DATA AGGRIGATION IN WIRELESS SENSOR NETWORKS

P.Padmaja
Assistant Professor/Department of ECE
VITS, Hyderabad, India

Dr.G.V.Marutheswar
Professor,Department of EEE
S.V.U.College of Engineering, Tirupati

***Abstract*— Data aggregation in Wireless Sensor Network (WSN) is applied to reduce redundancy and energy consumption. In WSN, in-network data aggregation performs aggregation of data in every router while forwarding data. Employing energy inefficient nodes in data aggregation affects lifetime of sensor network. Hence aggregation process in WSN should be optimized in energy efficient manner.**

When sensors are located in hostile environment, it is vulnerable to compromising attacks by adversaries. Compromised sensors inject false data during data aggregation process which results in false decision making at the Base Station (BS). Simple average data aggregation process is suitable only in attacker free environment. It is necessary to introduce a data aggregation mechanism that filters out attackers contribution during data aggregation. Behavior of nodes need to be observed in every round of data aggregation, and it should be reflected in subsequent rounds to filter out the impact of attacker contribution at the final result.

If the aggregator is compromised, then it affects entire aggregation accuracy. Hence it is necessary to propose a aggregation protocol that is resilient against compromised sensor and compromised aggregator in energy efficient and secure manner.

Index terms - WSN,TEE,LEACH, BS, SPIN,SAR,GAF, GEAR

I. I.INTRODUCTION

Now a days Wireless Sensor Network is a technology using in most of the applications.it is implemented in remote sensing applications of having advantages of less cost,less power consumption and mulitifunctionality feature.Beacuse of these advantages wireless sensor networks are implemented in many applications to aggregate correct data from intellectual sensors deployed in different areas.

A sensor networks consists large number of sensors which senses,shares and processing the received data from other nodes.So that it is must to separate algoritham and protocol for a wireless sensor network to performing the application without any errors.sensor networks have feature of on board processor.nodes are responsible for transmitting partially computated and processed raw data.primary sensor network are data centric than address-centric.Instead of sending sensed data to a particular sensor address, sends to sensors present in a cluster.

A cluster, having more sensors gets same data and locally aggregate the data. To reduce the bandwidth utilitzation,a node with in the cluster witch aggrigates the data called aggrigator node used for analysis of local data to reduce the data redundancy.A network hierarchy and clustering of sensor nodes improves the feature such as efficient utilization of resource,power consumption.finally the main moto of sensor networks is to improve cost.flexibility,reliability and easy to troubleshoot.

II. ENERGY EFFICIENT SECURE DATA AGGREGATION (EESDA) PROTOCOL FOR WIRELESS SENSOR NETWORKSDATA AGGREGATION

A. DATA AGGREGATION

In wireless sensor networks, data aggregation is considered as one of the fundamental distributed data processing procedures for saving the energy and minimizing the medium access layer contention (Zhenzhen et al 2006). Data aggregation is presented as an important pattern for routing in the wireless sensor networks. The basic idea is to merge the data from various sources, reroute it with the elimination of the redundancy thereby reducing the number of transmissions and saving energy (Krishnamachari et al 2002). The inbuilt redundancy in the raw data gathered from various sensors can be prevented by the in-network data aggregation. In addition, such operations are also useful for extracting application specific information from raw data. To preserve the energy in the system for maintaining longer lifetime in the network, it is important for the network to maintain high incidence of the in-network data aggregation (Kai-Wei et al 2007).

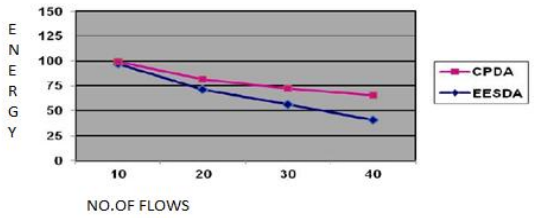

Figure 1. Flows Vs Overhead for CPDA and EESDA

B. SECURE DATA AGGREGATION

The issues related to the security in the data aggregation of WSN are Data Confidentiality witch means in particular, the basic security issue is the data confidentiality which safeguards the transmitted data that is sensitive from passive attacks like eavesdropping. The importance of the data confidentiality is in the hostile environment, where the wireless channel is more susceptible to eavesdropping. Even though cryptography has provided plenty of methods, the operation related to complicated encryption and decryption, like modular multiplication of large numbers in public key based cryptosystems, uses the sensor's power quickly.

Data Integrity prevents the alteration of the final aggregation value by the compromised source nodes or aggregator nodes. Sensor nodes can be easily compromised due to the lack of the expensive tampering-resistant hardware. Otherwise, used hardware may not be reliable at times. A compromised node is capable of modifying, forging and discarding the messages.

In general, for secure data aggregation in wireless sensor networks, two methods can be used. They are hop by hop encrypted data aggregation and end to end encrypted data aggregation.Hop-by-Hop encrypted data aggregation: In this technique, the encryption of the data is performed by the sensing nodes and decryption by the aggregator nodes. The aggregator nodes aggregate the data and again encrypt the aggregation result. At the end, the sink node on obtaining the final encrypted aggregation result decrypts it. End to End encrypted data aggregation: In this technique, the aggregator nodes in between have no decryption keys and can only perform aggregation on the encrypted data.

Energy efficient secured data aggregation protocol for wireless sensor networks have been proposed, which will alleviate the node misbehavior.This protocol involves Mechanism for energy efficient aggregator selection, Mechanism for efficient node selection for improving the network lifetime and reducing the delay,source node authentication by the sink.

III. PROPOSED SYSTEM

An optimized and secure data aggregation protocol is proposed that is resilient to false data injection attack launched by compromised sensor and aggregator. Proposed protocol performs secure data aggregation process along with trustworthiness estimation. Data aggregation process is optimized by performing aggregation in energy efficient manner through clustering. Sensor network is divided into clusters and each energy efficient Clusterhead (CH) aggregates data collected from its cluster members and transmits to BS. Secure data aggregation is carried out in two phases first at the aggregator to make it resilient against compromised sensors and second at BS to make it resilient against compromised aggregator.

In first module CH aggregates weighted average of reported value by each sensor in its cluster. Weight parameter is applied to reduce the impact of contribution of compromised sensor in the aggregation result. Trust value of the sensors is transformed into weight. Trust value of the previous round is applied as the weight of the current round. It is measured as the inverse proportion of deviation. Deviation is computed as the difference between aggregated value and the original value reported by the sensor. If the deviation is high then trust value is reduced. When the false data is injected by the compromised sensor, high deviation results in low trust value and weight that reduces the impact of attacker contribution in the final result.

In second module, BS executes verification mechanism to check the validity of the aggregation result reported by the CH. it selects subset of nodes from each cluster and queries original data from those nodes. The data from those sensors are propagated without aggregation. BS aggregates the received information from the sensors. Then it computes the deviation of aggregated result from the reported value by CH. The trust value for the CH is estimated from the computed deviation. If the CH is compromised its deviation becomes high that results in reduced trust value. Hence the contribution of the compromised CH is reduced at the BS.

Proposed protocol is optimized through cluster based data aggregation process and security is enhanced by making the protocol resilient against compromised aggregator along with compromised sensor. Trustworthiness measurement in the proposed work, assist in the secure data aggregation process as well as other network processes such as trust based routing, trust based cluster head selection and so on.

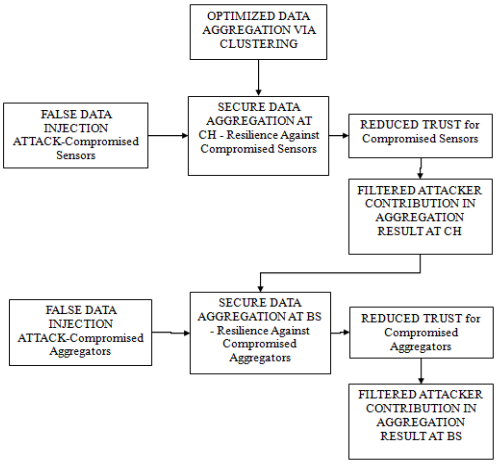

Figure 1. Overall implementation method

IV. ATTACKS ON WIRELESS SENSOR NETWORK

Attacks on WSN are generally classified as physical attacks, security attacks and routing attacks which are explained below in detail.

Physical attacks pose a great threat to WSN, because of their unattended nature and resource limitations. Roosta et al (2006) have divided physical attacks into two types as invasive attacks and non-invasive attacks.

Invasive attacks consist of probing techniques that require access to the chip level components of the device, where the embedded device is not opened and physically tampered. An

invasive attack is possible through the physical capture of a sensor node. There is no solution available to ensure the resistance of the sensor nodes to physical tampering. The microcontroller of the sensor nodes lacks any kind of hardware-based memory protection. In embedded systems, crypto-processors or physically secure processors have been used extensively to provide some level of resistance to physical tampering. Even though attacks on crypto-processors are known to occur, they still provide a first line of defense against physical tampering. Therefore, optimizing crypto-processors to fit the low-cost, low-energy requirements of sensor networks can play a significant part in raising the level of security achieved.

Non-invasive attacks, such as side-channel attacks, are also possible in sensor networks. For example, a recent study by Okeya and Iwata (2005) has shown that side-channel attacks on MAC can be launched using simple power analysis as well as differential power analysis. Their results suggest that several key bits can be extracted through the power analysis attack.

The fundamental security attacks on the actual sensor network as identified by Undercoffer et al (2002) are as follows:

i. Passive Information Gathering: An adversary with powerful resources can collect information from the sensor networks if it is not encrypted.
ii. Node Subversion: Capture of a node may reveal its information including disclosure of cryptographic keys and thus compromise the whole sensor network.
iii. False Node: A false node involves the addition of a node by an adversary to inject malicious data, whereby the false node is computationally robust enough to lure other nodes to send data to it.
iv. Node Malfunction: A malfunctioning node will generate inaccurate data which could jeopardize the integrity of sensor network especially if it is a data aggregating node such as a cluster leader.
v. Sinkhole attacks: Attracting traffic to a specific node, e.g. to prepare selective forwarding
vi. Sybil attacks: A single node presents multiple identities, allows reducing the effectiveness of fault tolerant schemes such as distributed storage and multi-paths etc.,
vii. HELLO floods: An attacker sends or replays HELLO packets to the routing protocol with more energy
viii. Node Outage: Node outage is when a node stops functioning.

In the case where a cluster leader stops functioning, the sensor network protocols should be robust enough to mitigate the effects of node outages by providing an alternate route.

- Message Corruption: Any modification of the content of a message by an attacker compromises its integrity.
- Traffic Analysis: Even when the messages transferred are encrypted, it still leaves a high possibility analysis of the communication patterns and sensor activities can potentially reveal enough information to enable an adversary to cause malicious harm to the sensor network.

V. Performance Evaluation

Proposed protocol is evaluated and compared with existing approach "Secure Data Aggregation in Wireless Sensor Networks: Filtering out the Attacker's Impact" for the following parameters using the ns-2 simulation.

Data Aggregation Deviation

It refers to the percentage of the aggregation error. It is calculated as the ratio of deviation to the true value sensed by the sensors.

Network lifetime

It refers to the time till half of the nodes in network becomes dead.

Overhead

It refers to the total number of control packets involved for the secure data aggregation process.

Attacker Impact Reduction Ratio

It refers to the ratio between the number of identified compromised sensors and the total number of compromised sensors resided in the network

Energy Consumption

It refers to the total amount of energy required for the data aggregation process.

VI. RESULTS

Data aggregation implemented in different routing protocols and compared their performances with the number of nodes with delay and packet rate.

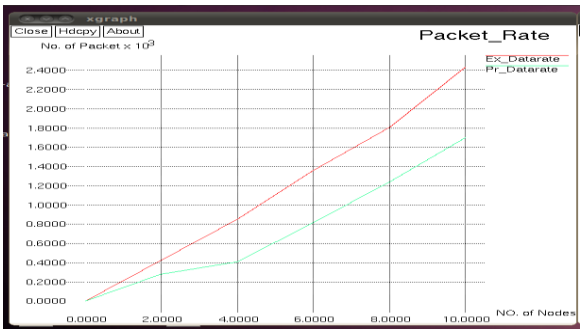

Figure 1. Xgraph generated for packetrate in LEACH protocol

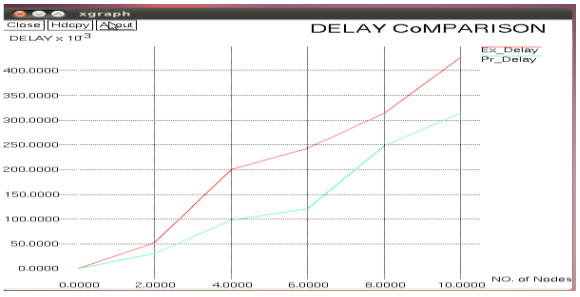

Figure 2. Xgraph generated delay comparison in LEACH

In leach protocol based on energy level of the node forms cluster head and aggregated data at cluster head and coresponding aggregated data at the base stations.

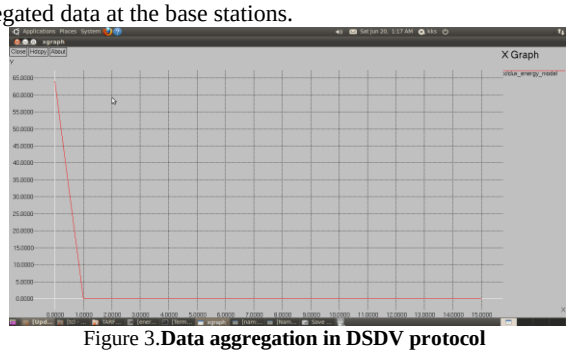

Figure 3.**Data aggregation in DSDV protocol**

The graph below shows comparison about data rate between LEACH, TEEN and HEF protocol. Data Aggregation mechanism will reduce the workload of CH. Here HEF protocol shows the higher throughput rate compared to other protocols.

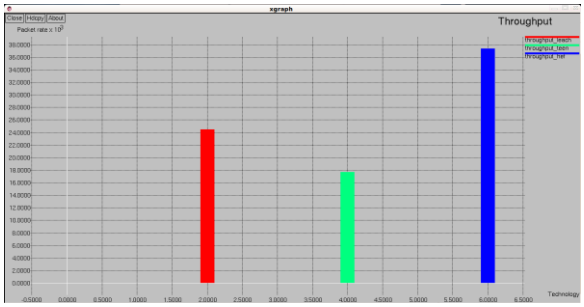

Figure 4. Throughput comparison of LEACH, TEEN and HEF protocols

The graph below shows comparison about DELAY between LEACH, TEEN and HEF protocol.From the below graph our proposed system proves less delay comparing to previous one.

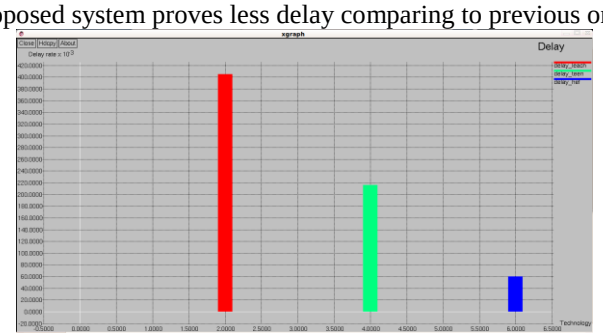

Figure 5. Delay comparison of LEACH, TEEN and HEF protocols

References

[1] Adrian Perrig, Robert Szewczyk, J. D. Tygar, Victor Wen and David E. Culler "SPINS: Security Protocols for Sensor Networks", Journal of Wireless Networks, Vol. 8, No. 5, pp. 521-534, 2002.

[2] Ahmed, A. A., Shi, H. and Shang, Y. "A Survey on Network Protocols for Wireless Sensor Networks", Proceedings of the International Conference on Information Technology Research and Education (ITRE), pp. 301-305, August 2003.

[3] Akkaya, K. and Younis, M. "A Survey on Routing Protocols for Wireless Sensor Networks", Journal of Ad-hoc Network, Vol. 3, No. 3, pp. 325-349, May 2005.

[4] Al-Karaki, J. N. and Kamal, A. E. "Routing Techniques in Wireless Sensor Networks: A Survey", IEEE Transaction on Wireless Communications, Vol. 11, No. 6, pp. 6-28, December 2004.

[5] Al-Karaki, J. N., Ul-Mustafa, R. and Kamal, A. E. "Data Aggregation in Wireless Sensor Networks: Exact and Approximate Algorithms",Proceedings of the IEEE Workshop on High Performance Switching and Routing (HPSR'04), Phoenix, pp. 241-245, April 2004.

[5] Amrita Ghosal and Jyoti Prakash Singh "Secure Data Aggregation Using Some Degree of Persistent Authentication in Sensor Networks" Proceedings of the Conference on Mobile and Pervasive Computing (CoMPC-2008), pp. 183-186, August 2008.

[6] Aravind Iyer, Sunil S. Kulkarni, Vivek Mhatre and Catherine P.Rosenberg "A Taxonomy-Based Approach to Design of Large-Scale Sensor Networks", proceedings of the Conference on Wireless Sensor Networks and Applications, Signals and Communication Technology,pp. 3-30, 2008.

[7] Banerjee, I., Chanak, P., Sikdar, B.K. and Rahaman, H. "EER: Energy Efficient Routing in Wireless Sensor Networks", Proceedings of the IEEE Students' Technology Symposium (TechSym) pp. 92-97, Jan 2011.

Authors Profile

P.PADMAJA received the B.Tech degree in electronics and communication engineering from the JNTU,KAKINADA, India, in 2004 M.Tech (with Distinction) Degree in DECS.Currently doing part-time ph.d on wireless sensor networks in sri venkateswara university college of engineering, s.v.university, tirupati,india.

G.Venkata Marutheswar received B.Tech Degree in Electrical Engineering, the M.Tech (with Distinction) Degree in Instrumentation and Control Engineering and Ph.D Degree in Electrical and Electronics Engineering from Sri Venkateswara University College of Engineering, S.V.University, Tirupati, Andhra Pradesh in 1985,1990 and 2009,respectively.Currently,he is Working as a Professor in the department of Electrical and Electronics Enginering, S.V.University College of Engineering,Tirupati, Andhra Pradesh, India.