International Journal of Engineering Sciences Paradigms and Researches (IJESPR)
(Vol. 16, Issue 01) and (Publishing Month: August 2014)
(An Indexed, Referred and Impact Factor Journal)
ISSN (Online): 2319-6564
www.ijesonline.com

Modified Ladder Diffusion in WSN

Priti Ahlawat[1] and Nitin Kumar[2]

[1]M. Tech. Scholar, Department of Electronics and Communication Engineering, GITAM, Kablana Jhajjar, Haryana (India)
pritiahlawat@gmail.com

[2]Assistant Professor, Department of Electronics and Communication Engineering, GITAM, Kablana Jhajjar, Haryana (India)

Abstract

A wireless sensor network is composed of hundreds or thousands of tiny resource-constrained sensors, equipped with non rechargeable batteries. For such sensors, transmission is much more energy consuming than computation. The innovative concept is to aggregate multiple sensing data by performing diverse operations like algebraic or statistical operations such as addition, median, minimum, maximum, and mean of a data set, etc., which is sensed by sensor nodes. The existing work proposes ladder diffusion (LD) algorithm to map out the data relay routes in wireless sensor nodes. The objective of the algorithm is to balance the data communication overhead, increasing the lifetime of sensor nodes and their transmission efficiency. The existing Ladder diffusion algorithm is modified by using the concept of cache memory. The cache memory is used to select the appropriate path using the most used path. The ladder diffusion works normally for the first time. But for the other times, for same source and destination the cached path is followed instead of the ladder diffusion path. This research proposes ladder diffusion algorithm and compare the performance of the proposed algorithm with the existing algorithm i.e. direct diffusion over the different scenario having 3, 30, 50, 150 nodes respectively. The comparison is done by suing the packet delivery ratio and the end 2 end delay. There is no impact of increase in number of nodes on the e2edelay in existing or proposed protocol. The PDR of the proposed protocol is enhanced a lot as compared to the existing algorithm. The PDR of the proposed algorithm is better in each scenario as compared to the existing algorithm. The better PDR show the better performance of the proposed protocol as compared to the existing algorithm.

Keywords: *Wireless Sensor Network, Aggregation, Ladder Diffusion*

I. Introduction

Wireless sensor network (WSN) is a self-organized multi-hop network composed of a large number of sensor nodes [1]. Each sensor node has the ability to sense data, process data, and communicates with others, so it is data-centric network. WSN is typically used in environment monitoring, healthcare, traffic management and battlefield. The data transmitted between the nodes may be sensitive (e.g. offensive weapon, troop movement, defense information). The whole network will be threatened if they are revealed by an eavesdropper. So it is vital for us to adopt effective strategy to ensure the transmission safety of the secret information.

Their low cost provides a means to deploy large sensor arrays in a variety of conditions capable of performing both military and civilian tasks. But sensor networks also introduce severe resource constraints due to their lack of data storage and power. Both of these represent major obstacles to the implementation of traditional computer security techniques in a wireless sensor network. The main aspects of wireless sensor network security into four major categories [2]: the obstacles to sensor network security, the requirements of a secure wireless sensor network, attacks, and defensive measures. A sensor network is a special type of Ad hoc network. So it shares some common property as computer network. There are usually several security requirements to protect a network [3]. These requirements should be considered during design of a security protocol, including confidentiality, integrity, and authenticity. An effective security protocol should provide services to meet these requirements.

II. Aggregation in WSN

Aggregation techniques are used to reduce the amount of data communicated within a WSN and thus conserves battery power [4]. Periodically, as measurements are recorded by individual sensors, they need to be collected and processed to produce data representative of the entire WSN, such as average and/or variance of the temperature or humidity within an area. One natural approach is for sensors to send their values to certain special nodes, i.e., aggregators. Each aggregator then condenses the data prior to sending it on. In terms of bandwidth and energy consumption, aggregation is beneficial as long as the aggregation process is not too CPU-intensive. The aggregators can either be special (more powerful) nodes or regular sensors nodes. The main objective of data aggregation is to increase the network lifetime by reducing the resource consumption of sensor nodes (such as battery energy and bandwidth). While increasing network lifetime, data aggregation protocols may degrade important quality of service metrics in wireless sensor networks, such as data accuracy, latency, fault-tolerance, and security [5]. Therefore, the design of an efficient data aggregation protocol is an inherently challenging task because the protocol designer must tradeoff between energy efficiency, data accuracy, latency, fault-tolerance, and security. In order to achieve this trade off, data aggregation techniques are tightly coupled with how packets are routed through the network. Hence, the architecture of the sensor network plays a vital role in the performance of different data aggregation protocols.

III. Ladder Diffusion

The innovative concept is to aggregate multiple sensing data by performing diverse operations like algebraic or statistical operations such as addition, median, minimum, maximum, and mean of a data set, etc., which is sensed by sensor nodes. Aggregation accuracy is looked-for for the final decision this is based on the aggregation result, especially for some sensitive applications where a small difference of result may lead to completely different decisions. The existing work proposes ladder diffusion (LD) algorithm to map out the data relay routes in wireless sensor nodes. The objective of the algorithm is to balance the data communication overhead, increasing the lifetime of sensor nodes and their transmission efficiency [6]. The existing ladder diffusion algorithm with ladder diffusion with verification algorithm in order to minimize energy consumption is presented.

A. The ladder diffusion phase

The locations of the sensor nodes deploy stable, and the routing table built by AODV (Ad-hoc On Demand Vector) is only a small portion of the entire wireless sensor network, energy consumption is increases by rebuilding the routing table for the deleted routes. In DD, the sink node can diffuse its interested query packets to other sensor nodes by broadcasting to the whole network, adjusting the route weights does not decreases the energy consumption in creating circle results. In this dissertation, the ladder diffusion algorithm concern to identify routes from sensor nodes to the sink node and avoid the generation of circle routes using the directed diffusion process. First, the sink node transmits the ladder-creating package with the node value of one, as shown in Figure 1. A node value of one means that the sensor node receiving this ladder-creating package transmits data to the sink node requires only one hop. In Figure 3.1, the sensor nodes ‘‘b’’ and ‘‘c’’ obtain a ladder-creating package with a node value of one from sink node ‘‘a’’. Then sensor nodes ‘‘b’’ and ‘‘c’’ increase the node value of the ladder-creating package to two and transmit the modified ladder-creating package. The sensor nodes ‘‘d’’, ‘‘e’’, and ‘‘f’’ receive ladder-creating packages with a node value of two from nodes ‘‘b’’ and ‘‘c’’ and each sensor nodes increases node value continuously until it reach the source node. Moreover, if many sensor nodes concurrently transmit ladder-creating packages with the same node value, the sensor nodes receive and record the packages in their respective ladder tables as back-up nodes. But the sensor nodes discard the package because the node value of the sensor nodes surrounding nodes is less than actual node value.

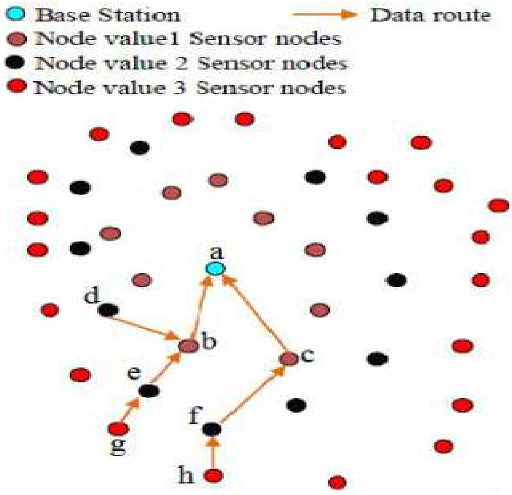

Figure 1: Data Transfer Routes for Sensor Nodes [6]

After the ladder diffusion process, the data transfer routes going from high grade value to low grade value which is depending on the ladder table already created, as shown in Figure 2. As the sensor nodes are required to send data to the sink node, the routes are energetically created by starting with nodes of high grade value and ending with nodes of low grade value. In accretion, each sensor node records the grade value of the relay node in its ladder table, and the ladder diffusion algorithm has the following advantages:

a. Avoiding redundant relays

Redundant relays could occur under DD, as Figure 3.2 shows. Figure 3.2 illustrates that sensor node ‘‘A’’ transmits data to the sink node only three hop counts along data path (route) 1. The packages returned faster in the sensor nodes on route 1 than in the route 2, then sensor node ‘‘a’’ will send data to the sink node along route 2. It has six hop counts to relay data along route 2, and energy would be ebbed.

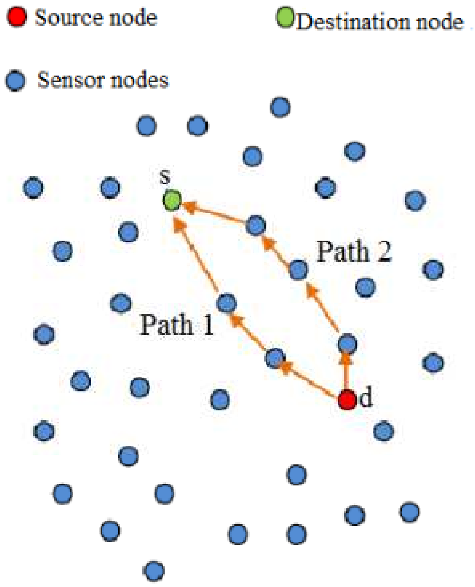

Figure 2: Redundant Relays in Wireless Sensor Networks

The phenomenon shown in Figure 2 can be solved using the LD algorithm. The LD algorithm can swear that the direction of data transfer always occurs from a high node value to a low node value, which means each relay is forwarded to the sink node since each sensor node records the node value of relay nodes in the ladder table. Thus, the LD algorithm can avoid power consumption due to redundant relays. The ladder diffusion algorithm can evade the situation in which nodes are moved or lost. The ladder diffusion algorithm records the node value of each sensor node in the ladder table. The sensor node can record more than one node as relay nodes in the ladder table when receiving the ladder-creating package with a grade value less than itself.

Verification Algorithm

The verification algorithm helps to detect the attacks in the network during data aggregation.

A. Protocol Operation

The verification protocol runs concurrently with the original ladder diffusion protocol described as follows. This existing work reminds the readers that in the original protocol M 1, ladder are computed. However, for ease of exposition, describe verification protocol with respect to one single ladder. Each ladder can be verified independently and hence our algorithm is readily applicable for computing multiple ladders.

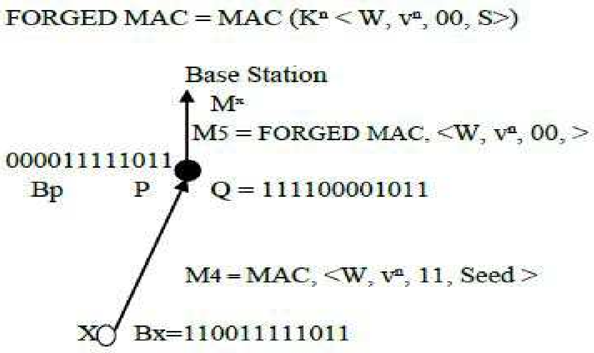
FORGED MAC = MAC (Kⁿ < W, vⁿ, 00, S>)
Base Station
Mˣ
M5 = FORGED MAC, <W, vⁿ, 00, >
000011111011
Bp
P
Q = 111100001011
M4 = MAC, <W, vⁿ, 11, Seed >
X
Bx=110011111011

Figure 3: MAC Forging During Aggregation Phase

```
**Algorithm 1** Verifiable Aggregation (X, Qx, k)
**begin**
receive $\{(B'x^1, M^{x1}), (B'x^2, M^{x2}), \ldots,$
$(B'xd, M^{x}d)\}$ from $d$ child nodes;
$B'x = Q'x \| B'x^1 \| B'x^2 \| \ldots \| B'xd$;/* aggregate received
```

ladder with local one ***/**
Ij$^{\times}$ = the index of the jth rightmost “1” bit in Bˈx, for 1 where is the largest such integer not higher than ; **/*** Bˈx may have fewer than k “1” bits where ***/**
generate one MAC for bit Ij$^{\times}$ in Qˈx, for 1 construct the union Ɱ of the received MAC’s and self-generated ones; randomly select Ɱ$^{\times}$ = {Ɱ**I1$^{\times}$**, Ɱ**I2$^{\times}$,.......** Ɱ**Ik**$^{\times}$ } from Ɱ; broadcast (Bˈx, Ɱ$^{\times}$) to parents;
end

IV. Proposed Work

The existing Ladder diffusion algorithm is modified by using the concept of cache memory. The cache memory is used to select the appropriate path using the most used path. The ladder diffusion works normally for the first time. But for the other times, for same source and destination the cached path is followed instead of the ladder diffusion path. The process can be understood by the following algorithm:

1. Select S and D from N nodes.
2. If cache empty
3. Use Ladder diffusion for the path between S and D
4. Store the selected path in cache.
5. Else
6. Match S and D of cache memory with current S and D
7. If S and D match
8. Then transfer data using selected path
9. Else
10. Go to step 3.
11. End if
12. End if

V. Simulation Results

The research implements the proposed protocol by using NS2.35 which is installed over fedora 17. The research has implemented the proposed ladder diffusion. The simulation is analyzed over different scenarios having nodes 3, 30, 100, 150 respectively. Whenever, TCL file is run then a trace file get generated. Trace file is used to analyze various parameters using AWK scripts. The parameters analyzed are given in next section.

Parameters

- **Packet Delivery Ratio**

The ratio of the number of delivered data packet to the destination. This illustrates the level of delivered data to the destination.
∑ Number of packet receive / ∑ Number of packet send
The greater value of packet delivery ratio means the better performance of the protocol.

- **End-to-end Delay**

The average time taken by a data packet to arrive in the destination. It also includes the delay caused by route discovery process and the queue in data packet transmission. Only the data packets that successfully delivered to destinations that counted.
∑ (arrive time – send time) / ∑ Number of connections

Results

The table1 to table 2 shows the result of various parameters on various protocols i.e. Existing and proposed diffusion. These results can be verified from the snapshots shown below.

- **Existing Algorithm**

Table 1: Parameter Analysis of Exiting Algorithm

Number of nodes	Generated Packets	Received Packets	PDR	E2E delay(ms)
3	160	135	84.375	0.304832
30	252	140	55.5556	0.304832
50	313	141	45.0479	0.304832
150	601	135	22.4626	0.304832

- **Proposed Algorithm**

Table 2: Parameter Analysis of Proposed Algorithm

Number of nodes	Generated Packets	Received Packets	PDR	E2E delay(ms)
3	512	511	99.8047	0.30426
30	1188	1142	96.1279	0.30426
50	1682	1566	93.1034	0.30426
150	4184	3503	83.7237	0.30426

The graphical analysis i.e. comparison of existing and proposed is shown from figure 4 to 7. The figure 4 shows the generated packets of existing and proposed, Figure 5 received packets of existing and proposed, Figure 6 comparison of PDR on various numbers of nodes for existing and proposed. The figure 7 shows comparison of E2Edelay respectively.

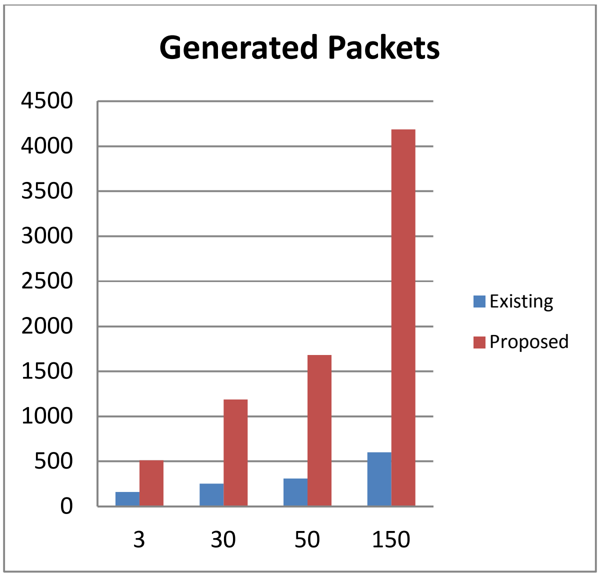

Figure 4: Generated Packets of Existing and Proposed Algorithm

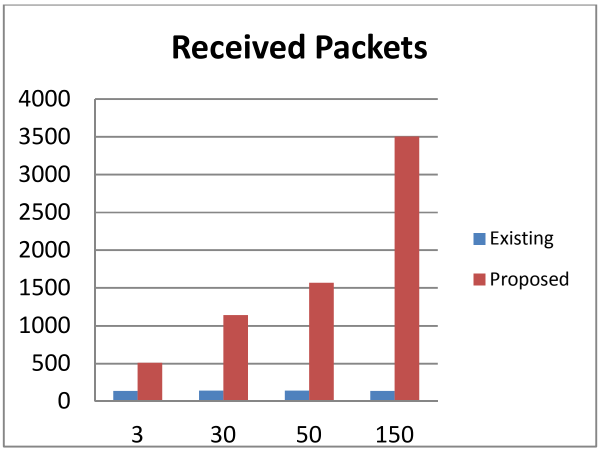

Figure 5: Received Packets of Existing and Proposed Algorithm

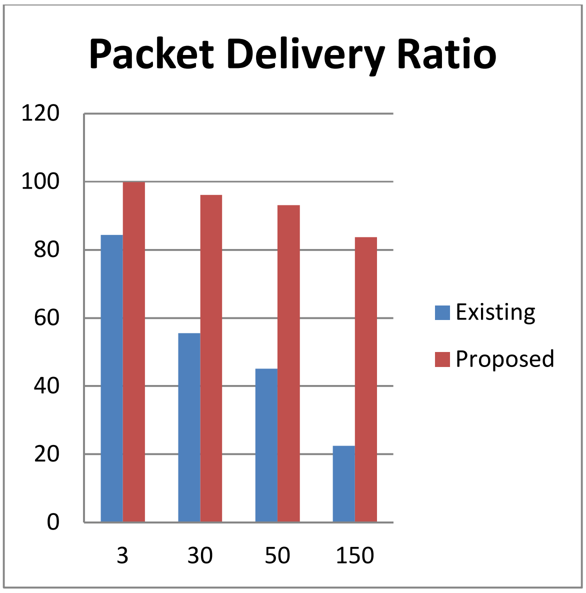

Figure 6: PDR of Existing and Proposed Algorithm

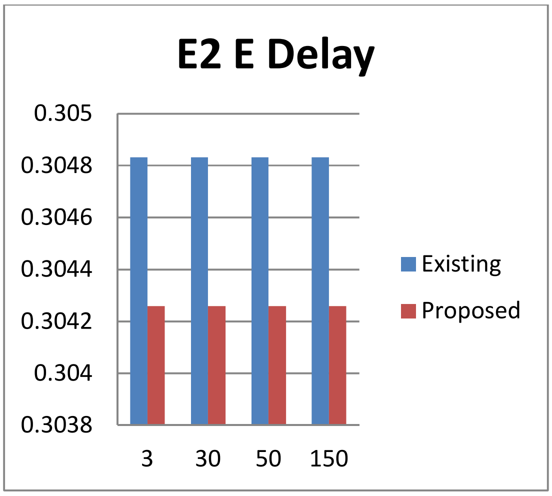

Figure 7: E2 E Delay of Existing and Proposed Algorithm

VI. Conclusion

This research proposes ladder diffusion algorithm and compare the performance of the proposed algorithm with the existing algorithm i.e. direct diffusion over the different scenario having 3, 30, 50, 150 nodes respectively. The comparison is done by using the packet delivery ratio and the end 2 end delay. There is no impact of increase in number of nodes on the e2edelay in existing or proposed protocol. The PDR of the proposed protocol is enhanced a lot as compared to the existing algorithm. The PDR of the proposed algorithm is better in each scenario as compared to the existing algorithm. The better PDR show the better performance of the proposed protocol as compared to the existing algorithm. In future following work can be done: The proposed protocol can be compared with other existing protocols like DSDV, ZRP etc., The proposed protocol can be analyzed on other parameters like normalized routing load and throughput etc.

References

[1] Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., & Cayirci, E. (2002). A survey on sensor networks. Communications magazine, IEEE, 40(8), 102-114.

[2] Walters, J. P., Liang, Z., Shi, W., & Chaudhary, V. (2007). Wireless sensor network security: A survey. Security in distributed, grid, mobile, and pervasive computing, 1, 367.

[3] Singh, S. K., Singh, M. P., & Singh, D. K. (2011). A survey on network security and attack defense mechanism for wireless sensor networks. Int. J. Comput. Trends Tech, 5-6.

[4] Castelluccia, C., Mykletun, E., & Tsudik, G. (2005, July). Efficient aggregation of encrypted data in wireless sensor networks. In Mobile and Ubiquitous Systems: Networking and Services, 2005. MobiQuitous 2005. The Second Annual International Conference on (pp. 109-117). IEEE.

[5] Ozdemir, S., & Xiao, Y. (2009). Secure data aggregation in wireless sensor networks: A comprehensive overview. Computer Networks, 53(12), 2022-2037.

[6] Vinu Raja Vijaya Kumar (2013) , Secure Data Aggregation using Ladder Diffusion Algorithm in Wireless Sensor Networks, International Journal of Emerging Trends in Electrical and Electronics (IJETEE – ISSN: 2320-9569) Vol. 3, Issue. 1, May-2013.