Asian Journal of Applied Science and Technology (AJAST)
Volume 1, Issue 1, Pages 186-190, February 2017

Secured Data Aggregation using SRL Protocol for Wireless Sensor Networks

V.Vinu Raja[1] and Mohammed Irfan Lebbai[2]

[1]*Department of Electronics and Communication Engineering, Sri Eshwar College of Engineering, Coimbatore, India. Email: vinurajaa@gmail.com*
[2]*Network Administrator, Tata Consultancy Services, Chennai, India. Email: mohamed.irfan1@tcs.com*

Article Received: 11 February 2017 *Article Accepted: 26 February 2017* *Article Published: 28 February 2017*

ABSTRACT

In wireless sensor network energy cutback is considered as a principle intensive challenge which is studied largely in the Wireless Sensor Networks (WSN) literature. Wireless Sensor Networks (WSNs) are pertinent in numerous arenas where WSNs may be used for sensing, ciphering, and communication elements that give a user or administrator the ability to instrument, observe, and retort to events and phenomena in a specific environment. But sensor devices are resource curbed, positioned in an open and unattended environment, different types of attacks and conventional techniques against these attacks are not desirable due to the resource constrained nature of these kinds of networks. An energy-balanced routing method based on forward-aware factor (FAF-EBRM) in which the next-hop node is elected according to the awareness of link weight and forward energy density. FAF-EBRM is compared with Ladder Diffusion Algorithm, which balances the energy utilization, sustain the function era and guarantees high QoS of WSN. The FAF-EBRM is proposed with Secure Routing Layer (SRL) Protocol which ensures that the secure data transmission is achieved without releasing private sensor readings and without introducing significant overhead on the battery-limited sensors.

Keywords: Energy balance routing, forward-aware factor, SPIN algorithm, Security and wireless sensor networks.

1. INTRODUCTION

Holocene technological debuts made in electronics and wireless communications have fostered the enlargement of wireless sensor networks (WSNs). A WSN is a self-organization wireless network system typically dwells of many small, low cost, low-power communication devices called sensor nodes. Each sensor node has restricted on-board processing, inadequate storage and radio capabilities. Owing to the limited communication ability and Non-rechargeable energy supply (e.g. battery), WSNs have rigorous requirements about power consumption. Therefore energy-efficient protocols are vital to save energy and protract network lifetime. Micro sensors are deployed to monitor the sensing field and collect information from physical or environmental condition and to co-operatively pass the collected data through the network to a main location.

Traditionally there are two approaches to accomplish the data collection task: Single-hop and Multi-hop forwarding. In single hop wireless communication (Direct), the sensor nodes upload data directly to the sink, which may result in long communication distances and degrade the energy efficiency of sensor nodes. But in multi-hop forwarding, data are transferred from the nodes to the sink through multiple relays, and thus communication distance is reduced. However, since nodes closer to the sink have a much heavier forwarding load, their energy may be exhausted quickly, which degrades the network performance.

Clustering is an effective technique to reduce energy consumption in WSNs. In clustering algorithm, a number of nodes in a network will be chosen as the cluster heads (CHs) and the remaining nodes will be regarded as the cluster members (CMs). CMs will form connections with the CHs. A head node will collect data from its CMs and the actual data transmitted to the base station (BS).In WSN clustered hierarchical routing protocols, at times CMs are closer to the sink than CH, but it should transmit data to CH earliest. This backward transmission result in waste of energy.

2. RELATED WORK

2.1 SECURE AGGREGATION TECHNIQUES

Several secure aggregation algorithms have been proposed assuming that the base station is the barely aggregator node in the network [8]–[6]. 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]–[10] 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" [5]; however, these algorithms are not designed for WSNs.

2.2 LOW ENERGY ADAPTIVE CLUSTERING HIERARCHY (LEACH) PROTOCOL

In LEACH, all the nodes in a network organize themselves into local clusters. The protocol is divided into a setup phase when the clusters are organized and a steady state phase when CH receive data from all the CMs, perform data aggregation and transmit data to the remote base station. The operation of LEACH in time slots is illustrated in Figure1.

© 2017 AJAST All rights reserved.

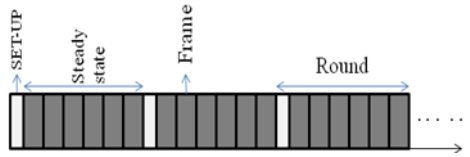


Fig.1. Timeline of LEACH operation

2.3 Forward Aware Factor - Energy Balanced Routing Method (FAF-EBRM)

In WSN routing protocol, sometimes cluster members in a cluster are nearer to the sink than the CH, but it should transmit data to CH first. It results backward transmission of data and thus leads to waste of energy. This reliable path method results in reduced energy consumption and the routing model is shown in Figure.2.

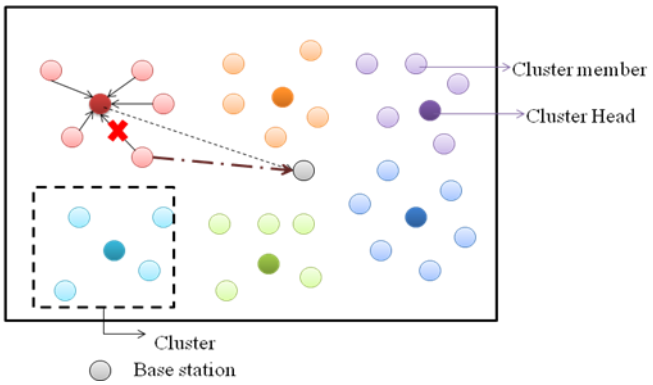


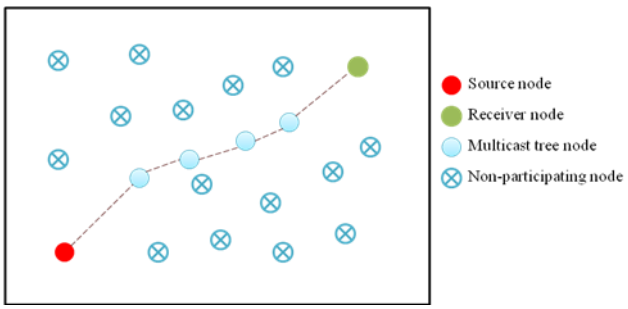
Fig.2. FAF-EBRM reliable path

In this method, an energy-balanced routing protocol is designed that uses forward transmission area (FTA) based on position of sink and final data flow direction. In other words, FTA define forward energy density which constitutes forward-aware factor with link weight, and propose a new communication protocol based on forward-aware factor, thus balancing the energy consumption and prolonging the network function lifetime.

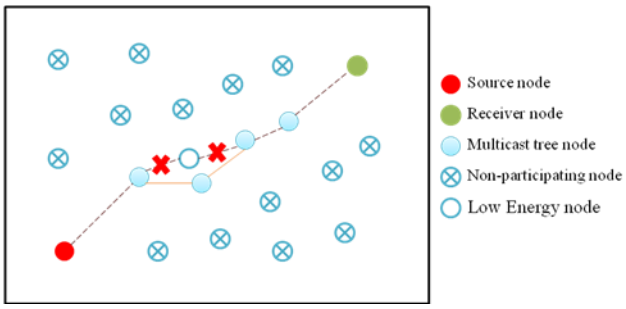
2.4 Local Topology Reconfiguration Mechanism

Nodes with greater signal strength will have more communication link and result in faster energy consumption. So selection CH is necessary after every data transmission. Similarly change of multicast tree node in a path is necessary by choosing alternate path.
The routing algorithm is divided into 3 stages.

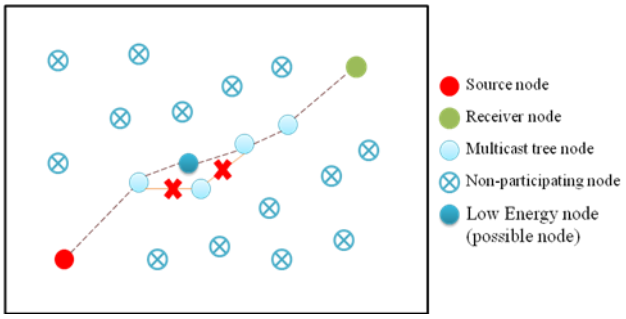
1) In FAF-EBRM, every time node finishes transmission, check the point strength of the next-hop node.



2) If it is less than the average value of all of the sensors' strengths in FTA, remove the link between the nodes.



3) The node removed may be the possible next-hop node when the next transmission is finished, and the revocation of the edge does not affect the possible reconnection. The node's real-time strength is needed to calculate the sum of strengths.



So the distribution of Strength of nodes, node degree and weight of edge leads to improved robustness, fault tolerance, reduces the successive node breakdown and enhances the synchronization of WSN.

3. SECURE ENERGY BALANCED ROUTING METHOD BASED ON FORWARD AWARE FACTOR

This paper proposes a Secure Forward Aware Factor-Energy Balanced Routing Method (FAF-EBRM) based on Verification algorithm. According to data transmission mechanism of WSN, we quantify the forward transmission area; define forward energy density which constitutes forward-aware factor with link weight. For energy efficient transmission in event-driven WSN, Data should be reduced. It requires proper routing method for reliable transmission of aggregated data to sink from the source nodes. This paper propose a new communication protocol based on forward-aware factor in order to determine next-hop node and verification algorithm to reduce the number of transmissions and thus balancing the energy consumption , prolonging the network function lifetime with secure data delivery to improve QoS of WSN.

3.1 Description of Network Model

Sensor nodes are arbitrarily distributed in a rectangular (WxH) sensing field. Normally data sent to the regional central node (CH), then transferred to the sink node. The network model descriptions are,
1) The entire nodes are isomorphic with inadequate communication ability.

© 2017 AJAST All rights reserved.

2) The energy of sensor nodes are limited with initial energy E_0.
3) Nodes can vary transmission power according to the distance to its receiver. Cluster Head have more connection, whose degree and intensity are higher than cluster members.

When the data transmission distance is larger than threshold d_0, the energy consumption would rise sharply, so the maximum communication radial of sensor nodes as d_0.

$$d_0 = \sqrt{\frac{\varepsilon_{fs}}{\varepsilon_{mp}}}$$

Where ε_{fs}- Free space
ε_{mp}-Multipath fading

The function for d(i,sink) is

$$f(d(i,sink)) \in (0, d_0)$$

3.2 Establishment of the network model

The forward transmission area of node i is the intersection of two circles of radius d(i,sink) and d_{ip}.

$$d_{ip} = \max(d_{ij}), j \in N'(i)$$

Where N(i)-set of nodes that have communication link with node i
$N'(i)$-Set of nodes of N(i) that have an edge with node i
d_{ij}- Distance between node a i and j
Generally nodes in the cluster are transmitting data to the sink via cluster head even through the source node is nearer to the sink node. This backward transmission results in waste of energy. So FAF-EBRM proposes a communication protocol that uses forward transmission area according to the position of sink and the final data flow direction. FTA(i) is the overlap section of the two circles, which contains all of the possible next nodes of i.

1. Forward Aware Factor:

The area of FTA(i) is $S_{FTA}(i)$ and is given by,

$$S_{FTA}(i) = \frac{1}{2}\pi d_2^2 - d_2\sqrt{d_1^2 - \frac{1}{4}d_2^2} + \left(d_1^2 - \frac{1}{2}d_2^2\right) \times \arccos\left[1 - \frac{1}{2}\left(\frac{d_2}{d_1}\right)^2\right]$$

Where $d_2 = d_{ip} = \max(d_{ij})$
d_1= d(I,sink)
The area of FTA(i) fulfills the inequality

$$0 < S_{FTA}(i) < \frac{1}{2}\pi d_0^2$$

Where do – maximum communication radial

2. Forward Energy Density

The node's forward energy density FED(i,t) fulfils the equality,

$$FED(i,t) = \frac{\sum_{j \in FTA(i)} E_j(t)}{S_{FTA}(i)}$$

Where $E_j(t)$ is the energy value of node j at time t and $\sum_{j \in FTA(i)} E_j(t)$ is all of the neighbors' energy combined in function FTA(i).

3. Selection of next-hop node

$$j = \max_j [FAF(ij)]$$

3.3 Design of the FAF-EBRM

The routing algorithm can be divided into seven stages as follows.
1) Determine FTA(i) and all of the possible next-hop nodes of node i. Calculate the communication radius d_0 in (1) and set of all possible nodes than have edges with i as N(i)'.Calculation of FTA is depends on sink node and final data flow direction.
2) Determine FTA(j) and area of FTA(j) as $S_{FTA}(j)$ of each possible next-hop node. Similar procedure is followed to determine FTA(j) as FTA(i).
3) Determine Forward energy density of j i.e. FED(j).
4) Calculate the weight of edges between i and each nodes. It uses non-negative constants, residual energy, distance between i and next node, data flow of edge.
5) Calculate FTA(i,j) from the values of FED(j),$w_{ij}(t)$ and calculate FAF of each possible transmit link and choose the next-hop node.
6) If there is no node closer to Sink than i in N(i)',directly compare FAF of all of the nodes in N'(i), and choose the next-hop node. If there is no node in N'(i), i will increase the transmit power to get a longer radius than d_0 until connected with another node, or i will abandon the packet.
7) If Sink is among the forward transmit nodes, I will transmit data directly to sink and complete the routing algorithm.

3.4 Routing parameters of nodes

Neighbor ID- Unique ID of each neighbor
Energy ID- Energy ID of each neighbor
Distance ID- Distance ID to each neighbor
FED ID- FED ID of each neighbor

These are the parameters needed for FAF-EBRM algorithm. The new communication launch node will calculate the weight of edge between neighbors. Neighbors can get their own FED. So it avoids the communication launch node doing all of the algorithms. Thus, each node's memory should capable of store its own ID, real time energy, distance to sink, and FED at every time, which could feedback to launch node quickly.

4. SECURE TRANSMISSION WITH SRL PROTOCOL

In this section we have described our proposed protocol framework for secure routing layer communication and key distribution in dynamic WSNs. Figure 3 show the block diagram of our proposed protocol which consists of base station (BS), two master nodes (S1, S2) and a slave node (N). This framework is divided into five stages viz.

a. Stage 0: Determination and Discovery of Master Nodes.
b. Stage 1: Master Nodes Communication Set-up.
c. Stage 2: Master Nodes Distribution of Authentication Keys.
d. Stage 3: Primary Authentication of Slave Nodes.
e. Stage 4: Secondary Authentication of Slave Nodes.

Secure Routing Layer Protocol (SRLP) is our proposed protocol framework for secure routing layer communication and key

© 2017 AJAST All rights reserved.

distribution between master and slave nodes. Consider a WSN environment of 40 numbers of nodes placed in network randomly from which we have selected one node as base station some nodes as master nodes and others are slave nodes.

4.1 Proposed mathematical model for secure routing layer protocol

Secure Routing Layer Protocol (SRLP) is our proposed protocol framework for secure routing layer communication and key distribution between master and slave nodes.

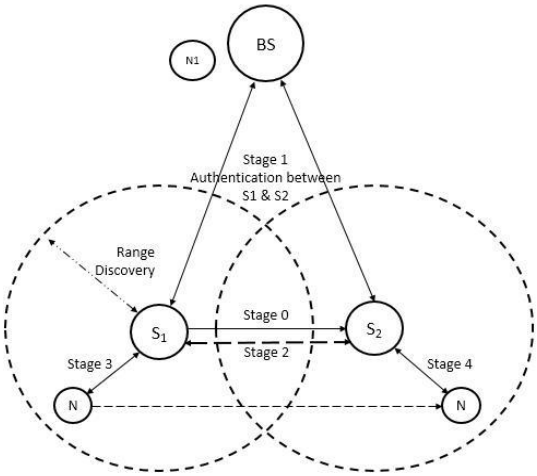


Fig.3. Secure Routing Layer Protocol

Consider a WSN environment of 40 numbers of nodes placed in network randomly from which we have selected one node as base station some nodes as master nodes and others are slave nodes

Here P is the set of phases P= {P_1, P_2, P_3, P_4, P_5}

Stage-0 : P_1 = {AP_I, E_I, M_I}

Where,I = {1, 2, 3….10}

P_1 = Discovery and determination of master nodes.

AP_I = Authentication Packet of master nodes I.

E_I = Encrypted Packet of master node I.

M_I = MAC for master node I.

$AP_I = S_I + \text{“}HELLO\text{”} + E_I + M_I$

S_I = Identification of I^{th} master node.

$E_I = R_I \oplus T_I$

$h:(h(E_I) \oplus h(S_I)) \rightarrow M_I$

$E_I = E_K (E_I \oplus S_I)$

Here, E_K = Encryption function.

R_I = Random number of I^{th} master node.

T_I = Current time stamp.

h = Regular hash function.

S_I: $AP_I \rightarrow$ Network.

4. SIMULATION RESULTS

In this section, the report investigates the simulation cram that examined the network life span and accuracy of our distributed predictive target tracking and verification algorithm. The evaluation result shows the better performance metrics for the parameters such as network lifetime and data security.

4.1 Simulation Environment

We have developed a simulation tool for the IEEE 802.15.4 slotted CSMA/CA mechanism using OPNET simulator. Moreover, we use the default wireless models of OPNET library for emulating the background noise, propagation delay, radio interferences, received power, bit error rate, etc.

4.2 Network Lifespan

The lifespan of the network is the time duration of survival of the node from the instigation of the network operation to the instant that the network can no more afford the readable information.

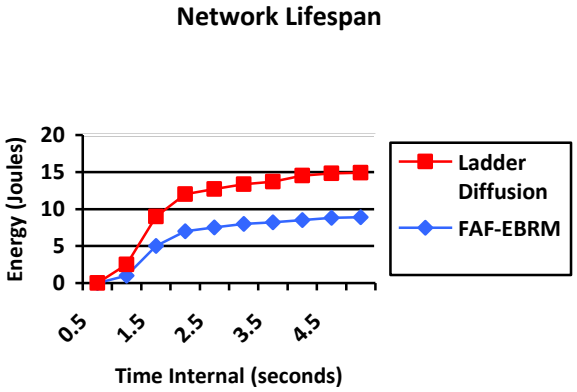


Fig.4. Network Lifetime

This Figure 4 shows the approach regarding the network lifetime under the influence of the protocols Ladder diffusion and FAF-EBRM. It shows that the lifespan of the proposed network is enhanced with reduced energy consumption due to cooperative scheduling of sensor nodes when compared to existing protocol.

4.3 Data precision

The data accuracy is defined as the ratio of summing up the collected image packets by data aggregation technique proposed and the summation of all data packets from individual sensor nodes.

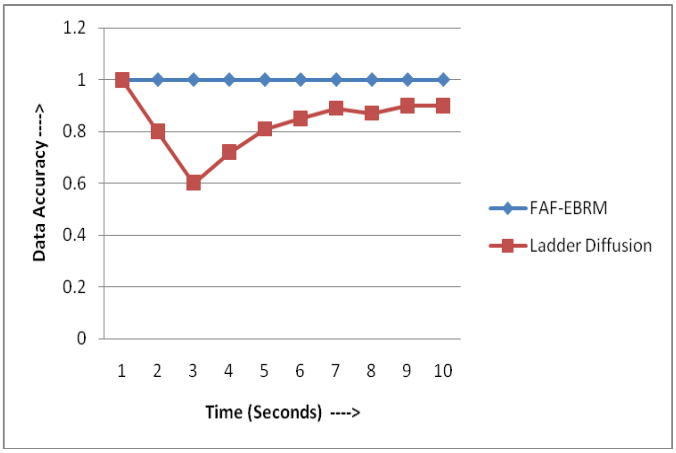


Fig.5. Data Precision

From Figure 5 the accuracy of the proposed technique shows better performance level when compared to existing protocol which contributes fewer chances for collision and furthermore provides better chance for delivery of packets within time limit.

© 2017 AJAST All rights reserved.

5. 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 FAF-EBRM Algorithm and Secure Routing Layer Protocol 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. In Wireless Multimedia Sensor Networks, battery life and the resource reticence plays a vital role. Transmission of image packets also results in more energy consumption. The paper proposes an algorithm for a mobile target tracking surveillance sensor network is supported by sleep docketing technique. The main spotlight of this technique is to optimize the recital metrics such as network lifespan, energy consumption and data security. By applying sleep scheduling method and reducing the efforts of the working nodes energy efficiency can be made superior. Data latency is another significant issue in wireless multimedia sensor applications, in future work the research will be preceded with alternative technique in exploring the communication overhead problem.

REFERENCES

[1] V.Vinu Raja, S.Chinnaiya, "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.*

[2] 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.

[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] I.F. Akyildiz, T. Melodia, and K.R. Chowdury, ―Wireless Multimedia Sensor Networks: A Survey,‖ IEEE Wireless Comm., vol. 14, no. 6, pp. 1339-1352, Dec. 2007.

[5] G. Anastasi, M. Conti, M. D. Francesco, and A. Passarella, ―Energy conservation in wireless sensor networks: A survey, Ad Hoc Networks, vol. 7, no. 3, pp. 537-568, 2009.

[6] A. Aziz, Y. Sekercioglu, P. Fitzpatrick, and M. Ivanovich, ―A Survey on Distributed Topology Control Techniques for Extending the Lifetime of Battery Powered Wireless Sensor Networks,‖ IEEE Commun. Surveys Tuts., vol. PP, no. 99, pp. 1–24, 2012.

[7] S. S. Chatterjea, T. Nieberg, N. Meratnia, and P. Havinga, ―A distributed and self-organizing scheduling algorithm for energy-efficient data aggregation in wireless sensor networks,‖ ACM Trans.Sen. Netw., vol. 4, no. 4, pp. 1-41, 2008.

[8] J. Denga, Y. S. Hanb, W. B. Heinzelmanc, and P. K. Varshney,―Balanced-energy sleep scheduling scheme for jigh density cluster-based sensor networks,‖ in computer communications: special issue on ASWN04, vol. 28, 2005, pp. 1631-1642.

[9] 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.

[10] 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.

AUTHOR BIOGRAPHIES

V.Vinu Raja received his B.E and M.E Degrees in Electronics & Communication Engineering in the year 2009 in Vinayaka Missions University, Salem, Tamilnadu, India and M.E in Applied Electronics in the year 2013 in Anna University, Coimbatore, Tamilnadu, India.. He is currently working as an Assistant Professor in Sri Eshwar College of engineering, Coimbatore. His research area includes Wireless Sensor Networking, Multimedia security, Ethical hacking etc. He is a life time member of ISTE.

Mohammed Irfan Lebbai currently working as a Network administrator in Tata Consultancy Services, Chennai. He is expert in Networking maintence and fixing bugs in realtime Networking environment.

© 2017 AJAST All rights reserved.