International Journal of Emerging Technology and Innovative Engineering
Volume 2, Issue 3, March 2016 (ISSN: 2394 – 6598)

Date of Publication: 30.03.2016

SYNOPSIS DIFFUSION BASED ATTACKER RESILLIENT ALGORITHM FOR SEDURE DATA AGGREGATION IN WSN

M.ALISHABANU[1],G.INDHU[2],J.MADHUBALA[3],S.MEENUSRI[4],P.THIRUSELVAN[5]

malishabanu@gmail.com,indhumadhig95@gmail.com,manju.srimeenu23@gmail.com

1,2,3,4 STUDENT, 5.Asst Professor

1,2,3,4,5 PSR RENGASAMY COLLEGE OF ENGGINEERING FOR WOMEN

ABSTRACT

Data aggregation is any process in which data is gathered and expressed in a summary form, for purposes such as statistical analysis. In WSN, data aggregation reduces the amount of communication overhead and energy is very important in WSN. Here an attack-resilient computation algorithm is proposed that computes the true aggregate by filtering out the contributions of attacker nodes in the aggregation hierarchy. The simulations are done by using network simulator. This system provides the communication overhead consumption. So, secure data aggregation is very important in WSN. This system provides the communication overhead less compared to existing system. The experimental results show that this method provides high security, throughput and filtering the attacks immediately when it was detected.

KEYWORDS: WSN, Aggregation, Attacks

I. INTRODUCTION:

In the last decade WSN is increasingly used in several real-world applications[1]-[4],such as wild habitat monitoring,volcano and fire monitoring,urbansensing,and military purpose.In network data aggregation[2],[3] can reduce the amount of communication and hence the energy saving,especially in large WNSs.To address this problem,we can make use of multi-path routing method for forwarding sub aggregate [2].[5][6] have presented cleaver algorithm to solve this double counting problem.A robust scalable aggregation framework is called synopsis diffusion has been proposed for computing duplicate-sensitive aggregate this approach uses a ring topology.The network is a group of two or more computer systems linked together. There are many types of computer networks. They are Local Area Networks, Wide Area Networks and Campus Area

Networks, Metropolitan Area Networks, Home Area Networks. Local-area networks are the computers that are geographically close together that is, in the same building). Wide Area Networks are the computers that are farther apart and are connected by telephone lines or radio waves. Computer area network are the computers that are within the limited geographic area, such as a campus or military base. (MANs) are a data network designed for a country or city. Home area networks are a network that contained within a user home that connects person digital devices. In addition to these types, the following characteristics are used to categorize different types of networks. They are topology, protocol and architecture. The geometric arrangement of a computer system based on topology is as follows. Common topologies include a bus, star, and ring. The protocol defines a common set of rules and signal that computers on the network use to communicate. One of the most popular protocols for local area network is known as Ethernet. Another popular LAN protocol for PCs is the IBM token-ring network. Networks can be broadly classified as using either node to node or client/server architecture.Computers on a network are sometimes said to be *nodes*. Computers and devices that allocate resources for a network are called *servers*.

II. APPROACHES

SYNOPSIS DIFFUSION:

The synopsis diffusion which is based on a ring topology. During the query distribution phase, nodes form set of rings around the base station are based on

their distance in terms of hope from BS. By Ti we denote the ring consisting of the system.In the sequence aggregation period starting in the outermost ring, each node generates a local synopsis.

The synopsis generation function is denoted as by SG (v), where v is the sensor value relevant to the query. A node in the ring Ti will receive broadcasts from all of the nodes in the communication range in ring Ti+1. It will then combine to the own local synopsis with the synopses received from its children using a synopsis fusion function and then broadcast the updated synopsis. Thus, the fused synopses generates a level by level until they reach BS, which combines the received synopsis using Synopsis fusion Finally, base station uses the synopsis evaluation function to translate the final synopsis to the query. Now we describe the synopsis diffusion algorithms for Count and Sum. These algorithm is based on Flajolet and Martin probabilistic algorithm for together with the number of distinct element in a multi-set[15].each node X generate a local synopsis Q(x) which is a bit vector.

A node B^{X}_{1}, B^{X}_{2}, . . . , $B^{X}_{d}$from d child nodes X_1, X_2, . . ., X_d, correspondly, then X computes BX as follows:

$$B^{X}= Q^{X}||B^{X}_{1}||B^{X}_{2}|| \ldots ||B^{Xd}(1)$$

where|| denotes the bitwise OR operator. Note that BX represents the sub-aggregated of node X, including its descendant nodes. We note that BBS is same as the final synopsis B.

A) EXISTINGMETHOD:

The existing system uses duplicate insensitive algorithm is used to accurately compute aggregates. The possibility of node attacker introduces more challenges because most of the existing in-network aggregation algorithms have no provisions for security. A attacker node attempt to the aggregation process by launching several attacks, such as secretely listen to the conversion,jamming, message lossing, message fabrication, and so on.

B) PROPOSEDMETHOD:

Synopsis diffusion approach.The synopsis diffusion approach is secure against the attacks like eavesdropping, jamming, message dropping, message fabrication launched by compromised nodes. This approach uses attack-resilient computation algorithm to enable the BS to securely compute predicate count or sum even in the presence of such an attack. This algorithm securely computes the aggregates such as Count and Sum despite the falsified sub aggregate attack.

III. LITERATURE SURVEY

Marc Lee And Vincent W.S. Wong "An Energy-Aware Spanning Tree algorithm for data aggregation in Wireless sensor networks",
IEEE journals, 2010

Technique:

This paper proposes E-Span, which is an energy-aware spanning tree algorithm. E-Span is a circulated protocol and facilitates the sources within the event region to perform data aggregation. In E-span, the source node which has the highest outstanding energy is choosen as the root. Other source nodes are chooses their corresponding root node among their neighbors based on the outstanding energy and distance to the root.

Advantage:

It provides high packet delivery ratio\

Disadvantage: This method is prohibitively expensive in terms of communication overhead

IV. OVERVIEW OF PROJECT TITLE:

SD is an approach and it is used to collect various of data from a different places and send the information to the basestation and BS check wheather, the correct data is to be send or not.Attacker resilient is an algorithm,it is capable of regaining its original position after compression or other deformation.Data aggregation is a process in which information is gathered in a summary form. WNS wireless sensor network,which connect the two nodes without any physical device connect between them.WNS intermediate is air.

V. MODULES:

1.Node Formation

2.Local Synopsis Generation

3.Data Aggregation

4.Filtering The Attack

5.Performance Analysis

VI. MODULES EXPLANATION:

1.Node formation:

In this a number of nodes created . Label the base station and create the sub nodes.Set the parameters such as MAC type, Channel type, energy, node positions, traffic type.

2.Local synopsis generation:

In this each node generate and broadcast a local synopsis.The synopsis generation functions are represented by SG(v), where v is the sensor value relevant to the queries Anode in ring Ti will receive broadcasts from all of the nodes in the communication range in ring Ti+1. It will then combine it own local synopsis with the synopse received from and its children using a synopsis fusion function SF() and then broadcast the updated synopsis

3.Data aggregation:

It is any process where, which information is gathered and expressed in a summary form.The collected datas are send to the base station. The common aggregation purpose is to get more information about particular groups based on specific variables such as age, profession and income. The information about such groups can then be used for belonging to one or more groups for which data has been collected.

4.Filtering the attack:

The filtering will filter out the attacker injected in the data.It filters the false data and send it to the base station.

5.Performance Analysis:

We evaluate our data aggregation scheme using synopsis diffusion scheme for reducing the communication overhead through NS-2. We use a bounded region of 1700 x 1700 sqm, in which we place nodes using a uniform distribution. The number of nodes is 25. We assign the power levels of the nodes such that the transmissions range as 275 meters. In the simulation, the capacity of channel mobile hosts is set to the same value: 2.5 Mbps. We use the distributed coordination function (DCF) of IEEE 802.11 for WLANs as the MAC protocol. The simulation is Constant Bit Rate (CBR).

VII. SYSTEM ARCHITECTURE:

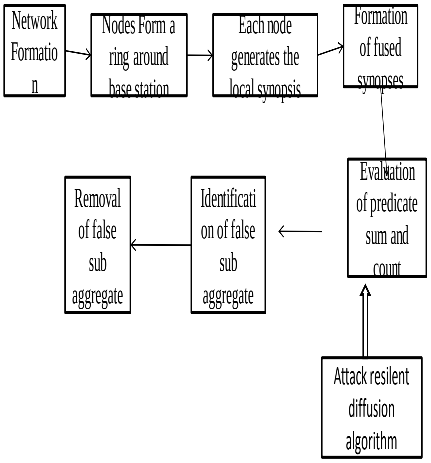
Network Formatio n
Nodes Form a ring around base station
Each node generates the local synopsis
Formation of fused synopses
Evaluation of predicate sum and count
Identificati on of false sub aggregate
Removal of false sub aggregate
Attack resilent diffusion algorithm

Fig 1: SYSTEM ARCHITECTURE

In figure 1 shows that, how the nodes where formed and generating a ring and the each node generates a local synopsis, each node generates a local synopsis diffusion and then forming a fused system, then it identifies the false data and removes the false sub aggregate data. this is done by using attacker resilient algorithm.

VIII. PERFORMANCE:

EXISTING SYSTEM DISADVANTAGE:

However, it provides a fault-tolerant solution but it does not address the problem of false aggregate values contributed by attacker node. It can launch several attacks, such as eavesdropping, jamming, message dropping, message fabrication. If a compromised node can inject an arbitrary amount of error, the final estimate of aggregate should be wrong. This attack is referred as falsified sub-aggregate attack

PROPOSED SYSTEM ADVANTAGE:

It provides security against attacks like eavesdropping, jamming. It reduces energy consumption. It is done by using ring topology, so it is more efficient compared to existing system

IX. CONCLUSION:

This scheme discusses the security issues of in network aggregation are to compute aggregates such as predicate Count and Sum. In particular, it shows the falsified sub-aggregate attack launched by a few attacker nodes can inject arbitrary amount of error in the base station estimate of the aggregate. The presented attack-resilient computation algorithm which would guarantized the successful computation of the aggregate

X. REFERENCE:

[1] M. Liu, N. Patwari, and A. Terzis, “Scanning the issue,” *Proc. IEEE,* vol. 98, no. 11, pp. 1804–1807, Apr. 2010.

[2] S. Madden, M. J. Franklin, J. Hellerstein, and W. Hong, “TAG: A tiny aggregation service for ad hoc sensor networks,” in *Proc. 5th USENIX Symp.Operating Syst. Des.Implement., 2002, pp. 1–3.*

[3] J. Zhao, R. Govindan, and D. Estrin, “Computing aggregates for

monitoring sensor networks,” in *Proc. 2nd Int. Workshop Sensor Netw. Protocols Appl., 2003, pp. 139–158.*

[4] (2006). *James Reserve Microclimate and Video Remote Sensing [Online]. Available:* *http://research.cens.ucla.edu/*projects/2006 /terrestrial/microclimate/defau%lt.htm

[5]J.Considine,F.Li,G.kollios,andJ.Byers,” Approximate aggregation techniques for sensor database,”inProc.IEEE 20thInt.Conf.Data Eng(ICDE),2004,pp.449_460.

[6]S.Nath,P.B.Gibbons,S.Seshan,andZ.Anderson,”Synopsis diffusion for robust aggregation in sensor networks,”in Proc. 2nd Int. Conf.EmmbeddedNetw.Sensor Syst.(SenSys),2004,pp.250-262

[7]M.Garofalakis,J.M.Hellerstein,andP.Maniatis,”Proofsketches:Verifiable in-network aggregation,” in Proc.23rdInt.Conf.Data Eng.(ICDE),2007,pp.996-1005.

[8]Y.Yang, X Wang, S. Zhu, and G.Cao,”SDAP: A secure hop-by-hop data aggregation protocol for sensor network,” in Proc. ACMMOBIHOC,2006,PP.356-367.

[9]H.Yu,”Secure and highly-available aggregation quries in large-scale sensor networks via set sampling,” in Proc.Int.Conf.Inf.process.sensor Netw.,2009,pp.1-12.

[10]S.Roy,M. Conti, S. Setia, and S. Jajodia, “Secure data aggregation in wireless sensor network”.