To Prevent Security Attacks and Network Degradation Problems in Wireless Sensor Networks

[1] R. Nivedha, B.TECH, M.TECH
[2]S.Arshiya Sulthana B.TECH, M.TECH
[1,2]*Assistant Professor,*
[1,2]*Department of Computer Science and Engineering,*
[1,2]*Golden Valley Integrated Campus (Affiliated to JNTU Anantapur).*
Andhra Pradesh.

Abstract—

Social affair the data of the Wireless Sensor Networks effective information accumulation is one of the primary issue like Heterogeneous and homogeneous based systems. Ongoing works have demonstrated that sink versatility improves the information accumulation and furthermore the vitality proficiency in the remote sensor systems. Be that as it may, In Existing Work, because of the way compel, a portable sink has restricted correspondence time to gather information from the sensor hubs conveyed haphazardly. These gangs noteworthy difficulties in together improving the measure of information gathered and decreasing the vitality utilization. In Proposed Work, To address this issue, a novel information gathering calculation called Enhanced Min-Max most brief path(EMMASP) and Source level investigation to oversee and reconfigure changing group head model(SAMRAM Model) that builds arrange throughput just as monitors vitality by streamlining the task of sensor hubs in the system is actualized. SAMRAM display is actualized as a two stage locking correspondence convention dependent on same bunch zone parcel. The re-directing procedure costs in data transmission and hub vitality utilization and the additional steering inactivity may influence QOS for system applications, debasing the system execution. To give rapid and top notch remote administrations with secure route in remote sensor systems. It centers around, Sensor hub Compromise, roof dropping and changing bundles drives security issues and the designation of traffic in different directing ways drives security issues. To illuminate this proposing a plan called Dynamically Routed Self Organized Distributed Authentication and key administration conspire, utilizes entomb 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. 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, EMMASP, SAMRAM adversary model, APMRC algorithm, Dynamically Routed Self Organized Distributed Authentication and key management scheme.*

I. INTRODUCTION

A WSN is characterized as being made out of countless which are sent thickly in nearness to the marvel to be checked. Every one of these hubs gathers information and courses the information to a sink or Base Station (BS). WSN have a few confinements, for example, constrained vitality supply, restricted figuring force, and restricted transmission capacity of the remote connections associating sensor hubs. A portion of the plan difficulties are vitality productivity, heterogeneity,network lifetime, equipment limitations, information accumulation/combination, multi-bounce directing, adaptation to non-critical failure, strength, arrangement organize cost and, and so forth.

The systems have self-sorting out abilities since the places of individual hubs are not foreordained. Collaboration among hubs is the prevailing element of this kind of system, where gatherings of hubs coordinate to spread the data accumulated in their region to the userIn Wireless Sensor organizes, every sensor hub has restricted remote computational capacity to process and exchange the live information to the base station or information accumulation focus. In social occasion the data of the WSN productive information accumulation is one of the primary issue. To address this issue, a novel information accumulation method called Enhanced Min-Max Amount shortest path(EMMASP) can be used to collect information from heterogeneous and homogenous There are three types of data transmission techniques are used namely unicasting , multicast, broadcast for transmission of packets in Wireless Sensor Networks. The below mentioned schemes and techniques used:

- Clustering
- Enhanced Digital Signature with Secure hash session misused key detection scheme(EDSHSMKD).
- To design an energy efficient protocol for both intra-cluster and inter-cluster transmission for heterogeneous and homogeneous networks.
- **Example of Clustered based key management scheme**

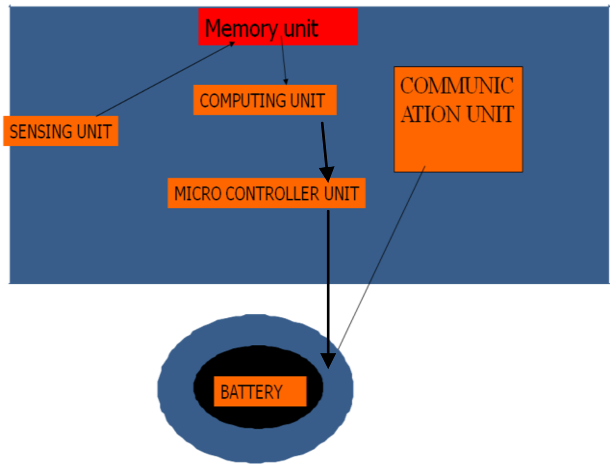


Fig:1. Architecture of wireless sensor networks

II. RELATED WORK

Hearty information total is a genuine worry in WSNs and there are various tasks examining noxious information infusion by considering the different enemy models. There are three groups of business related to our examination : IF calculations, trust and notoriety frameworks for WSNs, and secure information collection with traded off hub discovery in WSNs.

There are various distributed investigations presenting IF calculations for taking care of information accumulation issue . We inspected three of them in our near tests in proposed six unique calculations, which are on the whole iterative and are similar. The main distinction among the calculations is their decision of standard and accumulation work. Aydayet al. proposed a slight diverse iterative calculation in their fundamental contrasts from different calculations are:

1) The appraisals have a period markdown factor, so in time, their significance will become dull; and

2) The calculation keeps up a boycott of clients who are particularly terrible raters. proposed an iterative calculation which past just utilizing the rating framework, additionally utilizes the informal community of clients. Despite the fact that the current IF calculations think about straightforward deceiving conduct by enemies, none of them consider modern malignant situations, for example, conspiracy assaults.

This work is likewise firmly identified with the trust and notoriety frameworks in WSNs. Ganeriwal et al. in proposed a general notoriety system for sensor organizes in which every hub builds up a notoriety estimation for different hubs by watching its neighbors which make a trust network which utilizes relationship to distinguish broken readings. Besides, they acquainted a positioning structure with partner a dimension of dependability with every sensor hub dependent on the quantity of neighboring sensor hubs are supporting the sensor. Proposed PRESTO, a model-driven prescient information the board design for various leveled sensor systems. PRESTO is a two level structure for sensor information the board in sensor systems. The fundamental thought of this structure is to consider various intermediary hubs for overseeing detected information from sensor hubs. Proposed an interdependency connection between system hubs and information things for surveying their trust scores dependent on a patterned structure.
The primary commitment of Sun et al. in is to propose a blend of trust system, information accumulation, and adaptation to non-critical failure to upgrade information dependability in Wireless Multimedia Sensor Networks (WMSNs) which considers both discrete and consistent information streams. Tang et al. in proposed a trust framework for sensor networks in cyber physical systems such as a battle-network in which the sensor nodes are employed to detect approaching enemies and send alarms to a command center. Although fault detection problems have been addressed by applying trust and reputation systems in the above research, none of them take into account sophisticated collusion attacks scenarios in adversarial environments. Reputation and trust concepts can be used to overcome the compromised node detection and secure data aggregation problems in WSNs.

Proposed a system to recognize traded off hubs in WSN and afterward apply a product confirmation for the distinguished hubs. They revealed that the denial of recognized traded off hubs can not be performed because of a high danger of false positive in the proposed plan. The principle thought of false aggregator identification in the plan proposed in is to utilize various checking hubs which are running accumulation activities and giving a MAC estimation of their conglomeration results as a piece of MAC in the esteem registered by the group aggregator. High calculation and transmission cost required for MAC-based uprightness checking in this plan makes it unacceptable for arrangement in WSN. Lim et al. in proposed an amusement hypothetical barrier methodology to ensure sensor hubs and to ensure an abnormal state of reliability for detected information. Also, there is a vast volume of distributed examinations in the zone of secure minor total in WSNs. These examinations center around identifying false accumulation activities by an enemy, that is, on information aggregator hubs getting information from source hubs and creating incorrectly amassed qualities. Thusly, they address neither the issue of false information being given by the information sources nor the issue of agreement. Be that as it may, when an enemy infuses false information by an intrigue assault situation, it can influences the aftereffects of the legitimate aggregators and therefore the base station will get skewed total esteem. For this situation, the traded off hubs will authenticate their bogus information and subsequently the base station expect that all reports are from fair sensor hubs. In spite of the fact that the previously mentioned research take into account false data injection for a number of simple attack scenarios, to the best of our knowledge, no existing work addresses this issue.

As indicated by Shashidhar Rao Gandham, Milind Dawande, Ravi Prakash and S.Venkatesan are proposed a calculation on Energy Efficient Schemes for remote Sensor Networks with Multiple Mobile Stations. One of the principle configuration issues for a sensor arrange is preservation of the vitality accessible at every sensor hub. They propose to send different, portable base stations to draw out the lifetime of the sensor organize. They split the lifetime of the sensor organize into equivalent timeframes known as rounds. Base stations are moved toward the beginning of a round. Our technique utilizes a whole number direct program to decide new areas for the base stations and a flow-based steering convention to guarantee vitality efficient directing amid each round. They propose four assessment measurements and look at our answer utilizing these measurements. In view of the reproduction results we demonstrate that utilizing various, portable base stations as per the arrangement given by our plans would significantly expand the lifetime of the sensor organize Survey.

The arrangement we propose in this task recommends that the base station be portable; along these lines, the hubs found near it change after some time. Information gathering conventions would then be able to be improved by considering both base station portability and multi-jump directing. They first think about the previous, and reason that the best portability procedure comprises in following the outskirts of the system (we expect that the sensors are conveyed inside a circle). They consider mutually versatility and steering calculations for this situation, and demonstrate that a superior directing technique utilizes a blend of round courses and short ways. They give a definite expository model to every one of our announcements, III.PROBLEM DEFINITION

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) plot for homogeneous WSNs. The fundamental focal point of IEECHDA plot is to break down the ideal likelihood with which a hub will turn into a CH so as to limit the system's vitality utilization. It Proposes Alternative reconfiguration procedure that enables the switch to take individual earlier sort of choices without having overheads of system debasement parcels like bundle dropping, hub disappointments, frail connection disappointments and so forth.

Under heterogeneous architecture, we have assumed two approaches:
(1) single hop approach and
(2) multi-hop approach

A. Problems with existing algorithms

- 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.

III. 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 .

- 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.

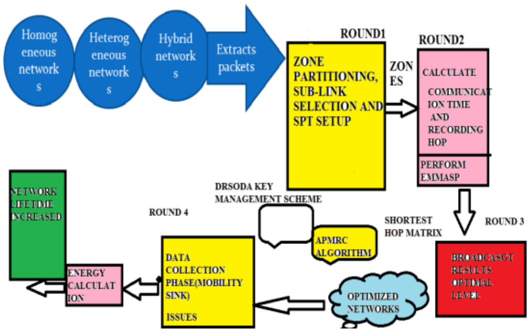

Homogeneous networks
Heterogeneous networks
Hybrid networks
Extracts packets
ROUND1
ZONE PARTITIONING, SUB-LINK SELECTION AND SPT SETUP
ZONES
ROUND2
CALCULATE COMMUNICATION TIME AND RECORDING HOP
PERFORM EMMASP
ROUND 3
SHORTEST HOP MATRIX
BROADCASGT RESULTS OPTIMAL LEVEL
DRSODA KEY MANAGEMENT SCHEME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

FIG 2 : Proposed architecture of SAMRAM MODEL

A. ActivePro Multiple Routing Configurations (APMRC)

We present a new recovery scheme called ActivePro Multiple Routing Configurations (APMRC). It can be implemented with only minor changes to existing solutions. In this thesis it presents 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 **AP**MRC is used.

Recovery load distribution through APMRC

(a) The link weight assignment used in the normal configuration

(b) The structure of the backup configurations, i.e., which links and nodes are isolated in each

(c) The link weight assignments used in the backbones of the backup configurations.

B. DRSODA key management scheme

The proposed new DRSODA key management scheme for clustered based multi-hop scheme used for hop-by-hop distributed and localized security control for multi-hop clustered based networks which not only helps in security measures but also reduce the authentication problems with key maintenance overheads and also it suitable for distributed and Centralized or Hybrid related security control algorithms.

- DRSODA network assumption model
  - Node assumption
  - Operations
    - Certificate request/reply.
    - Acknowledgements
  - Notations

DRSODA key management scheme rotates the packets dynamically irrespective of three types of multi-hop networks it follows two mechanisms:

1. It provides security by using hop-by-hop authentication and key management schemes in multi-hop networks it minimizes the overall authentication overheads and countermeasures for security vulnerabilities.
2. This network generate efficient keys and certificates and their local repositories for storage purpose. Multi-hop networks can provide more converge area and it can able to produce high throughput.

- New routing algorithms such as multi tier data dissemination model for large scale WSN are needed in order to handle the overhead of mobility and topology changes in such energy constrained . The following are part describe some of these issues and challenges.
- How to effectively utilize the bandwidth and energy application.
- To make sensor nodes self-organizing and self reconfigurable.
- To make routing protocols secure in WSNs
- To satisfy dense sensor networks with a large number of nodes.

Apart from the above related problems our contribution work in this paper is as follows:

Problem 1.Related to Hot spot, energy hole problems to rectify.

To consider the network life time because minimizing the total energy consumption may not lead to maximum network lifetime and the proposed scheme is considered for different trajectories for the mobile sink to the validation process.

- **Solution:** The EMMASP is an efficient data collection scheme which maps between sensor nodes and sub sinks is optimized with two phase communication locking protocol to maximize the amount of data collected by mobile sinks and also balance the energy consumption in the network. The proposed methods in terms of data gathering and utilization of the energy in the networks.

Problem 2.The node clone is serious and dangerous one

In sufficient storage consumption performance in the existing system and low security level. Existing mechanisms or algorithms have overhead problems but it doesn't having control over Dos and other attacks.

Solution: To analyze existing solutions under the proposed model. By finding transformation of observed data and removes or minimizes the effect to the nuisance information that leads to avoid low security level problems. here proposing an advanced distributed node detection algorithm to identify failure nodes in WSNs.

Sensor node Compromise, eaves dropping and modifying packets leads security problems

- Basically WSNs doesn't have proper infrastructure due to that the network topology can changes drastically during transmission period of time , the attacker might have chance to compromise the sensor node at any hierarchical level and can make eaves dropping and modifying packets leads security problems .In proposed frame work conflict detection and resolution conflicting segments are identified and address the problem of packet dropping and modification.

Solution: To propose a simple yet effective scheme to identify misbehaving forwarders to modify packets. Extensive analysis and simulations have been conduct and verify the effectiveness of the proposed scheme in various scenarios

(i) Being effective in identifying both packet dropper and modifier.

(ii) low communication and energy overhead and

(iii) being compatible with existing false packet filtering schemes.

To identify the bad nodes with small false positives using advanced routing algorithm in WSNs can be useful for solution.

Problem 4: Reduce the impact of failures in networks and network disconnection and network cut node problems.

■ Existing cut detection system deployed only for wired networks. The following

■ Limitations are identified in existing work (i)Unsuitable for dynamic network configuration.

■ ii) single path routing approach

■ (iii) Algorithm proposed only for detecting linear cuts in the networks.

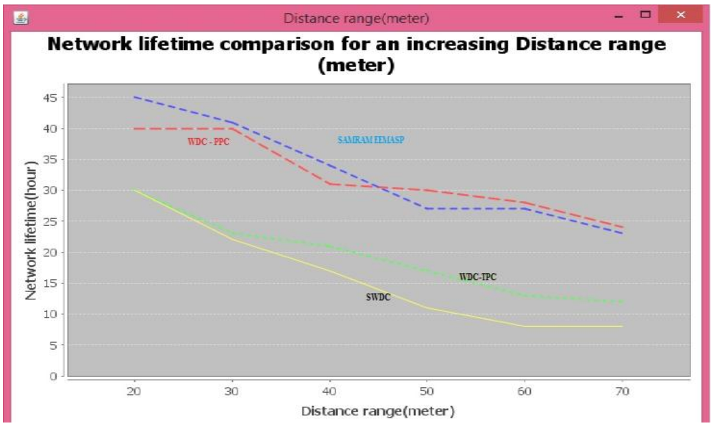
■ (iv) In flooding based techniques, routes from the nodes to the base station and back have to recomputed when node failures occur

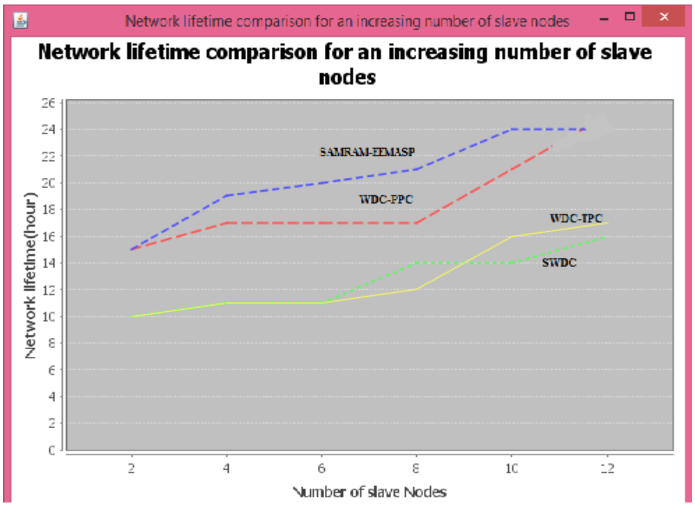
■ .(v) critical overhead come at the cost of high rate of incorrect detection.

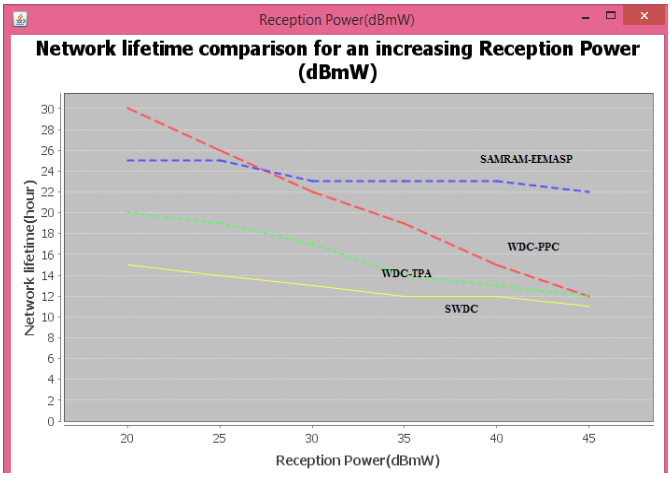
Solution: Comes with provable characterization on the Dos detection accuracy. BCCOS events detection can be identified. Enhanced DCD algorithm enables base station and also node to detect if it is disconnected from the base station.

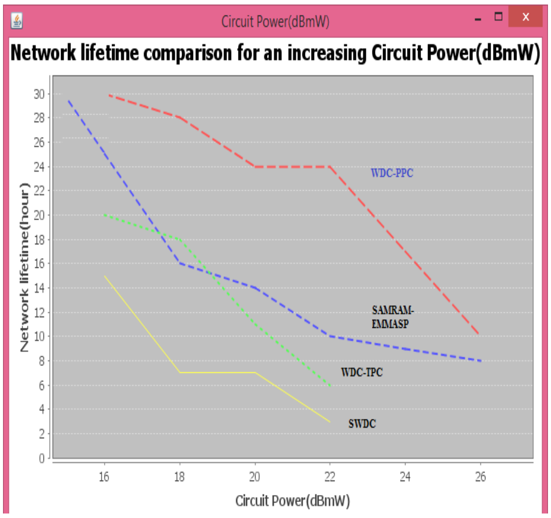
IV. PERFORMANCE METRICS AND SIMULATION RESULTS

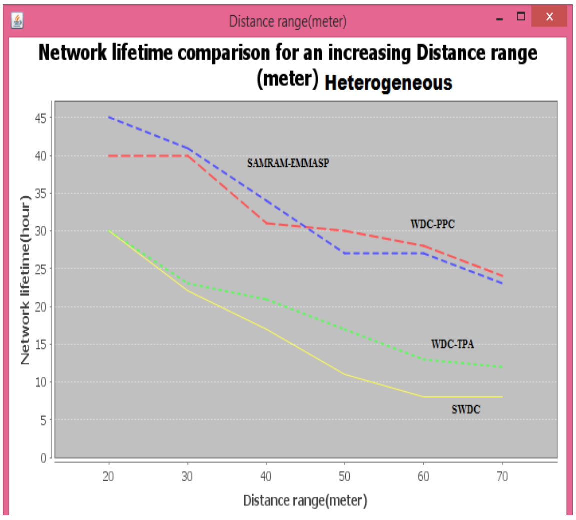
Performance metrics like Packet deliver ratio and End-to-End delay etc. are also considered for comparative analysis among these protocols.











V. CONCLUSION

Finally, we conclude that the proposed model effective prevents security attacks and 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.

REFERENCES

[1] S. Ozdemir and Y. Xiao, "Secure data aggregation in wireless sensor networks: A comprehensive overview," Comput. Netw., vol. 53, no. 12, pp. 2022–2037, Aug. 2009.

[2] L. Wasserman, All of Statistics : A Concise Course in Statistical Inference. New York, NY, USA: Springer,.

[3] A. Jøsang and J. Golbeck, "Challenges for robust trust and reputation systems," in Proc. 5th Int. Workshop Security Trust Manage., Saint Malo, France, 2009, pp. 253–262.

[4] K. Hoffman, D. Zage, and C. Nita-Rotaru, "A survey of attack and defense techniques for reputation systems," ACM Comput. Surveys, vol. 42, no. 1, pp. 1:1–1:31, Dec. 2009.