A Study on Efficient and Cost-Effective Measures to Preserve Communication Security and Privacy of Data in WSNs

#1 K.Ramesh Rao, *2 Dr. S.N.Tirumala Rao, #3 Prof. P. Chenna Reddy

[1] Reseacrch Scholor, Dept. of CSE, JNTUA , Anantapuramu (A.P)-India
[2] Professor, Dept. of CSE, NarasaraoPet Engineering College, Narasaraopet, Guntur (A.P)-India
[3] Professor, Dept. of CSE, JNTU College of Engineering, Pulivendula, Kadapa, (A.P)-India
[1] karanamramesh@yahoo.com
[2] naga_tirumalarao@yahoo.com

***Abstract:* A Wireless Sensor Network (WSN) refers to a collection of low-power wireless devices connected through radio communication facilities. These devices have limited methoding speed, storage capacity, and communication bandwidth. They can be deployed in a distributed environment sensing, monitoring or collecting data, methoding and communicating the data and coordinating actions with other peers or nodes at a higher hierarchy in an infrastructural setting. Such WSNs have a wide range of potential applications including utilities, transportation system automation, and patient's medical condition monitoring, etc. Some of these application areas impose stringent privacy and security requirements on data transmissions, methods and management. Assuming reliable cryptographic techniques can be used to provide communication security, it is not clear how data privacy could be preserved in such a context.**

I. INTRODUCTION

The wireless sensing element network is created by sizable amount of sensing element nodes. sensing element nodes could also be homogenized or heterogeneous. These networks are extremely distributed and incorporates several variety of less value, less power, less memory and self-organizing sensing element nodes. The sensing element nodes have the aptitude of sensing the temperature, pressure, vibration, motion, humidity, sound as in [1] etc. These sensing element nodes consists four main units: sensing unit, methoding unit, transmission unit, and electrical measure unit. For listening event, sensing element nodes are programmed. once an occasion happens, by generating wireless traffic sensors inform the top purpose or sink node. In wireless sensing element networks because the variety of sensing element nodes will increase the possibilities of congestion will increase close to the event. There are numerous applications of WSN like forest observation, producing, forecast systems, military police work, health, home, workplace observation and plenty of intelligent and good systems. Knowledge aggregation in wireless sensing element networks is a very important technique as a result of it helps in reduction of energy consumption, communication overheads and tries to cut back the matter of localized congestion. It permits collection helpful knowledge from the sensing element nodes so transmittal helpful knowledge to the top nodes or sink node.

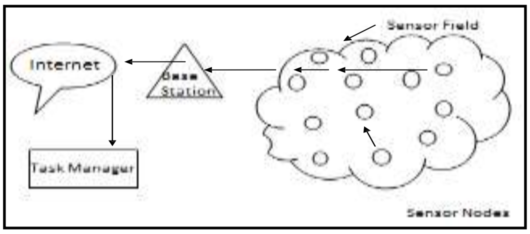

Fig1.Communication Architecture for WSN

II. DATA AGGREGATION IN WSN

Data Aggregation may be a technique of mixing and summarizing the information from device nodes in wireless device networks by victimization aggregation operate like grievous bodily harm, MIN, AVG, COUNT, total as in [2] etc. on someone nodes. Information Aggregation may be a technique of eliminating redundant information from numerous device nodes. information aggregation techniques as outlined that however the information is to be routed on the network and technique that square measure applied on the information packets.

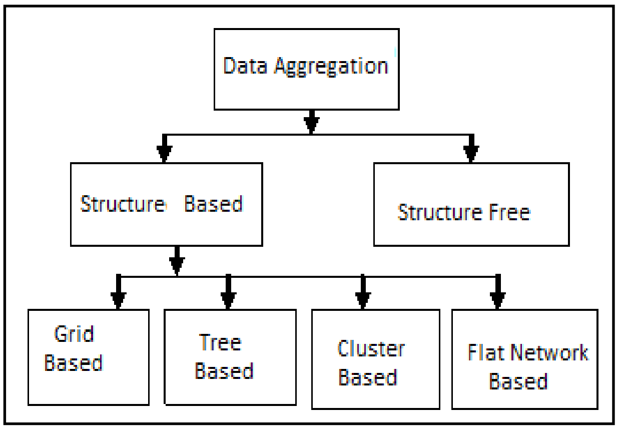

Fig.2. Data Aggregation

A. Data Aggregation Approaches are

1) **Centralized Approach**: During this approach just one detector node play a job of individual node and every one different detector nodes are unit connected to individual node. All different detector nodes sense the information and transmit to the individual node that is named as Centralized node.

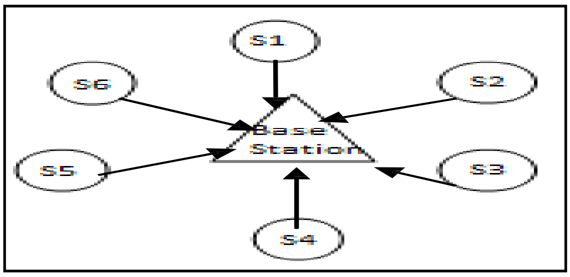

Fig3. Centralized approach for data aggregation in WSN

2) **Decentralized Approach**: During this approach all detector nodes performs individual perform to the perceived knowledge .In this approach there’s no single centralized individual node however all nodes have same priority to combination the perceived knowledge.

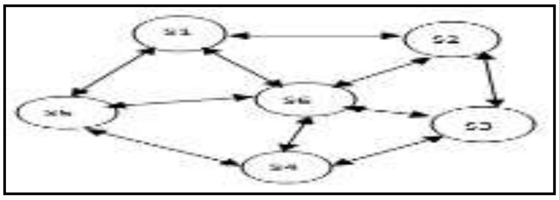

Fig4. Decentralize approach for data aggregation in WSN

3) **Network Aggregation Approach**: This approach aggregates multiple information into single information. it's necessary for rising the network time period and reduces the dimensions of transmitted information on the network.

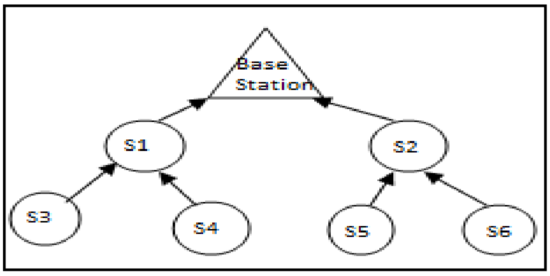

Fig5. Network aggregation approach in WSN

B. Data Aggregation perform in WSN:

For aggregation of perceived information varied aggregation perform is required and associated with device network application such as: scoop (Maximum), Min (Minimum), Avg (Average), Count, Sum, Median [4] etc.

C. Performance Metrics of Data aggregation:

There are several performance measures [4] are Energy efficiency, Network life time, Data Accuracy, Latency and Communication Overhead.

III. SECURITY NEEDS IN DATA AGGREGATION

Data Aggregation in wireless sensor network is a very important technique additionally as security to collective knowledge is a very important issue. In some necessary application like military police work and varied life important application knowledge transmission, knowledge aggregation, and knowledge reception ought to be in a very secured and energy economical approach. thus to attain this several facts ought to be thought of such as: Confidentiality of knowledge, Integrity of knowledge, Freshness of knowledge, supply Authentication, and Secure Node localization [4]. The needs are,

1. Confidentiality of Data , 2. Integrity of Data 3. Freshness of knowledge, 4. Secure Node localization, 5. Supply Authentication ,

In Abstract Diffusion for strong Aggregation in device Networks [5], this paper designed associate aggregation framework referred to as abstract diffusion. this is often in network aggregation theme and it avoids double enumeration by victimization “order-and duplicate-insensitive (ODI) synopses” that summarize intermediate result. each ODI abstract and abstract diffusion has the property of making elusive acknowledgement of packet delivery.

In A Secure Hop-by Hop information Aggregation Protocol (SDAP) [9], this protocol relies on “divide and conquer and commit and attest” principles. 1st to divide the device nodes during a tree topology of comparable sizes it used a completely unique probabilistic grouping technique. For security reason base station identifies the dishonest teams that square measure supported the set of cluster aggregates. This protocol is applicable to multiple aggregation perform.

In A Secure information Aggregation and verification Protocol (SDAV) [6], this paper designed 2 sub-protocols. 1st protocol used verifiable secret sharing of cluster keys in device network by victimization Elliptic Curve Cryptography (ECC). Second, designed Secure information Aggregation and Verification Protocol. during this protocol base station ne'er accepts false mixture information and by victimization Merkle Hash Trees, it checks integrity of knowledge.

In Secure and economical protocol for information Aggregation (SEDAN) [11], this paper developed 2 hops verification mechanism for information integrity. This theme doesn't need base station to verify and find mistakes in collective results, and every node will verify integrity of knowledge of 2 hops away neighbours and aggregation of immediate neighbours. This theme is helpful to avoid useless transmission of counterfeit information and saves energy of device nodes.

Secure End-to-End information Aggregation in Wireless device Networks [7] this paper represents a protocol for secure information aggregation, referred to as secure end-to-end information aggregation, it provides finish-to end information privacy of the collective information, the information is encrypted at device nodes and decrypted by the bottom station .This protocol uses additive holomorphic secret writing technique for secret writing of the information.

Secure and economical information Aggregation for Wireless device Networks [8] bestowed the Leaf Node illustration theme (LNR) to unravel ID downside in key stream-based secret writing for WSN with static tree design, during this theme leaf's node id will represent alternative node's id in its route to the bottom station. The Delayed Hop-by-hop Authentication theme (DHA) guarantee the information integrity for WSN with dynamic cluster primarily based design and it uses individual key for encoding.

It uses mack for authentication of knowledge and integrity of knowledge. For providing confidentiality to information, secret writing approach is employed during this paper.

IV. CONCLUSION

Wireless Sensor Networks are very useful in various applications such as military surveillance, health, home, office monitoring and in many intelligent and smart systems. In Wireless Sensor Networks there are several issues to the security of the network and secure data aggregation is also a big issue. In addition, cryptographic techniques are computationally expensive, and inappropriate use of these techniques could lead to excessive computing power and energy consumption. The aim of this Paper is to investigate and research efficient and cost-effective measures to achieve security and preserve privacy in a WSN environment.

REFERENCES

[1] [1] Aashima Singla, Ratika Sachdeva "Review on Security Issues and Attacks in Wireless Sensor Networks", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 3, Issue 4, 2013.

[2] Vaibhav Pandey, AmarjeetKaur and Narottam Chand "A Review on Data Aggregation Techniques in Wireless Sensor Network", Journal of Electronic and Electrical Engineering Vol.1, Issue 2, 2010.

[3] N.Sugandhi, D.Manivannan "Analysis of Various Deterioration Factors of Data Aggregation in Wireless Sensor Networks", International Journal of Engineering and Technology, ISSN: 0975-4024 Vol. 5 No 1 Feb-Mar 2013.

[4] Mukesh Kumar Jha, T.P Sharma "Secure Data aggregation in Wireless Sensor Network: A Survey", International Journal of Engineering Science and Technology, ISSN: 0975-5462, Vol. 3 No.3, March-2011

[5] S.Nath, P.B.Gibbons, S.Seshan, and Z.R.Anderson "Abstract Diffusion for Robust Aggregation in Sensor Networks" in Proc. ACM conf. Embedded Network Sensor System Nov-2004

[6] A.Mahimkar, T.S.Rappaport "A Secure Data Aggregation and verification Protocol for Sensor networks", IEEE Communications Society Globecom 2004

[7] A.S.Poornima, B.B.Amberker "Secure End-to-End Data Aggregation in Wireless Sensor Networks", in IEEE international Conference, 2010

[8] X.Wang, J.Li, X.Peng, and B.Zou "Secure and Efficient Data Aggregation for Wireless sensor Networks", in IEEE International Conference, 2010

Selected Paper from International Conference on Computing (NECICC-2k15)