OPTIMIZATION OF WIRELESS SENSOR NETWORKS IN SECURED DATA AGGREGATION

Mrs. P.Padmaja[1], Dr.G.V.Marutheswar[2], K.Sai Niharika[3]

[1]Research Scholar, S.V.U.College of Engineering, Tirupati, Andhra Pradesh, (India)

[2]Professor, Dept of EEE, S.V.U.College of Engineering, Tirupati, Andhra Pradesh, (India)

[3] Student,Vignan Institute of and Science, Hyderabad (India)

ABSTRACT

The applications of wireless sensor networks has wide varieties in which the network contains significant number of nodes for a particular area,where all the nodes are not connected directly.The data exchange is supported by multihop communications. Routing protocols are mainly used to discover the routes and maintain the routes in the network.Any particular routing protocol depends on the capability of its nodes and on the required applications. Secured data transmission is possible by implementing IF Algoritham at the cluster head.This traces the hacking node.data from hacked node is neglected.This IF Algoritham is implemented in TEEN,LEACH and DSDV their comparison is given in X-graphs. Ability for nodes to effectively communicate even in the presence of active adversaries in the network is SECURITY.Due to hostile environments and unique properties of wireless sensor networks, it is a challenging task to protect sensitive information transmitted by wireless sensor net-works. In addition, wireless sensor networks have security problems that traditional networks do not face. Therefore, security is an important issue for wireless sensor.

Keywords: WSN; TEEN; LEACH; BS; IF ALGORITHAM

I. INTRODUCTION

A wireless sensor network (WSN) consists of sensor nodes capable of collecting information from the environment and communicating with each other via wireless transceivers. The collected data will be delivered to one or more sinks, generally via multi-hop communication. The sensor nodes are typically expected to operate with batteries and are often deployed to not-easily-accessible or hostile environment, sometimes in large quantities. It can be difficult or impossible to replace the batteries of the sensor nodes. On the other hand, the sink is typically rich in energy. Since the sensor energy is the most precious resource in the WSN, efficient utilization of the energy to prolong the network lifetime has been the focus of much of the research on the WSN. The communications in the WSN has the many-to-one property in that data from a large number of sensor nodes tend to be concentrated into a few sinks. Since multi-hop routing is generally needed for distant sensor nodes from the sinks to save energy, the nodes near a sink can be burdened with relaying a large amount of traffic from other nodes.

A wireless sensor network (WSN) consists of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. The more modern networks are bi-directional, also enabling control of sensor activity. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on.

Due to the low deployment cost requirement of wireless sensor networks,sensor nodes have simple hardware and severe resource constraints. Hence, it is a challenging task to provide efficient solutions to data gathering problem. Among these constraints, ‘‘battery power” is the most limiting factor in designing wireless sensor network protocols. Therefore, in order to reduce the power consumption of wireless sensor networks, several mechanisms are proposed such as radio scheduling, control packet elimination, topology control, and most importantly data aggregation. Data aggregation protocols aim to combine and summarize data packets of several sensor nodes so that amount of data transmission is reduced. An example data aggregation scheme is presented in Fig. 1 where a group of sensor nodes collect information from a target region. When the base station queries the network, instead of sending each sensor node’s data to base station, one of the sensor nodes, called data aggregator, collects the information from its neighboring nodes, aggregates them (e.g., computes the average), and sends the aggregated data to the base station.

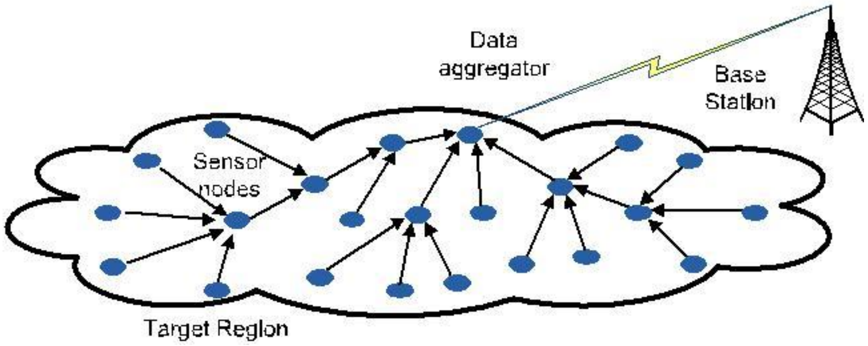

Fig. 1. Data Aggregation in a Wireless Sensor Network

Node deployment are of two types they are Manual deployment in which Sensors are manually deployed and Data is routed through predetermined path.In Random deployment Optimal clustering is necessary to allow connectivity & energy-efficiency and Multi-hop routing.

1.1 Algorithm Paradigms for Wireless Sensor Networks

A wireless sensor network supports the execution of following algorithms. They are Centralized Algorithms: These are executed by that node which has the knowledge of the whole network. These algorithms are rare as it is cost effective in order to provide whole information to single node.

- Distributed Algorithms: The communication is done by message-passing.
- Local based Algorithms: The nodes use restricted data collected from a close area. The algorithm is executed in one node by using that node
- MCFA (Minimum Cost Forwarding Algorithm): Assume the direction of routing is always known, i.e., toward the fixed base station (BS), No need for a node to have a unique ID or routing table,Each node maintains the least cost estimate from itself to BS,Broadcast a message to neighbors,A neighbor checks if it’s on the least cost path btwn the source and BS,If so, it re-broadcasts the message to its neighbors Repeat until BS is reached .In this Each node has to know the least cost path estimate to BS

- BS broadcasts a message with cost set to 0

Every node initially sets its cost to BS to ∞

When a node receives the msg from BS, it checks if the estimate in the packet + 1 < the node’s currentestimate to base station.

II. ROUTING PROTOCOLS WIRELESS SENSOR NETWORKS

2.1 Leach(Low Energy Adaptive Clustering Hierarchy)

In LEACH the the performance is based on the cluster head is periodically transferred between the nodes in the network in order to distribute the energy consumption. The performance of LEACH is based on rounds. In each round a cluster head is elected . The number of nodes that have not been cluster heads and the percentage of cluster heads are used For this election. Once the cluster head is defined in the setup phase, it forms a TDMA schedule for the transmissions in its cluster. Base on this scheduling allows nodes to switch off their interfaces when they are not going to be employed. The router acts as a cluster head to the sink and it is also responsible for the data aggregation. As the cluster head performs the job to controls the sensors located in a close area, the data aggregation performed by this leader permits to remove redundancy. Cluster-based protocol,Each node randomly decides to become a cluster heads (CH),CH chooses the code to be used in its cluster,CDMA between clusters.CH broadcasts Adv; Each node decides to which cluster it belongs based on the received signal strength of Advantes of CH creates a xmission schedule for TDMA in the cluster,Nodes can sleep when its not their turn to transmitmit,.CH compresses data received from the nodes in the cluster and sends the aggregated data to BS and CH is rotated randomly Advantages are Distributed, no global knowledge required and Energy saving due to aggregation by CHs.Disadvantages are LEACH assumes all nodes can transmit with enough power to reach BS if necessary (e.g., elected as CHs) and Each node should support both TDMA & CDMA.Extension of LEACH.High level negotiation, similar to SPIN and Only data providing new info is transmitted to BS

2.2 TEEN (Threshold Sensitive Energy Efficient Network Protocol)

Teen is the other hierarchical protocol that responds immediately when parameters are changed. The cluster head in this protocol has hard threshold and soft threshold values. When the parameter first reaches the hard threshold value, the node sends the data through transmitter. The data is then transmitted to the current cluster period. The main drawback is that when thresholds are not reached, nodes never communicate.Reactive, event-driven protocol for time-critical applications a node senses the environment continuously, but turns radio on and xmit only if the sensor value changes drastically.No periodic transmission.it Don’t wait until the next period to xmit critical data.Save energy if data is not critical.

Reactive, event-driven protocol for time-critical applications.A node senses the environment continuously, but turns radio on and xmit only if the sensor value changes drastically .No periodic transmission..Don’t wait until the next period to xmit critical data.Save energy if data is not critical.

CH sends its members a hard & a soft threshold.These are two types.Hard threshold meansA member only sends data to CH only if data values are in the range of interest.Soft threshold means a member only sends data if its value changes by at least the soft threshold.Every node in a cluster takes turns to become the CH for a time interval called cluster period.Hierarchical clustering are shown in fig.2.

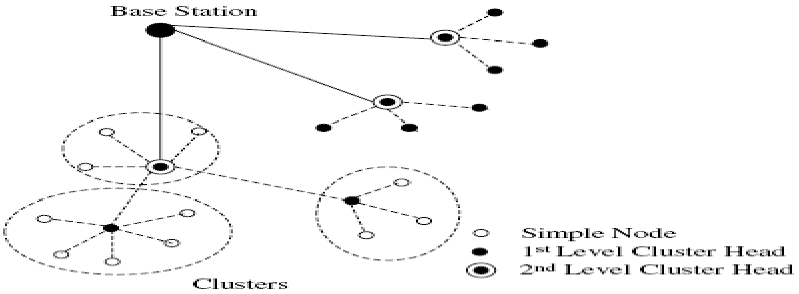

Fig.2. TEEN and APTEEN Routing Protocols.

It is good for time-critical applications as it has characterstics of energy saving,less energy than proactive approaches,soft threshold can be adapted,hard threshold could also be adapted depending on applications.Inappropriate for periodic monitoring, e.g., habitat monitoring.Ambiguity between packet loss and unimportant data (indicating no drastic change)

2.3 APTEEN (Adaptive Threshold sensitive Energy Efficient Network protocol)

Extends TEEN to support both periodic sensing & reacting to time critical events.Unlike TEEN, a node must sample & transmit a data if it has not sent data for a time period equal to CT (count time) specified by CH.Compared to LEACH, TEEN & APTEEN consumes less energy (TEEN consumes the least).Network lifetime is more in TEEN compare toAPTEEN and LEACH.Drawbacks of TEEN & APTEEN are Overhead and complexity of forming clusters in multiple levels and implementing threshold-based functions

III. SIMULATORS FOR WIRELESS SENSOR NETWORKS

Sensor networks are composed of large numbers of tiny sensing and computing devices. Each of these devices, called motes, has very limited communication, computational and energy resources. Often embedded in uncontrolled physical environments, these networks require distributed algorithms for efficient data processing, while individual motes require highly concurrent and reactive behavior for efficient operation. Sensor networks face many problem s that do not arise in other types of networks Power constraints, limited hardware, decreased reliability, and a typically higher density and number of nodes than those found in conventional networks are few of the problems that have to be considered when developing protocols for use in sensor networks.

NS-2 is a discrete event simulator target ed at networking research. NS-2 began as a variant of the REAL network simulator in 1989 and has evolved substantially over the past few years. NS-2 has a modular approach and hence is effectively extensible [10]. The environment: It provides substantial support for simulation of TCP, routing, and multicast protocols over wired and wireless (local and satellite) networks. Support for wireless networks was added later to simulate wireless LAN protocols, mobile ad-hoc net works and wireless sensor networks. The simulator focuses on following the ISO/OSI mode Simulation language: Simulations are based on a combination of C++ and OTcl.The Key features of NS- 2's extensibility is perhaps what has made it so popular for sensor networks. It has an object-oriented design which allows for straightforward creation and use of new protocols. The key features for WSNs include sensor channels, battery models, lightweight protocol stacks, hybrid simulation support, and scenario generation tools. It provides a visualization tool called NAM (Network AniMator). Due to its popularity and ease ofprotocol development, there are a high number of different protocols that are publicly available.

IV. COLLISION ATTACK IN WIRELESS SENSOR NETWORK

Most of the IF algorithms occupy simple assumptions about the initial values of weights for sensors. In case of our opponent model, an attacker is able to misinform the aggregation system from side to side cautious range of report data standards. Assume that ten sensors report the values of temperature which are aggregated using the IF algorithm planned in with the reciprocal discriminated function.

In scenario 1, all sensors are reliable and the result of the IF algorithm is close to the actual value.

In scenario 2, an adversary compromises two sensor nodes, and alters the readings of these values such that the simple average of all sensor readings is skewed towards a lesser value. As these two sensor nodes report a lower value, IF algorithm penalizes them and assigns to them lower weights, because their values are far from the values of other sensors. In other words, the algorithm is robust against false data injection in this scenario because the compromised nodes individually falsify the readings without any knowledge about the aggregation algorithm. The algorithm assigns very low weights to these two sensor nodes and consequently their contributions decrease.

In scenario 3, an adversary employs three compromised nodes in order to launch a collusion attack. It listens to the reports of sensors in the network and instructs the two compromised sensor nodes to report values far from the true value of the measured quantity. It then computes the skewed value of the simple average of all sensor readings and commands the third compromised sensor to report such skewed average as its readings.

V. IF ALGORITHM

✚ Cluster Formation

✚ Cluster Head(CH) Selection

• Cluster Head selects by the all the sensor nodes

o All the nodes share their energy level to all the neighbors

• All nodes check their energy into received energy level

• CH will select if the node which one get high energy message

o If I have high energy

 Yes, intimate all the nodes and share I am CH

 No, waiting for the CH request

✚ Cluster Members (CM) send the data to CH.

✚ Now cluster head can collect all data from each cluster member and pack all data into single pack

✚ Aggregated data can send to another CH via data aggregation technique

✚ CH can validate the cluster for every iterative round

o Every node can calculate average of neighbor nodes

o If difference is more high or less than threshold valve, it will be marked as hacker

o i.e.,$N2 - N1, N1 - N0 > Th_{max}$

 If it yes N1 will be marked has hacker

✚ Hacker node will be terminated from the cluster network.

Without false data injection data will be forwarded to Base station.

VI. CONCLUSION

The combination of smart, light-weight sensors familiarized wireless sensor network. The constrained abilities of the devices should be taken into account for the development of applications for these networks. Concerning the routing protocols, the minimizes energy resources, the scalability and the resilience arise as the main limitations in wireless sensor networks. This paper presents a survey on how routing protocols are adapted to these characteristics.

The following figures shown gives the comparison of all routing protocols for optimizing wireless sensor networks the complete analysis of routing protocols is require.

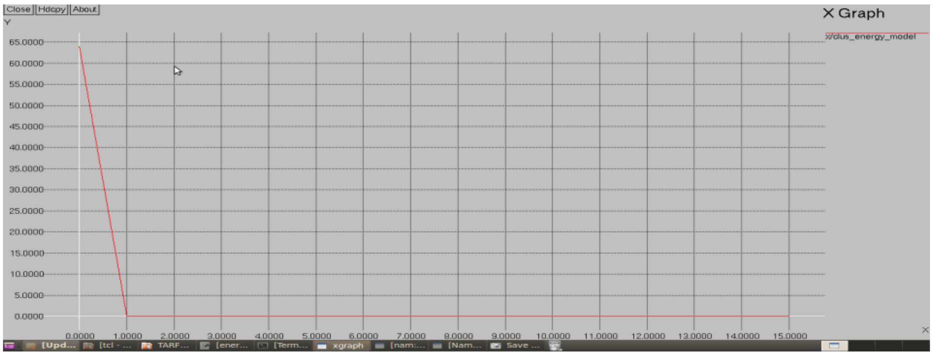

Fig 3. DSDV-XGRAPH

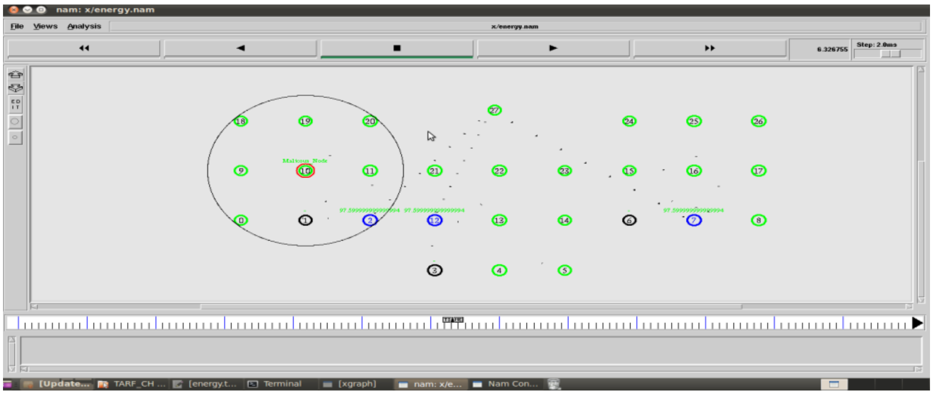

Fig 4.DSDV-NAM

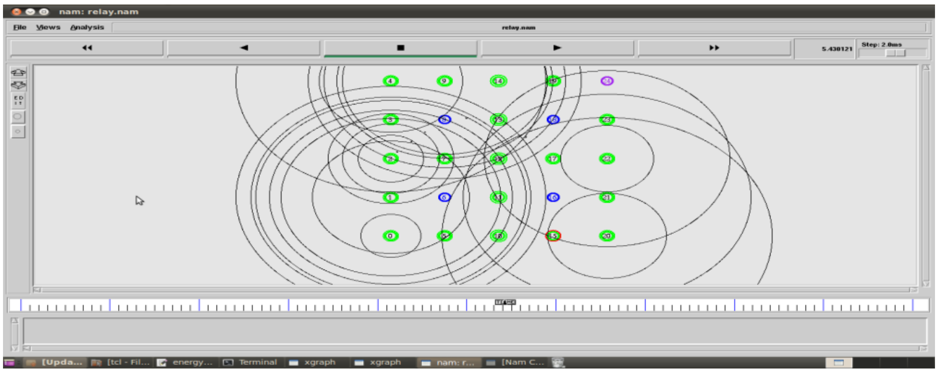

Fig 5.LEACH-NAM

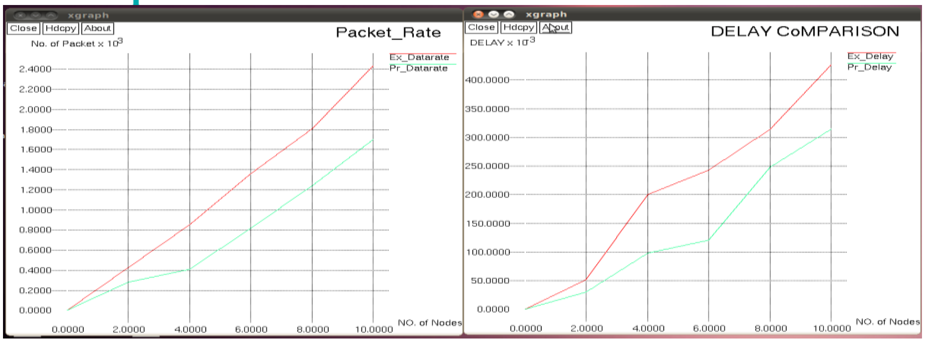

Fig.6.COMPARISON OF LEACH AND TEEN

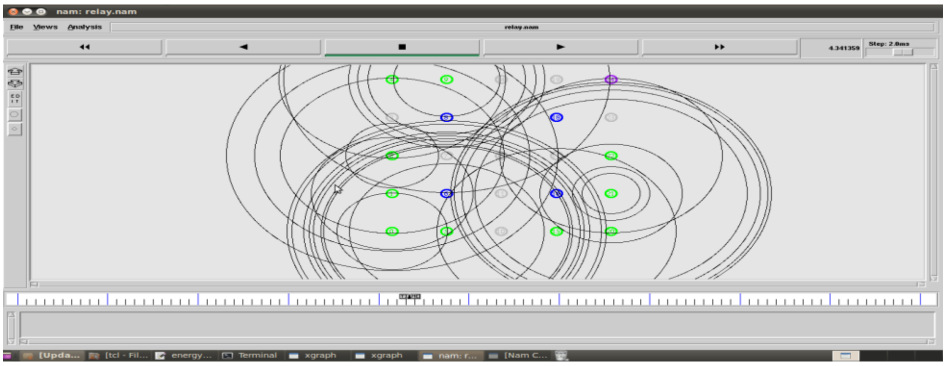

Fig.7.TEEN-NAM

REFERENCES

[1]. S. Ganeriwal, L. K. Balzano, and M. B. Srivastava,“Reputationbased framework for high integrity sensor networks,” ACM Trans. Sen. Netw., vol. 4, no. 3, pp.15:1–15:37, Jun. 2008.

[2]. Y. Yang, X. Wang, S. Zhu, and G. Cao, “SDAP: a secure hop by hop data aggregation protocol for sensor networks,” in MobiHoc, 2006, pp. 356–367.

[3]. He, W., Liu, X., Nguyen, H. V., Nahrstedt, K., andAbdelzaher, T. 2011. “Privacy preserving data aggregation for information collection "ACM Transaction Sensor Network. Article 6 (August 2011.DOI = 10.1145/1993042.199)3048.

[4]. H.-S. Lim, Y.-S. Moon, and E. Bertino, “Provenance-based trustworthiness assessment in sensor networks,” inProceedings of the Seventh International Workshop on Data Management for Sensor Networks, ser. DMSN ‟10, 2010, pp. 2–7.

[5]. S. Roy, M. Conti, S. Setia, , and S. Jajodia, “Secure data aggregation in wireless sensor networks,”Information Forensics and Security, IEEE Transactions on, vol. 7, no. 3, pp. 1040–1052, 2012.