Secure Data Aggregation using Ladder Diffusion Algorithm in Wireless Sensor Networks

Vinu Raja VijayaKumar¹ S.Chinnaiya²

Abstract: The scarcity in wired environment has been decupled in wireless technology. Wireless sensor networks reigns over wired in cost, technology, scalability and flexibility. It has its own authority over industrial informatics, automation and in computational field. This global enterprise is ubiquitous, pervasive and tangible with emerging simulation tools. However, the wireless environment has its own ailment due to inherent stringent bandwidth, energy constraints and with fading security. This paper marches towards the kinship between security and data aggregation. Data aggregation can evidently help to reduce the energy consumption by discarding redundant data and decrease the communication overhead. The proposed ladder diffusion algorithm is employed to route paths for data relay and transmission in wireless sensor networks, which decreases both power consumption and dispensation time to create the routing table and concurrently avoiding network congestion. In this paper, the ladder diffusion approach secures against attacks during data aggregation. Data aggregators are under the threat of various types of attacks. The verification algorithm ensures that the secure data transmission is achieved without releasing private sensor readings and without introducing significant overhead on the battery-limited sensors. The performance of proposed scheme is analyzed using Network simulator to show the approach is scalable and efficient.

Keywords: Base station, data aggregation, ladder diffusion, wireless sensor networks.

I. INTRODUCTION

Wireless Sensor Networks (WSN) has been widely deployed in many applications, e.g., accident report, environment monitor, military field surveillance, health care, etc. 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. Therefore, the amount of communication overhead should be kept as low as possible, in order to extend the lifetime of wireless sensor networks.

Generally, sensors are inhibited in data transfer, battery power, and computation ability; therefore, reducing the power consumption is prior concern for a WSN. Recently, a realistic solution called data aggregation [4]-[9]-[20] was introduced.

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. This paper 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.

In this paper, an algorithm used to compute aggregates, such as Count and Sum, and to enable the base station to verify if the computed aggregate is valid. The paper proposes the verification algorithm, though strictly speaking, it is an aggregate computation and verification algorithm. The key observation which we exploit to minimize the communication overhead of this algorithm is that to verify the correctness of the final ladder(the aggregate of the whole network) each nodes does not need a privacy key for all sensed messages which sent to base station. It is to be noted that while our algorithm is designed having WSNs in mind, it is straightforward to extend our solution for secure aggregation query processing in a large-scale distributed database system over the Internet [6].

II. RELATED WORK

Some researchers have wilful problems allied to data aggregation in WSNs.

A. Data Aggregation without any Provision for Security

In the paper [3] introduced the directed diffusion (DD) protocol in 2003. DD aims to decrease the data relay and energy consumption. Basically, DD is a query-driven transmission protocol. The collected data are transmitted only if they fit the query from the sink node, thereby decreases the energy consumption due to data transmission. First, the sink node provides involved queries in the form of attribute-value pairs to the other sensor nodes by broadcasting the involved query packets to the entire network. Subsequently, the sensor nodes only transmit the

Vinu Raja VijayaKumar pursuing Master of Engineering in Applied Electronics, K. S. R. C. E, Tamil Nadu. Email: vinurajaa.v@gmail.com. S. Chinnaiya is working as Senior Assistant Professor in Department of EEE, K. S. R. C. E, Tamil Nadu. Email: chinnaiyas@gmail.com.

collected data back to the sink node in case they fit the fascinated queries. In DD, all sensor nodes are bound into a route when broadcasting the interested queries, even if the route is such that it will never be used.

Also several circle route are built concurrently when transmitting the queries, result in wasted power consumption and storage. Thus, the paper attempts to design an approach that allows the base station to receive all sensing data but still reduce the transmission overhead.

B. Secure Aggregation Techniques

Several secure aggregation algorithms have been proposed assuming that the base station is the barely aggregator node in the network [12]–[16]. It is not straightforward to extend these works for verifying in-network aggregation unless we direct each node to send an authentication message to the base station, which is a very expensive solution. A tree-based verification algorithm was designed in [2]–[18] by which the base station can detect if the final aggregate, Count or Sum, is falsified. The paper is unable to extend this idea for verifying a synopsis because the synopsis computation is duplicate-insensitive. A verification algorithm for computing Count and Sum within the synopsis diffusion approach was designed in [6]. In addition, algorithm provides extensive theoretical analysis to find the best tradeoffs between the security and communication overhead. Recently, a few novel protocols have been proposed for “secure outsourced aggregation” [11]; however, these algorithms are not designed for WSNs.

III. LADDER DIFFUSION

In this section, traits on our proposed ladder diffusion algorithm that with ladder diffusion with verification algorithm in order to minimize energy consumption are 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 paper, 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 Fig. 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 Fig. 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.

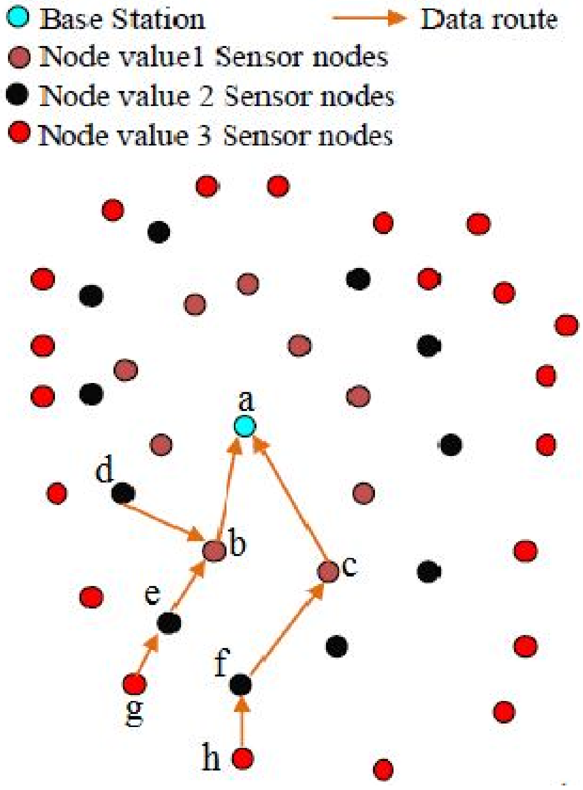

Figure 1: Data transfer routes for sensor nodes

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 Fig. 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 Fig. 2 shows. Fig. 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.

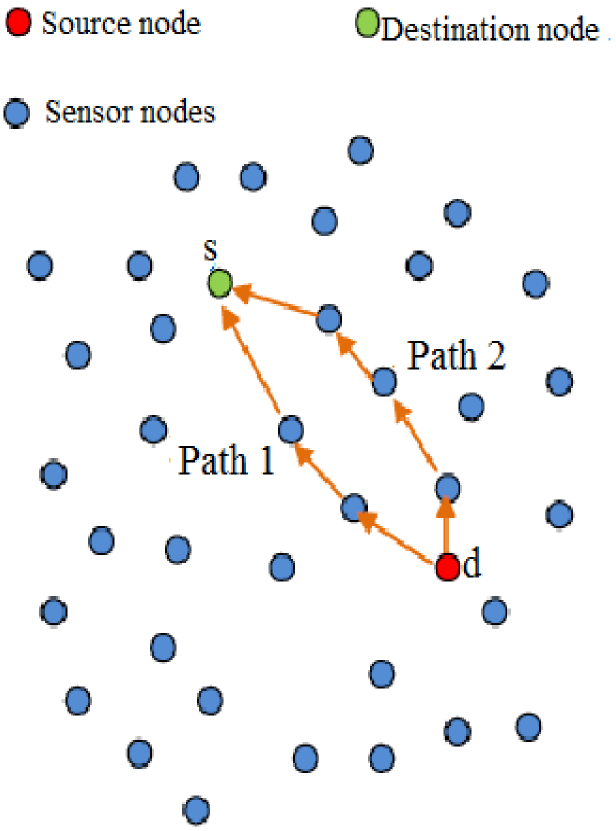

Figure 2: Redundant relays in wireless sensor networks

The phenomenon shown in Fig. 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.

IV. 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 [4]–[12] described as follows. We remind the readers that in the original protocol M $\geq$1, ladder are computed. However, for ease of exposition, we describe our 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.

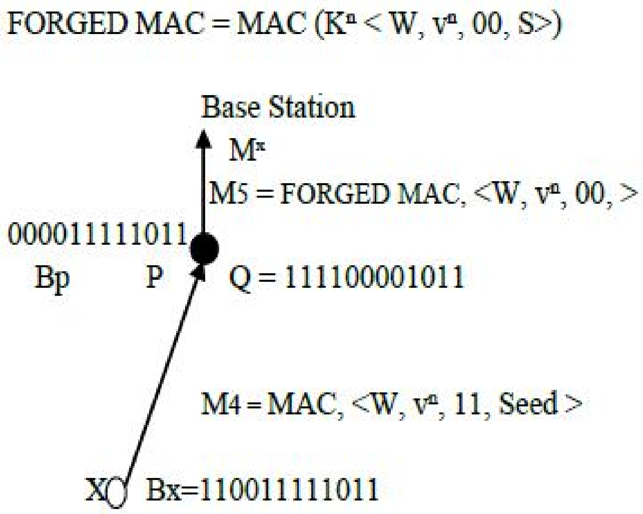
FORGED MAC = MAC (Kⁿ < W, vⁿ, 00, S>)
Base Station
Mˣ
M5 = FORGED MAC, <W, vⁿ, 00, >
000011111011
Bp
P
Q = 111100001011
M4 = MAC, <W, vⁿ, 11, Seed >
X
Bx=110011111011

Figure 3: MAC Forging during Aggregation Phase

```
Algorithm 1 Verifiable Aggregation (X, Qx, k)
begin
receive {( B'x¹, M̡ˣ¹), (B'x², M̡ˣ²),.....,
(B'xd, M̡ˣd)} from d child nodes;
B'x = Q'x‖ B'x¹‖ B'x²‖.....‖B'xd;/* aggregate received ladder with local one */
Ijˣ = the index of the jth rightmost "1" bit in B'x, for $1\leq j \leq k'$, where $k'$ is the largest such integer not higher than $k$; /*
 B'x may have fewer than k "1" bits where $k' < k$. */
generate one MAC for bit Ijˣ in Q'x, for $1\leq j \leq k'$;
construct the union M̡ of the received MAC's and self-generated ones; randomly select M̡ˣ = {M̡I1ˣ, M̡I2ˣ,....... M̡Ikˣ } from M̡; broadcast (B'x, M̡ˣ) to parents;

end
```

B. *Example (With Attack)*

In the example, if P is malicious, it may inject a false "0" in at the 1st bit resulting in B'p = 111111111110. It can also generate a false MAC to vouch for this false "1". Node P forwards the MACs for the five rightmost "0" bits (M7, M8, M9, M10, and M11) to its parent nodes. An example of such an attack is shown in Fig. 3. In this example, MAC M11 is claimed to be generated by an arbitrary node W selected by the adversary, and W's sensed value being ϑw. Also, note that (W, ϑw, Seed) set to the 1st bit equal to "1". For ease of exposition, the relevant messages are forged and it is forwarded directly to the BS (BS being the parent of node

P).In this paper BS does the verification and detects this attack.

V. SIMULATION RESULTS

In this section, the report explores the simulation study that examined the performance and security of our verification algorithm. The evaluation is done based on several metrics, such as power consumption, network lifetime and communication overhead.

A. Simulation Environment

Simulations were written based on the Network simulator (NS2). In particular, we added the security functionality to the source code, which simulates their multipath aggregation algorithm in the Network simulator environment. The loss rate of packets is less than 10%.

B. Results and Discussion

In the proposed scheme, the data aggregation is done using ladder diffusion which is results in decreasing the power consumption communication overhead. The verification protocol helps in check the accuracy of data destined to BS from each sensor node.

a. Energy consumption

In each simulation of experiment, the energy assign to nodes are changed with number of packets. T Average energy LD (Ladder Diffusion) can effectively balance energy consumption between the sensor nodes with relatively low energy consumption and those with relatively high energy consumption. Average energy consumption is shown in Table I based on 50 repeated simulations. As shown in Table I, in proposed LD reduce average energy consumption by 3.3% and 53.9% as compared with AODV and DD, respectively. In short, LD can efficiently increase the lifetime of sensor nodes.

TABLE I

Average Energy Consumption

	20nodes (μJ)	40 nodes (μJ)	80 nodes (μJ)	Average Energy (μJ)
AODV	9005	10123	2782	5448.76
DD	10452	12021	11856	11443.03
LD	5078	6873	1412	4454.33

b. Communication overhead

In this paper the communication overhead of verification protocol is compared with the directed diffusion approach. The aggregation process is deployed repeatedly with different nodes. Fig. 4 plots the number of message or packets a node transmits on average during verification protocol considering different time interval.

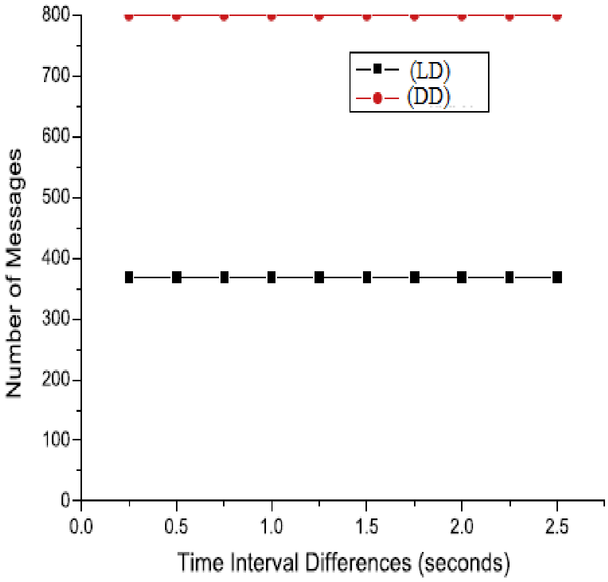

Figure 4: Communication overhead

The total number of messages or packets communicated during each aggregation round as the metric. Simulation results show that the bandwidth consumption of DD is higher than that of LD. This can be explained by analyzing the number of exchanged messages in each scheme.

c. Accuracy

The accuracy metric is defined as the ratio between the collected summation by the data aggregation scheme used and the real summation of all individual sensor nodes in [10].

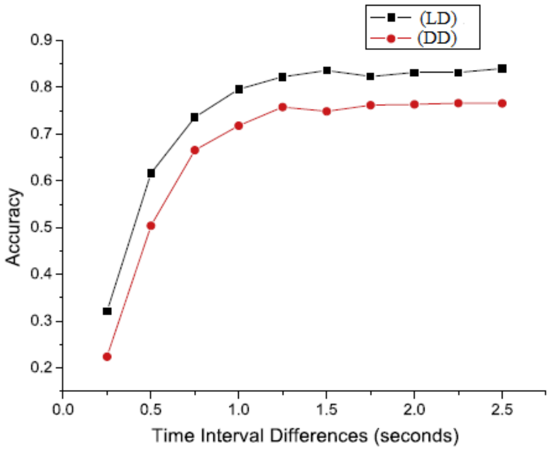

Figure 5: Data Accuracy

From Fig. 5 the accuracy increases as the time interval increases. Two reasons contribute to this, which have already been analyzed in [10]. (1) With longer time interval, the data messages to be sent within this duration will have less chance to collide. (2) With longer time interval, the data messages will have a better chance of being delivered within the deadline.

VI. CONCLUSION

In wireless sensor networks, sensor nodes are usually resource inhibited and battery-limited. And transmission is much more energy consuming than computation. Therefore, communication overhead is an important issue in wireless sensor networks. Data aggregation can diminish the communication overhead and energy consumption, thus extending the lifetime of wireless sensor networks. In this paper, the ladder diffusion approach and verification algorithm is implemented. In addition, to make sure the safety and reliability of data transmission, the algorithm provides back-up routes to avoid wasted power consumption and processing time when rebuilding the routing table in case of a sensor node is missing. The result shows that the power consumption and communication overhead is decreased with secure transmission in the network. The experimental results can be extended to transmit the multimedia messages from sensor nodes that exchange audio and video signals showing how the proposed solution can be tailored to many application domains.

REFERENCES

[1] Buttyan, L, P. Schaffer, and I. Vajda, "Resilient aggregation with attack detection in sensor networks," in *Proc.* 2nd IEEE Workshop Sensor Networks and Systems for Pervasive Computing, 2006.

[2] Chan, H, A. Perrig, and D. Song, "Secure hierarchical in-network aggregation in sensor networks," in Proc. ACM Conf. Computer and Communications Security (CCS), 2006.

[3] Chalermek Intanagonwiwat, Ramesh Govindan, Deborah Estrin, John Heidemann, Fabio Silva, Directed diffusion for wireless sensor networking, IEEE ACM Transactions on Networking 11 (February) (2003) 2–16.

[4] Considine, J, F. Li, G. Kollios, and J. Byers, "Approximate aggregation techniques for sensor databases," in Proc. IEEE Int. Conf. Data Engineering (ICDE), 2004.

[5] Frikken. K. B, and J. A. Dougherty, "An efficient integrity-preserving scheme for hierarchical sensor aggregation," in Proc. 1st ACM Conf. Wireless Network Security (WiSec), 2008.

[6] M. Garofalakis, J. M. Hellerstein, and P. Maniatis, "Proof sketches: Verifiable in-network aggregation," in Proc. 23rd Int. Conf. Data Engineering (ICDE), 2007.

[7] James Reserve Microclimate and Video Remote Sensing 2006 [Online]. Available: http://research.cens.ucla.edu.

[8] Jessica, A, Carballido, Ignacio Ponzoni, Nélida, B, Brignole, A graph-based genetic algorithm for sensor network design, Information Sciences 177 (22) (2007) 5091–5102.

[9] Madden, S, M. J. Franklin, J. M. Hellerstein, and W. Hong, "TAG: A tiny aggregation service for ad hoc sensor networks," in Proc. 5th USENIX Symp. Operating Systems Design and Implementation (OSDI), 2002.

[10] Nath, S, P. B. Gibbons, S. Seshan, and Z. Anderson, "Synopsis diffusion for robust aggregation in sensor networks," in Proc. 2nd Int. Conf. Embedded Networked Sensor Systems (SenSys), 2004.

[11] Nath, S, H. Yu, and H. Chan, "Secure outsourced aggregation via one-way chains," in Proc. 35th SIGMOD Int. Conf. Management of Data, 2009.

[12] Przydatek, B, D. Song, and A. Perrig, "SIA: Secure information aggregation in sensor networks," in Proc. 1st Int. Conf. Embedded Networked Sensor Systems (SenSys), 2003.

[13] Pan, J, Y. Hou, L. Cai, Y. Shi, X. Shen, Topology control for wireless sensor networks, in: The Ninth ACM International Conference on Mobile Computing and Networking, 2003, pp. 286–299.

[14] Rajiv Misra, Chittaranjan Mandal, Ant-aggregation: ant colony algorithm for optimal data aggregation in wireless sensor networks, in: 2006 IFIP International Conference on Wireless and Optical Communications Networks, 2006.

[15] Roy, S, S. Setia, and S. Jajodia, "Attack-resilient hierarchical data aggregation in sensor networks," in Proc. ACM Workshop Security of Sensor and Adhoc Networks (SASN), 2006.

[16] D. Wagner, "Resilient aggregation in sensor networks," in Proc. ACM Workshop Security of Sensor and Adhoc Networks (SASN), 2004.

[17] Wen-Hwa Liao, Yucheng Kao, Chien-Ming Fan, Data aggregation in wireless sensor networks using ant colony algorithm, Journal of Network and Computer Applications 31 (2008) 387–401.

[18] Y. Yang, X. Wang, S. Zhu, and G. Cao, "SDAP: A secure hop-by-hop data aggregation protocol for sensor networks," in Proc. Seventh ACM Int. Symp. Mobile Ad Hoc Networking and Computing (MobiHoc), 2006.

[19] Yu, H, "Secure and highly-available aggregation queries in large-scale sensor networks via set sampling," in Proc. Int. Conf. Information Processing in Sensor Networks, 2009.

[20] Yu, Y, Govindan, R, Estrin, D, "Geographical and energy aware routing: a recursive data dissemination protocol for wireless sensor networks," Technical report UCLA/CSD-TR-01-0023. UCLA Computer Science Department; 2001.

[21] Younis, O, Fahmy, S, "Heed: a hybrid, energy-efficient, distributed clustering approach for ad-hoc networks," IEEE Transactions on Mobile Computing 2004; 3(4):366–9.

[22] Zhao, J, R. Govindan, and D. Estrin, “Computing aggregates for monitoring sensor networks,” in Proc. 2nd Int. Workshop Sensor Network Protocols Applications, 2003.

[23] Zhen Hea, Byung Suk Lee, X. Sean Wang, Aggregation in sensor networks with a user-provided quality of service goal, Information Sciences 178 (9) (2008) 2128–2149.

[24] Zhu, X, “Pheromone based energy aware directed diffusion algorithm for wireless sensor network,” In: Proceedings of the international conference on intelligent computing (ICIC); vol. 4681; 2007. 283–91.

[25] Zaman, N, Abdullah A. B, “Energy efficient routing in wireless sensor network: research issues and challenges,” In: Proceedings of IEEE international conference on intelligence and information technology; 2010.

Vinu Raja VijayaKumar received B.E degree in Electronics and communication in Vinayaka Mission’s University. He is pursuing Master of Engineering in Applied Electronics at K. S. R. College of Engineering. He presented a paper in an International conference at Karunya University. His research interests include wireless sensor network, multimedia network security, and applied cryptography.

S. Chinnaiya received B.E degree in Electrical and Electronics Engineering in Mahendra Engineering College in 2004. He received M.E degree in Power Electronics and Drives in Bannari Amman Institute of Technology in 2006. He is working as a Senior Assistant Professor in Department of EEE in K. S. R. College of Engineering. He is pursuing PhD under Anna University, Chennai. His area of interest includes Power Electronics Converter, Digital Controller based Drives.