iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 8 **Issue:** X **Month of publication:** October 2020

DOI: https://doi.org/10.22214/ijraset.2020.32032

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue X Oct 2020- Available at www.ijraset.com

Data Aggregation and Multicast Authenticated Scheme for Wireless Sensor Networks

Dr. S. Saira Banu[1], Dr. E. Siva Senthil[2]
[1]*Associate Professor,* [2]*Head of the Department, Department of Physics, Karpagam Academy of Higher Education, Coimbatore*

Abstract: ***Wireless Sensor Networks consists of sensor nodes which moves randomly. It does not depend on any infrastructure like ad=hoc networks. Due to the development of information technology, data transmission plays a significant role in communication.***
Wireless Sensor networks are one such communication paradigm. Data aggregation as a typical operation in data gathering application can cause a lot of energy wastage since sensor nodes, when not receiving data may keep in the listen state during the data collection process. WSN consists of a large number of battery-powered wireless sensor nodesIn this research work routing is a major issue in ad hoc sensor network where the nodes consume more energy. Security is an important issue in Wireless Sensor Networks where the mobile sensor nodes are easily compromised by means of several attacks. The types of attacks are active attacks and passive attacks. These attacks are vulnerable to network devices and make network inevitable. This research work focus on development of secure multicast groups. The public key encryption and decryption is developed to protect node from attackers.
Keywords: Wireless Sensor Networks, Data Aggregation, Data Transmission, Encryption, Decryption , Authentication

I. INTRODUCTION

The current technological advancement has already come to terms with immense potential of Wireless Sensor Network, which consists of tiny sensor nodes scattered in a region communicating with each other over well defined protocols and transferring information of temperature, humidity etc between each other. Mobile sensor networks (MSN) have been widely used in many dynamic applications, search and rescue operations and disaster relief efforts etc.. Mobile nodes are communicated in a broadcast manner through radio signals.. Routing has been widely used in many applications such as corporate audio/video conference, collaborative communications and groupware systems etc. A single stream of data packets can be shared with many destinations and when packets are duplicated. Security protocols are required to add reliable authenticated features to the base routing protocols. Attackers are divided as active and passive. It may arise from inside or outside the network. Key management scheme is the basic block of secure routing protocols but it is not fit for ad hoc network where nodes can be varied with different network devices. It is required to ensure genuine members which hold authorized keys at any time. While deploying security features, overhead and energy consumption becomes a bigger task to manage. It should be reduced to achieve successful packet transmission. Data aggregation is the process of collecting and aggregating the useful data. Data coming from multiple sensor nodes are aggregated as if they are about the same attribute of the phenomenon when they reach the same routing node on the way back to the sink. All data collected and aggregated is stored at a storage location in database server.

II. RELATED WORK

Ravidra gupta et.al [1] explored security threats in wireless sensor network and made an extensive study to categorize available data gathering protocols and analyze possible security threats on them. Due to limitations of sensor devices, the networks exposed to various kinds of attacks and conventional defenses against these attacks are not suitable due to the resource constrained nature of these kinds of networks. Therefore, security in WSNs is a challenging task due to inheritance limitations of sensors and it becomes a good topic for researchers.
Wenjing Lou et.al [2] analysed that both theoretical analysis and simulation results that multipath routing provides many performance benefits, including the improved fault tolerance, security, and reliability, improved routing efficiency and reduced routing overhead, more balanced traffic load and energy consumption, reduced end-to-end latency and aggregated network bandwidth, etc. Significant research efforts have been made and are continuously being made in developing multipath routing protocols and multipath packet forwarding techniques in order to achieve the abovementioned performance gains effectively and efficiently.

Saira Banu, and R.Dhanasekaran [3] proposed a New Multipath Routing Approach (NMRA) for increasing the energy efficiency in WSNs. In WSNs, the best route is being determined by choosing efficient strategy to forward the data to the base station. Due to that, the node consumes more energy unnecessarily. In this method a New Multipath Routing Approach was developed which attains energy model, maintenance of optimal energy path, multipath construction phase to make a correct balance between network life time, energy consumption and throughput to the sensor nodes.

A literature review is presented, [4] based on packet-forwarding scheme to reduce the event-reporting delay and to prolong the lifetime of wireless sensor networks employing asynchronous sleep- wake scheduling. When the wake-up rates of the sensor nodes are given, it develop an efficient and distributed algorithm to minimize the expected event-reporting delay from all sensor nodes to the sink. Using a specific definition of the network lifetime, it study the lifetime-maximization problem to optimally control the sleep-wake scheduling policy and the any cast policy, in order to maximize the network lifetime subject to a upper limit on the expected end-to-end delay.

In [5] The Response time minimization algorithm is used to share the load to the available VM efficiently. It improves the response time and minimizes the delay time. Hence the load balancing is achieved. Several performance metrics such as availability, utilization, and responsiveness used to investigate the impact of different strategies on both provider and user point of views. This paper identifies that Response Time Minimization grid task scheduling algorithm outperforms the Round Robin and Equally spread algorithm in a heterogeneous distributed environment.

In[6] The McTMAC protocol that can efficiently handle the delay over multihop WMN and extended the time- slot assignment of the PETAR09 algorithm to multichannel time-slot allocation and enhanced the distance-1 channel assignment.

In [7], the author proposed and established a relationship between packet priority and node energy in the form of the „Priority-Energy Based Data Forwarding Algorithm", which decides on the best energy- efficient forwarding choice.

In the paper [8], secure on demand routing protocol was proposed to choose efficient and trusted path based on different objectives. Trust values of nodes or alternative uses in cognitive network were calculated to differentiate goof and malfunctioning nodes. The effective routes and trusted level of intermediate nodes were also considered in this scheme.

In [9], authors introduced Secure Best Forwarding Route Estimation to provide optimal routes based on the computation of trust value and hop count at one hop level. The overall performance was observed based on packet equivalence ratio. By managing this ratio, the network performance will get improved. Suspicious nodes were removed through alternative routes based on this forwarding route estimation with authentication.

In [10], authors proposed a new approach for calculating and balancing the energy and security. The reliable paths were estimated to reduce energy consumption and remove least residual energy of nodes. The dynamic behavior of nodes was captured using the concept of computational intelligent technique.

III.IMPLEMENTATION OF PROPOSED SCHEME

A. Method of Data Aggregation

The sensor nodes are correlated in terms of time and space, transmitting only the required and partially processed data. The required data should be secure and efficient than sending a large amount of raw data. The duplicated messages sent to the same node and neighboring nodes waste energy, if two nodes share the same observing region. The data aggregation aggregates data progressively as it is passed through a network.

The data packet size, the number of data transmissions and the number of sensor nodes involved in collecting data from WSN can be reduced by using In-network data aggregation.

The main approach of the data aggregation and in-network processing are to combine the data arriving from different sources at certain aggregation points. The aggregation points eliminate redundancies. Removing redundancies results in transmitting less number of bits, and hence reduces energy consumption and increases the sensor nodes lifetimes

Data aggregation reduces the amount of energy consumption. The data from sensor nodes are correlated depends on the terms of time, transmitting only the required and partially processed data is efficient than sending a large amount of unnecessary data. WSNs lifetime is enhanced by reducing unnecessary traffic.

Involving as many sensor nodes during data collections, utilize maximum resources of every sensor node by the sink nodes. As a result, the sensor nodes closer to the sink run out of energy sooner than other nodes and the network loses its service ability, regardless of a large amount of residual energy of the other sensor nodes.

B. Energy Efficient Data Aggregation in WSN

Energy efficiency in Wireless Sensor Networks are achieved by the method of data aggregation scheme which exploits sensing with arbitrary topology. It uses wavelets to a sparse basis that characterizes the minimum-energy compressed data aggregation problem. It is designed as a proper sparse basis based on diffusion wavelets to achieve high-fidelity recovery for data aggregated from deployed Wireless Sensor Networks. It develops the idea to allow for network partitions and to integrate temporal correlations along with the spatial ones, which can reduce energy consumption while maintaining the fidelity of data recovery.

C. Network and Attacker Model

The proposed network model, topology is established which consists of routers and nodes. The routers are created to form a multicast backbone which forwards the traffic to main gateways. Neighbour nodes are connected according to mesh based multicast network structure.

Location of mobile nodes is known to source and destination node. Geographical position of nodes is updated to source node. Nodes are randomly deployed and roaming as ad hoc fashion. Random waypoint mobility pattern is adopted in this proposed network model. The following assumptions are made in the attacker model.

1) Attacker can be able to capture all the traffic in the network region.
2) There may be some possibilities of attackers based on dropping of packets inside the network
3) Attacker may eavesdrop the network communication and can track the information, its packet size etc..

D. To Establish Multicast Routing

In this phase a multicast tree is constructed based on the geographical position of mobile nodes. The multicast group message is added with group ID and the redundant nodes for all multicast groups will be removed from the multicast tree. Parent nodes update their child node locations by sending Request_Join message. Routes are established from multiple source and multiple destination. If any node falls the category of high mobility, it will be isolated. In this scheme, mobility of nodes is kept small. During the construction of multicast tree, source node broadcasts Route_Join message to all neighbour nodes. The tree is formed until the target node or destination node joins.

In order to avoid link breakage, node location ID is installed in routing tables of all mobile nodes. In this phase, parent node finds its transmission power to forward the packets to destination node. Parent nodes periodically transmit the location aware message with maximum power that contains Parent ID and sender location information. There are three possible states of nodes. i.e. Active, Monitor and Idle mode. In active mode, nodes keep on sending request message. Once the request message is expired, state will be changed to monitor. In idle mode, node will not participate in route discovery and route maintenance process. Link connectivity is checked with intermediate nodes.

E. Key generation, Encryption and Decryption

1) Key Generation

Node should obtain a public key and its own private key.

a) *Step1:* Generate an integers as system parameters i.e. *q,m,s.*
b) *Step 2:* Each node U should follow the steps from 3 to 6.
c) *Step 3:* Select a $q \times m$ generator matrix *GM* for a binary linear code (*m,q*) to correct *e* errors.
d) *Step 4:* Choose a random $k \times k$ binary non singular matrix S.
e) *Step 5:* Find $q \times m$ matrix = SGML
f) *Step 6:* Finally U's public key is (*GM, e*) and private key is (*S,GM, L)*

2) Encryption

U encrypts the message *m* for V

a) *Step 1:* U find V's authenticated public key
b) *Step 2:* Message is presented as binary string with binary length *L.*
c) *Step 3:* Select a binary error vector value *x* of length *m.*
d) *Step 4:* Determine the binary vector $z = hGM + x$.
e) *Step 5:* Send the encrypted text *z* to V.

3) Decryption

a) Step 1: D decrypts the cipher text and do the following.

b) Step 2: Determine $z' = zL^{-1}$ where L^{-1} is the inverse of L.

c) Step 3: Generate code by decoding cipher text to plain text.

Table 1 Packet Format

Parent ID	Child ID	LI	Authentication	LR	CRC
2	2	4	2	2	2

IV. PERFORMANCE METRICS

The following metrics are used to evaluate the performance of proposed protocol.

1) End-to-End Delay: The end-to-end delay is averaged over all surviving data packets from source to destinations.

2) Packet Delivery Ratio: It is defined as the ratio of packet received with respect to the packet sent.

3) Throughput: It is defined as the number of packets received at a particular point of time.

4) Control Overhead: The control overhead is defined as the ratio of excessive number of control packets to the total number of received data packets.

5) Node Authentication Ratio: It assures the authentication of node from unauthorized uses. It is the ratio of authenticated nodes to the total number of nodes deployed in the network region.

V. PERFORMANCE EVALUATION

The proposed protocol is evaluated with network simulator tool (NS 2.34) version. This version is suitable for the simulation of all networks i.e. sensor networks, cognitive radio and Wimax applications. The simulation tool languages are C++ and Tool Command Language (TCL). Only 150 nodes are deployed in 1200 x 1200 sq.m network simulation area. Mobility model is Random walk model to simulate the packet with the size of 80 bytes. The simulation settings are tabulated below.

TABLE 2
Simulation and Settings parameters

No. of Nodes	150
Area Size	1200 x 1200 m^2
Mac	802.11
Radio Range	250 m
Simulation Time	100 sec
Traffic Source	Constant Bit Rate (CBR)
Packet Size	512 bytes
Mobility Model	Random Walk
Protocol	DSR

VI. RESULT AND DISCUSION

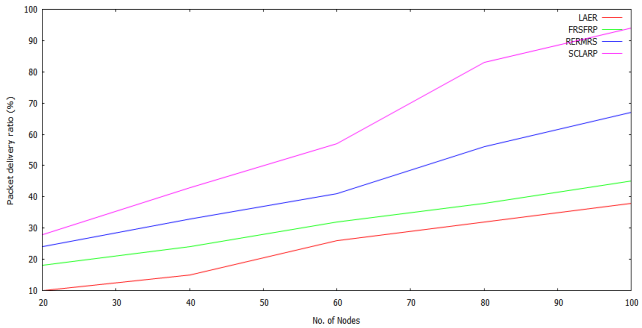


Fig. 1 Packet Delivery Ratio Vs Number of Nodes

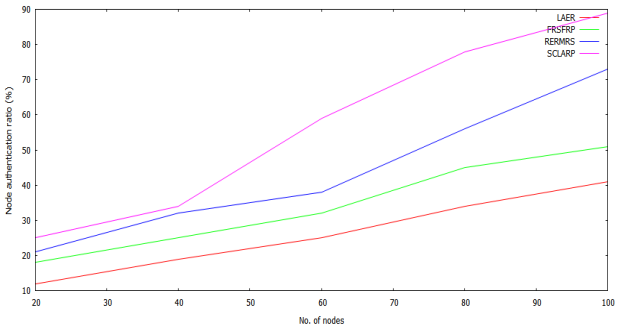


Fig. 2 Node Authentication ratio Vs No. of Nodes

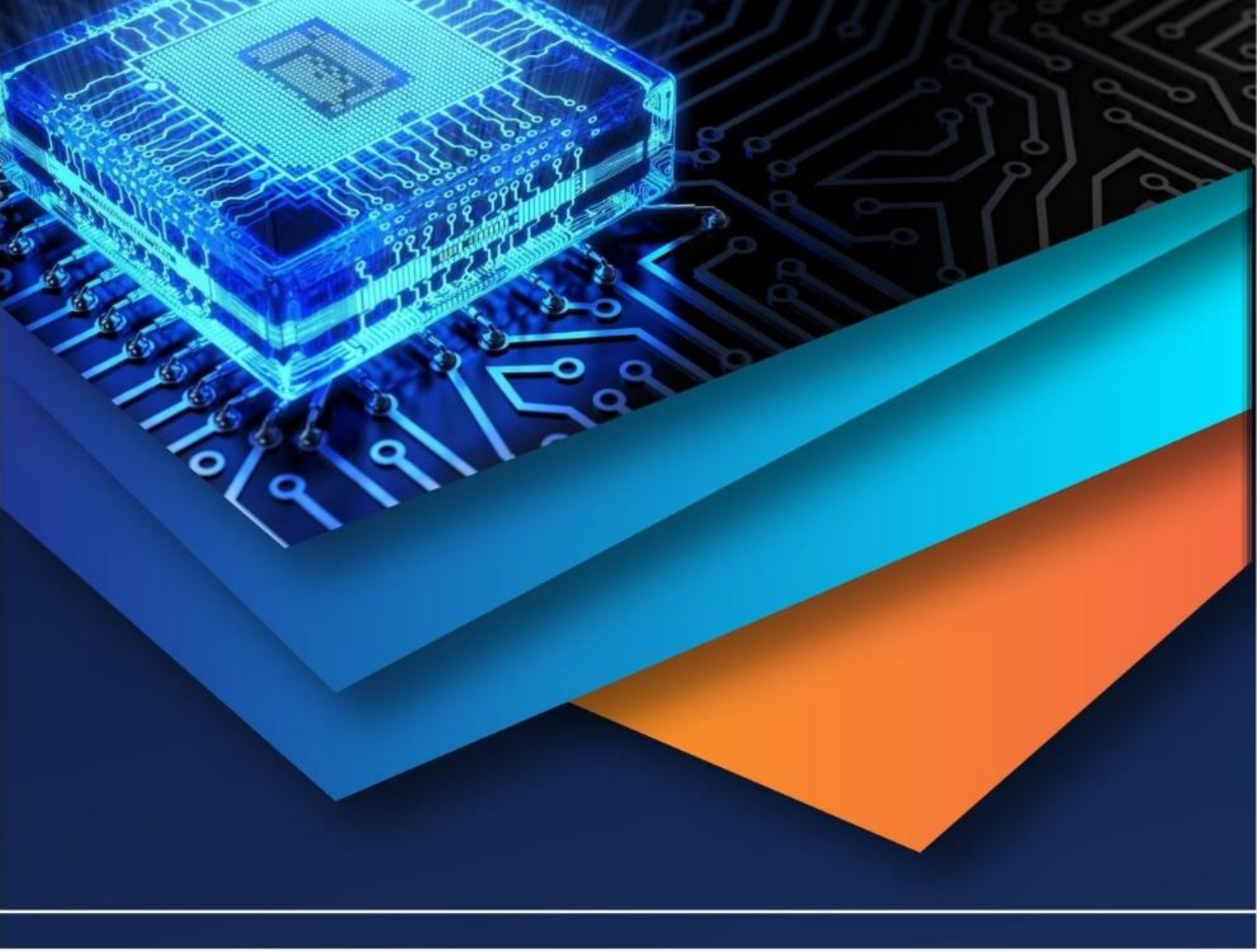
Fig. 1 shows the simulation of packet delivery ratio while varying number of nodes from 10 to 150 nodes. When the number of nodes is increasing, packet delivery ratio may get reduced. Due to frequent link failures, packet lost may occur. So the delivery ratio may be reduced. In the proposed protocol SCLARP, high packet delivery ratio (28-94)% is attained. Compared to the existing schemes, SCLAR outperforms better. Fig. 2 shows node authentication ratio Vs number of nodes. From the results, SCLARP achieves more authentication ratio (25-89)% than existing schemes. It is because of public key encryption and decryption.

VII. CONCLUSIONS

In this research work data aggregation and multicast authenticated scheme is developed foe the Wireless Sensor Networks Wireless Sensor Networks are prone to many security attacks which impede the deployment and data propagation of sensor. In the presence of node mobile period, nodes are compromised by attackers and it may damage the network connectivity. Multicasting supports security and authentication in ad hoc networks. A Multicast tree is established from the computation of location integrity and node authentication. Selection of reliable links was done in the construction phase of multicast tree. Only mesh based routing is established from parent node to child node and then destination node. If any link is making more packet loss or any node doing malfunctioning, it will be immediately identified using public key encryption and decryption technique.

REFERENCES

[1] Ravindra Gupta, Hema Dhadhal , “Secure Multipath routing in Wireless Sensor Networks”, International Journal of Electronics and Computer Science Engineering, Vol.1, No.2, 2012, pp.5859
[2] Wenjing Lou, Wei Liu and Yanchao Zhang, “Performance Optimization using Multipath Routing in Mobile Ad Hoc and Wireless Sensor Networks”, Combinatorial Optimization in Communication Networks, 2005, Kluwer Academic Publishers, pp.1-29
[3] Saira Banu and Dr. R.Dhanasekaran, “ A New Multipath Routing Approach for Energy Efficiency in Wireless Sensor Networks”, International Journal of Computer Applications (0975 – 8887), Volume 55, No.11, 2012, pp.24-30
[4] SunYuezhongyi, “ Reliable and Secure Routing Ad-Hoc Algorithm Based on Collaborative Monitor Nodes in VANETS”, International Journal of Security and Its Applications Vol. 9, No. 6 (2015), pp. 89-100.
[5] Jenish R.Gandhi and Rutvij H. Jhaveri, “ Packet Forwarding Misbehaviour Isolation using Fuzzy Trust-based Secure Routing in MANET”, International Journal of Computer Applications, Vol.122, No.3, 2015, pp.30-35.
[6] Sethulekshmi and Manoj Kumar, “Energy Efficient Secure Routing in Manets Based on Multipath Erasure Coding”, International Journal of Engineering and Computer Science, Vol.4, Issue 10, 2015, pp. 14717-14724.
[7] Harold Robinson and M. Rajaram, “Energy-Aware Multipath Routing Scheme Based on Particle Swarm Optimization in Mobile Ad Hoc Networks”, Scientific World Journal, 2015,pp.1-10.
[8] Sangita Pal and Srinivas Sethi, “ A Secure On-Demand Routing Protocol in Cognitive Radio Ad Hoc Network”, International Journal of Emerging Technologies in Computational and Applied Sciences, Vol.14, No.2, 2015, pp.103-109.
[9] Rutuja Shah, Sumathy Subramaniam and Dhinesh Babu Lekala Dasarathan, “Mitigating Malicious Attacks Using Trust Based Secure-BEFORE Routing Strategy in Mobile Ad Hoc Networks”, CIT. Journal of Computing and Information Technology, Vol. 24, No. 3, September 2016, pp.237–252.
[10] Kumuda, Usha and PallapaVenkatraman, “ An Approach for Energy based Secure Routing Protocol”, International Journal of Computer & Mathematical Sciences, Vol.4, No.12, 2015, pp.11-14.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY