ENERGY EFFICIENT SECURE PROVENANCE TRANSMISSION IN WSN

Shindhiyaa .L [1], Monisha .V [2], Reena .R [3], Kapilavani .R.K [4]

[1,2]*Department of Computer Science and Engineering, Prince Shri Venkateshwara Padmavathy Engineering College, Chennai, India.*

[3]*Assistant Professor, Department of Computer Science and Engineering, Prince Shri Venkateshwara Padmavathy Engineering College, Chennai, India.*

[4] *Assistant Professor, Department of Computer Science and Engineering, Prince Dr. K. Vasudevan College of Engineering and Technology, Chennai, India.*

ABSTRACT

Sensor networks are used in numerous application domains and providing security to Wireless Sensor Network (WSN) includes several challenges such as energy efficiency, assessing trustworthiness of the provenance management. To address these issues we propose an approach to efficiently transmit the provenance data by finding an optimized path. In this paper the provenance data size is reduced by lossless compression technique called LZ4. In addition to this, in order to provide security we use an encryption technique. Through simulation results, we show the energy efficiency of our proposed scheme.

Keyword:- *Provenance, LZ4 lossless compression, energy-efficient.*

1. INTRODUCTION

Wireless sensor network comprise of multiple nodes and it is applicable in several domains such as environmental monitoring , home security, medical monitoring, military operations, agriculture . Each sensor node gathers data from the physical environment and transmit the gathered data through the intermediate node to the Base Station which performs decision taking. Sensor node has some limitations such as limited energy supply, limited memory capacity, limited storage and computation and providing security to such network is crucial since it is an open communication.

Data provenance includes the transfer history of sensor nodes from the source to the sink. Provenance management is a difficult because of its size and trustworthiness of the data.

Challenges:

1. To reduce the provenance size without any loss of data.

2. To securely transmit the provenance data and sensor data efficiently with less energy consumption.

However, [1],[2] existing research work has mainly focused on reducing the provenance size which resulted in loss of data on reaching the base station. And it sometimes takes longest path to reach the destination.

In order to address these issues we propose a framework to find the optimized path by the hybrid energy efficient routing protocol [7]and transmit the provenance data which includes source address, destination address and next hop securely by public key cryptography technique. Since during encryption the size of data may be increased so we compress the data by lossless compression technique[3],[4],[5],[6].

2. SYSTEM MODEL

a)NETWORK MODEL

We consider the grid topology for large scale wireless sensor network as shown ion figure 1. The grid topology can configure the source and sink node dynamically.

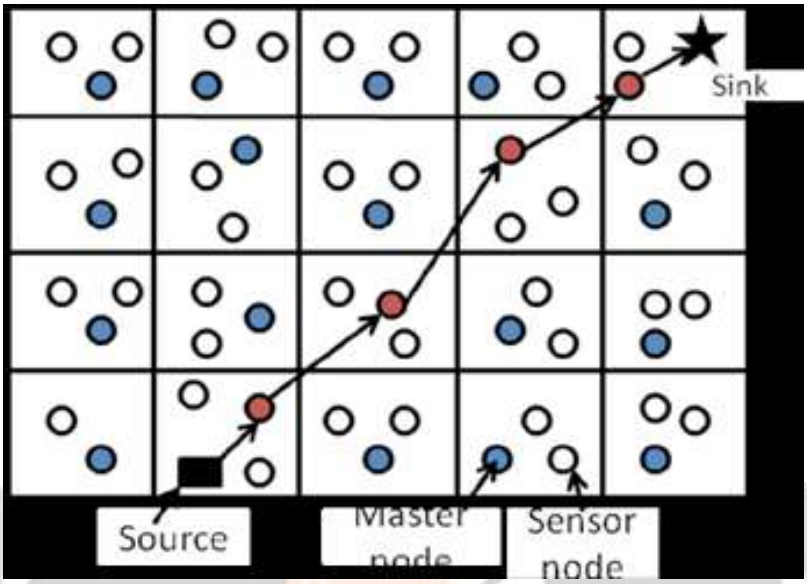

Figure1: Grid topology.

In grid topology, each grid contains few sensor nodes. Each grid contains a master head. A node with the highest energy will act as a master head. A sensor node (source node) transmits the sensed data to the master head after gathering the information from the physical environment. Since we are selecting the master head for each grid based on its energy, the lifetime of network is increased.

b)PROVENANCE MODEL

Our proposed provenance records at each nodes that are involved at each step of data processing during transmission. The provenance that are recorded in each nodes includes sequence number, source address, destination address, packet path.

3. PROPOSED SYSTEM

In our proposed system, we find the optimized path by using an energy efficient algorithm. For secure transmission, we use public key cryptography and lossless compression technique.

A)ROUTE OPTIMIZATION ALGORITHM

In route optimization technique, some assumptions made during this process.

i) Every node transmit sensed data to sink node so destination to all the node is same.
ii) Every node in the network is having initial energy different.
iii) Master head selection to be executed periodically. So node with highest energy is selected as master head. As a master head changes periodically since its energy changes rapidly.
For large scale wireless sensor communication, the energy consumption model is calculated as follows

$$\varepsilon(n) = t(n) \times a(n) \times e(n)$$

Where
t (n) is the number of transmitted bit,
a (n) is the average number of nodes for the communication,
e (n) is the energy consumption to transmit single bit.

Every node transmits data to the grid node (i.e. a(n) =1) so energy consumption for individual node ni is in time t,

$$\varepsilon \text{ (ni)} = \text{t (ni)} \times 1 \times \text{e (ni)} \times \text{ri} \times \text{t}$$

Where,
ri is sampling rate of node ni in samples per second,
t is time in seconds.

Master node is responsible for forwarding all data in grid, energy consumption of master head is

$$\varepsilon \text{ (mh)} = \text{n (mh)} \times \sum_{i=0}^{n} (\varepsilon\ (ni))$$

Where,
n (mh) is number of nodes for transmission from master head to sink,
n is number of nodes in grid.
In existing approach the master node is selected based on RSSI value. Energy consumption of master node in time t is

$$\varepsilon_t \text{ (mh)} = \text{t} \times \text{n(mh)} \times \sum_{i=0}^{n} (e(ni)) \qquad \textbf{…….(1)}$$

In our approach master head is selected periodically based on remaining energy of node, every node in a grid get chance to be master head for certain period, i.e. in period t every node is master head for time t/n and (t - t/n)time for normal node. Energy consumption by each node in time t is

$$\varepsilon\ (n_i) = \text{t}\ (n_i) \times 1 \times \text{e}(n_i) \times r_i \times (\text{t} - \text{t/n}) + \text{t/n} \times \text{n(mh)} \times \sum_{i=0}^{n} (e(ni)) \qquad \textbf{……(2)}$$

By comparing (1) and (2) , it is clearly that proposed system consumes less energy and energy efficient.

Algorithm 1:
Route Optimization algorithm

1. Every node participates in route deciding process. Each node stores master head = self , master Energy = self - remaining energy initially. Every node transmits Route Request Packet with following format

RREQ (seqno , source address , remainEnergy, InitialEnergy)

2.For every RREQ packet received from neighbor sensor node repeat step 3

3.(a) If master head = self then

i) If RREQ packet received has remaining energy more than current node then it sets master head = source address in received packet

ii) Set master energy = remaining - Energy in received packet

(b) Compare master energy with remaining Energy in received packet

i) If remaining Energy in received packet is more than master Energy then

ii)Sets master head = source address in received packet

iii)Set master energy = remaining energy in received packet

4.If master head =self then broadcast announcement message Announce(SourceAddress,remainingEnergy)

B)SECURE TRANSMISSION

After finding the optimized path ,we securely transmit the provenance data by using an public key cryptography technique called **ELLIPTIC CURVE CRYPTOGRAPHY(ECC)**,which involves two keys-private key and public key. This public key is assigned by the BaseStation to the source. Using this key the encryption is done at the source node. The decryption process is done at the base station using its own private key. This ECC provides a faster key generation and faster encryption and decryption with lower energy and less CPU computation time.

Algorithm 2:

Encryption

Let 'm' be the message that we are sending

Consider *'m'* has the point *'M'* on the curve *'E'*.Randomly select 'k' from [1 - (n-1)].

Two cipher texts will be generated let us consider as **C1** and **C2**.

$$C1 = k*P$$

$$C2 = M + k*Q$$

C1 and C2 will be sent.

Decryption

We have to get back the message 'm' that was sent

$$M = C2 – d * C1$$

M is the original message that we have send.

Sometimes, the packet size may become larger in worst case after encryption. To overcome this worst case and to provide security we use **LZ4 lossless compression technique** as shown in figure 2.

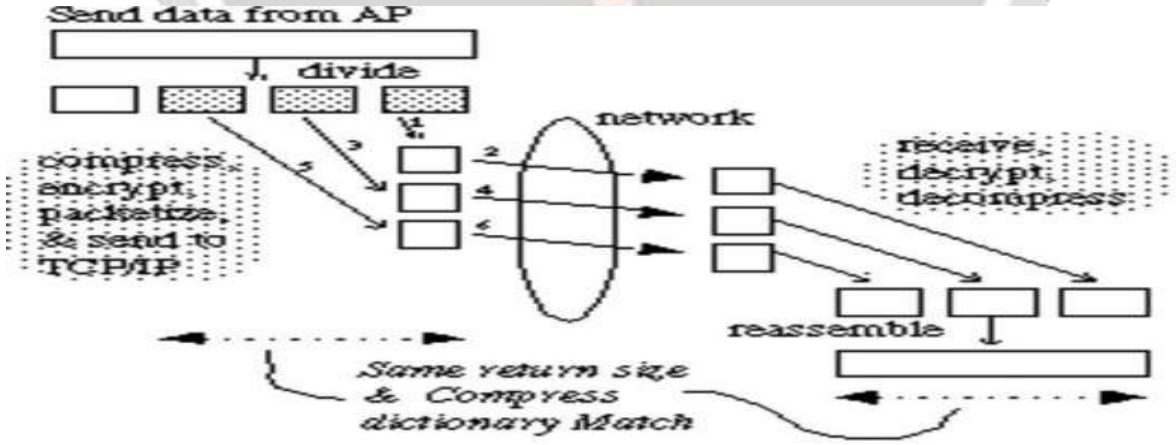

Figure 2: LZ4 compression working.

LZ4 is a lossless data compression algorithm that is focused on compression and decompression speed. The lossless compressed data can save storage space ,speedup data transmission and transmit a data without loss.LZ4 providing compression speed at 400 MB/s per core(0.16 Bytes/cycle).

4.PERFORMANCE ANALYSIS

Through simulation results we have shown energy consumption, performance ratio and packet transmission of our proposed system by comparing it with other existing system shown in figure 3.

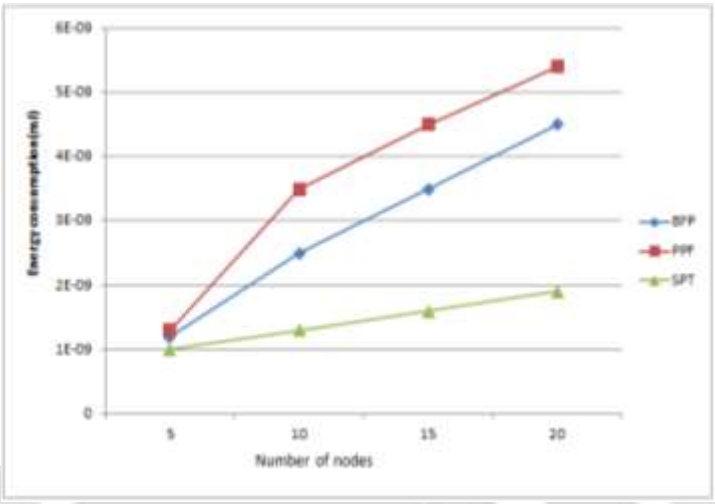

Figure 3.Total energy consumption for different nodes count.

Figure.3 illustrates the total energy consumption in Secure Provenance Transmission(SPT),BloomFilter Packet (BFP) and Probabilistic Provenance Flow (PPF) schemes for different nodes count over 100 packet transmission.

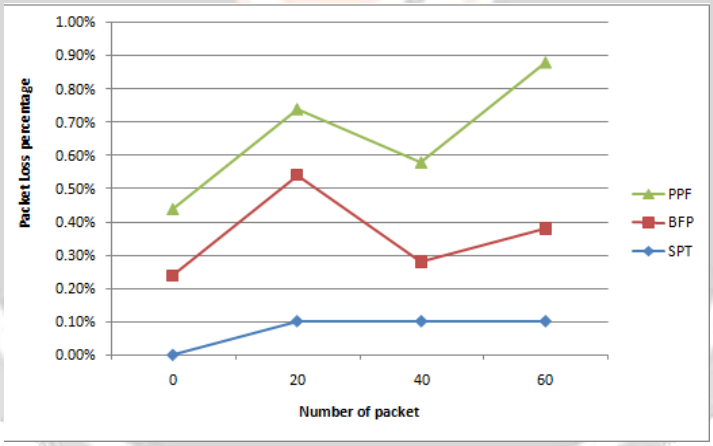

Figure 4. Packet loss rate

Figure 4. illustrates packet loss percentage of existing and proposed system.

5.CONCLUSION

In this paper, we propose an energy efficient schemes for provenance data and we securely transmit provenance data and sensor data to the destination by finding the optimized path. By using LZ4 lossless compression technique we reduce the provenance size. Simulation and experimental results show that our proposed system can save more energy and can increase the lifetime than other existing system.

6.REFERENCES

[1] S. Sultan, G. Ghinita, E. Bertino, and M. Shehab, ”A lightweight secure provenance scheme for wireless sensor networks”, in proc.IEEE 18thInt.Conf.Parallel.Distrib.Syst.2012,pp.101-108.

[2] S. M. I. Alam and S. Fahmy, “Energy-efficient provenance transmission in large –scale wireless sensor networks”, inProc. IEEEInt. Symp. World Wireless, Mobile Multimedia Netw , 2011, pp 1-6

[3] J. Ziv and A. Lempel, "A universal algorithm for sequential data compression", IEEE Trans.Inform.Theory , Vol. 24, no. 3,pp.337-343,May 1977.

[4] J. Ziv and A. Lempel, "Compression of individual sequences via variable-rate coding" ,IEEE Trans. Inform.Theory,vol.24,no.5,pp.530-536,sep 1978.

[5] W. Zhou, M. Sherr, T. Toa, X. Li, B. T. Loo and Y. Mao, "Efficient querying and maintenance of network provenance at internet scale", Proc.ACM SIGMOD Int.Conf. Manag. Data, 2010,pp.615-626.

[6]S. Chen and J. H. Reif, "Efficient lossless compression of trees and graphs", in Proc. IEEE Data Compression Conf .Mar.1996, p.428.

[7]Lun Zhang, Wenchen Yang, Qian Roa, Wei Nai, Decun Dong, "An energy saving routing algorithm based on Dijkstra in wireless sensor networks", journal of Information and computational science, 2013 pp 2087-2096.