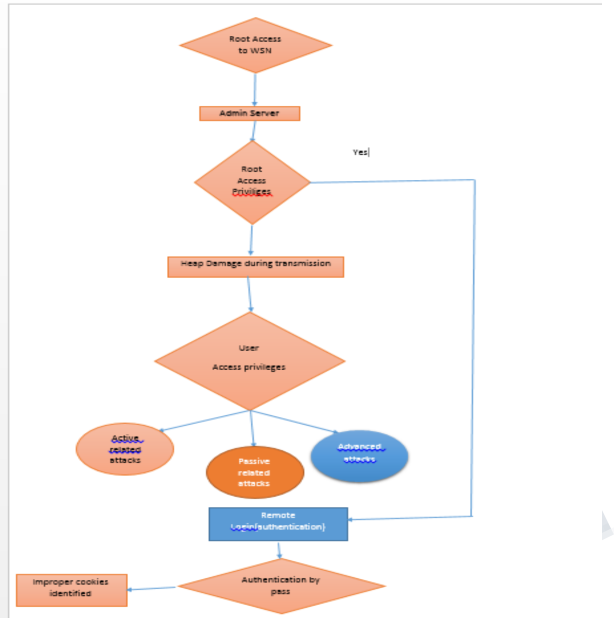


Fig 3: Test the network attacker graph

Lemma :

If ɵ should be greater than 0.

Let assume that value of ɵ = 0.5

Test the network attacker graph for Estimator Methodology

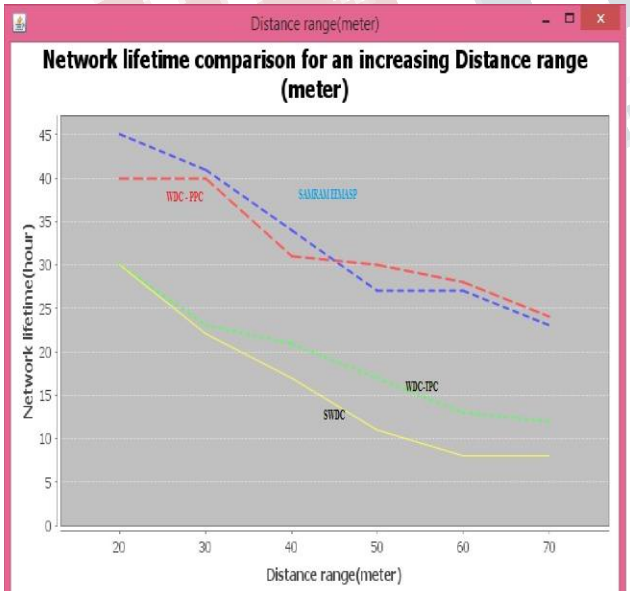
VI Performance Metrics and Simulation Results

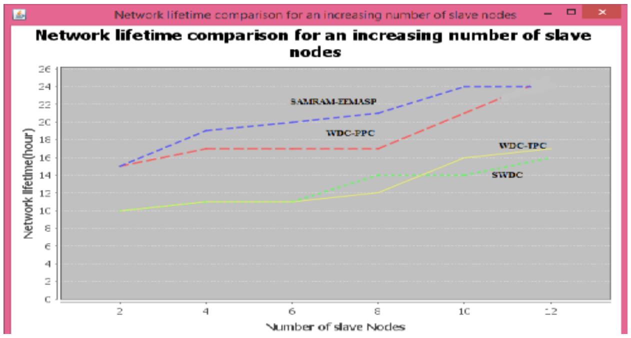
Performance metrics like Packet deliver ratio and End-to-End delay etc. are also considered for comparative analysis among these protocols used SAMRAM EEMASP protocol introduced to increased network life time. Below we have compared with few existing protocols.

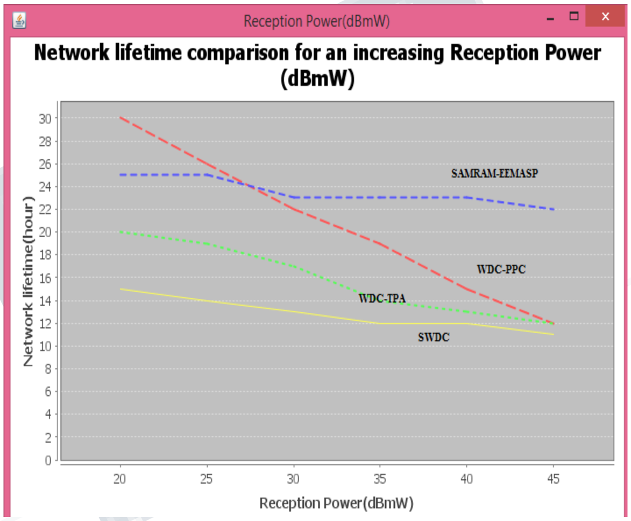
We run simulations in a 400X400m with randomly generated networks topology. Unless stated otherwise, we set the percentage of the bad nodes to 10% the network size to 100 sensor nodes, the per-node packet reporting interval to 3 to below 10 packets measured and averaged based on simulations over 15 random 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.

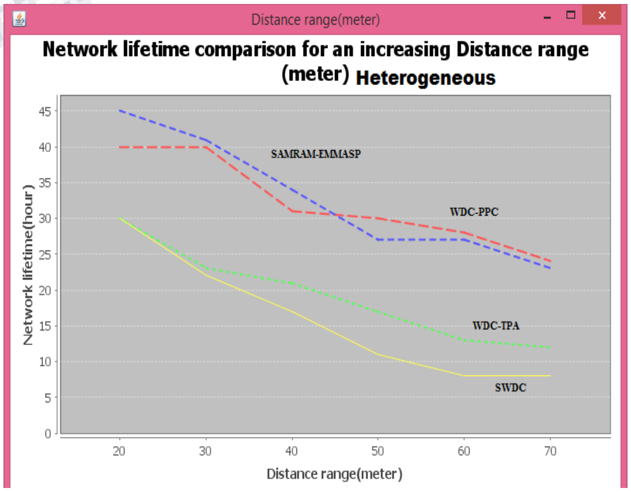
Table 1 Analysis of packet information for node interval communication within the homogeneous and heterogeneous with sample range of 100 nodes.

Type of network	Node interval	Detection rate	packet status
homogenous	10-20	0.0000000	No packet drops
homogenous	20-40	0.0000000	No packet drops
homogenous	40-60	0.977423	packet drops
homogenous	60-80	0.400044	suspiciously packet drops
homogenous	80-100	0.913749	packet drops
heterogeneous	10-20	0.0000000	No packet drops
heterogeneous	40 -60	0.993395	packet drops
heterogeneous	80-100	0.987742	packet drops
heterogeneous	More than 100	~NAN	No packet Transmission









VI. CONCLUSION

Finally, we conclude that the proposed model effective prevents Reduces network degradation problems in wireless sensor networks. Energy of node will be increased and node failures and security attacks can be prevented. This model applicable for both heterogeneous and homogeneous networks. future work can be extended for hybrid networks.

ACKNOWLEDGMENT

We are thankful for all referenced authors cited below.

REFERENCES

[1] Ramkishor Kourav, Prof. Pankaj Rechariya; Probability Based Clustering For Efficient Energy Conservation Routing in Sensor Network. International Journal of Scientific Progress And Research (IJSPR), Vol. 28, No. 02, Pages 80-83, 2016, ISSN: 2349-4689.

[2] Ramkishor Kourav, Prof. Pankaj Rechariya; Literature Review on Different Routing Methodologies in Wireless Sensor Networks. International Journal of Innovative Trends In Engineering (IJITE), Vol. 22, No. 01, 2016 Pages 31-36, 2016, ISSN: 2395-2946.

[3] Chand, K.K., Bharati, P.V., Ramanjaneyulu, B.S., Optimized Energy Efficient Routing Protocol for life-time improvement in Wireless Sensor Networks, Advances in Engineering, Science and Management (ICAESM), 2012 International Conference on , vol., no., pp.345,349, 30-31 March 2012.

[4] Katiyar, V., Chand, N., Gautam, G.C., Kumar, A Improvement in LEACH protocol for large-scale wireless sensor networks, Emerging Trends in Electrical and Computer Technology (ICETECT), 2011 International Conference on , vol., no., pp.1070,1075, 23-24 March 2011.

[5] Arabi, Z., HERF: A hybrid energy efficient routing using a fuzzy method in Wireless Sensor Networks, Intelligent and Advanced Systems (ICIAS), 2010 International Conference on , vol., no., pp.1,6, 15-17 June 2010.

[6] Yanwei Wu, Xiang-yang Li, Mo Li, Wei Lou, Energy-Efficient Wake- Up Scheduling for Data Collection and Aggregation, Parallel and Distributed Systems, IEEE Transactions on , vol.21, no.2, pp.275,287,Feb. 2010.

[7] Z.A. Eu, H.P. Tan, and W.K.G. Seah. Opportunistic routing in wireless sensor networks powered by ambient energy harvesting. Computer Networks, 54(17):2943_2966, 2010.

[8] N. Pantazis, S. Nikolidakis, and D. Vergados. Energy-e_cient routing protocols in wireless sensor networks: A survey. [9] S.K. Singh, MP Singh, and DK Singh. Routing protocols in wireless sensor networks_a survey. International Journal of Computer science and engineering Survey (IJCSES), 1(2):63_83, 2010.

[10] DA Vidhate, AK Patil, and SS Pophale. Performance evaluation of low energy adaptive clustering hierarchy protocol for wireless sensor networks. 6)Mobile Applications and Testing: https:// experitest. com/blog/seetestautomation/streamline-cicdmethodology-blog/